Bitdefender ANTIVIRUS PLUS

HƯỚNG DẪN SỬ DỤNG

Bitdefender Antivirus Plus
Hướng dẫn sử dụng

Publication date 09/27/2019

Bản quyền© 2019 Bitdefender

Văn bản Pháp lý

Bảo lưu mọi quyền. Không được sao chép hoặc phát hành bất cứ phần nào của cuốn sách này dưới mọi hình thức hoặc mọi phương tiện, điện tử hay trên giấy, bao gồm cả việc sao chụp, ghi lại hoặc lưu trữ hoặc phục hồi thông tin, mà không có sự cho phép bằng văn bản từ một đại diện được uỷ quyền của Bitdefender. Có thể bao gồm cả bản đánh giá vắn tắt khi xem xét đến nguồn trích dẫn. Không được sửa đổi nội dung dưới mọi hình thức.

Cảnh báo và không chấp nhận. Sản phẩm này và các tài liệu của nó được bảo vệ bằng luật quyền tác giả. Thông tin trong tài liệu này được cung cấp "như là" nguyên bản mà không cần bảo đảm. Mặc dù tất cả các biện pháp phòng ngừa đã được thực hiện trong việc chuẩn bị tài liệu này, các tác giả sẽ không có bất kỳ trách nhiệm pháp lý cho bất kỳ cá nhân hoặc tổ chức đối với bất kỳ tổn thất hoặc thiệt hại gây ra hoặc bị cáo buộc là nguyên nhân trực tiếp hoặc gián tiếp bởi thông tin nêu trong tài liệu này.

Cuốn sách này chứa những liên kết tới các trang web của bên thứ ba không chịu sự kiểm soát của Bitdefender, vì vậy Bitdefender không chịu trách nhiệm đối với nội dung của trang web được kết nối đến. Nếu bạn truy cập một trang web của bên thứ ba liệt kê trong tài liệu này, bạn sẽ phải tự chịu trách nhiệm. Bitdefender cung cấp các liên kết này chỉ để tham khảo, và việc đề cập tới đường kết nối không có nghĩa là Bitdefender xác nhận hoặc chịu trách nhiệm cho nội dung trang web của bên thứ ba.

Thương hiệu. Thương hiệu được đăng ký có thể xuất hiện trong cuốn sách này. Mọi nhãn hiệu đã đăng ký hoặc chưa đăng ký nêu trong tài liệu này là tài sản của chủ sở hữu hợp pháp và được xác nhận chính thức.

Bitdefender

Mục lục

Các bước cài đặt 1
1. Chuẩn bị cho cài đặt 2
2. Yêu cầu hệ thống 3
2.1. Yêu cầu phần mềm 3
3. Đang cài đặt sản phẩm Bitdefender 4
3.1. Cài đặt từ Bitdefender Central 4
3.2. Cài đặt từ đĩa cài đặt 6
Bắt đầu 11
4. Những điều cơ bản 12
4.1. Mở cửa sổ Bitdefender 13
4.2. Thông báo 14
4.3. Hồ sơ 15
4.3.1. Cấu hình tự động kích hoạt các hồ sơ 15
4.4. Mật khẩu bảo vệ thiết lập Bitdefender 16
4.5. Báo cáo sản phẩm 17
4.6. Thông báo khuyến mãi đặc biệt 17
5. Giao diện Bitdefender 18
5.1. Biểu tượng tại khay hệ thống 18
5.2. Chức năng điều hướng 20
5.3. Bảng Điều Khiển 20
5.3.1. Khu vực trạng thái bảo mật 21
5.3.2. Tự động 21
5.3.3. Hành động nhanh 22
5.4. Phần Bitdefender 23
5.4.1. **Bảo vệ** 23
5.4.2. **Riêng tư** 25
5.5. Tiện ích bảo mật 26
5.5.1. Quét các tập tin và thư mục 27
5.5.2. Ẩn / hiện Trình tiện ích bảo mật 28
5.6. Thay đổi ngôn ngữ sản phẩm 28
6. Bitdefender Central 29
6.1. Truy cập Bitdefender Central. 29
6.2. Xác thực hai yếu tố 30
6.2.1. Thêm thiết bị đáng tin cậy 32
6.3. Các Dịch vụ của tôi 32
6.3.1. Kiểm tra các thuê bao có sẵn 32
6.3.2. Thêm một thiết bị mới 33
6.3.3. Gia hạn đăng ký 33
6.3.4. Kích hoạt đăng ký 34
6.4. Các thiết bị của tôi 34
6.5. Thông báo 36

7. Giữ Bitdefender được cập nhật 37
7.1. Kiểm tra xem Bitdefender đã cập nhật chưa 37
7.2. Thực hiện một cập nhật 38
7.3. Bật hoặc tắt chế độ tự động cập nhật 38
7.4. Điều chỉnh các thiết lập cập nhật 39
7.5. Cập nhật liên tục 40

Làm thế nào 41

8. Các bước cài đặt 42
8.1. Làm thế nào để cài đặt Bitdefender trên một máy tính thứ hai? 42
8.2. Làm cách nào để cài đặt lại Bitdefender? 42
8.3. Tôi có thể tải về sản phẩm Bitdefender từ đâu? 43
8.4. Làm thế nào tôi có thể thay đổi ngôn ngữ của Bitdefender sản phẩm? 44
8.5. Làm thế nào để sử dụng bản quyền Bitdefender sau khi nâng cấp Windows? 44
8.6. Làm cách nào để nâng cấp lên phiên bản Bitdefender mới nhất? 47

9. Bitdefender Central 48
9.1. Làm cách nào để tôi đăng nhập vào tài khoản Bitdefender bằng tài khoản khác? 48
9.2. Làm thế nào để tắt tin nhắn trợ giúp Bitdefender Central? 48
9.3. Tôi quên mật khẩu tôi đặt cho tài khoản Bitdefender của tôi. Làm thế nào để thiết lập lại nó? 49
9.4. Làm cách nào để quản lý các phiên đăng nhập được kết hợp với tài khoản Bitdefender của tôi? 49

10. Quét với Bitdefender 51
10.1. Làm thế nào để quét một tập tin hoặc một thư mục? 51
10.2. Làm thế nào để quét hệ thống? 51
10.3. Làm thế nào để lập lịch quét? 52
10.4. Làm thế nào để tạo ra một tác vụ quét tùy chỉnh? 52
10.5. Làm thế nào để loại trừ một thư mục khỏi bị quét? 54
10.6. Phải làm gì khi Bitdefender phát hiện một tập tin sạch mà coi như bị nhiễm virus? 55
10.7. Làm thế nào để kiểm tra Bitdefender đã phát hiện mã độc gì? 55

11. Bảo vệ thông tin cá nhân 57
11.1. Làm thế nào để đảm bảo an toàn giao dịch trực tuyến của tôi? 57
11.2. Làm thế nào để loại bỏ một tập tin vĩnh viễn với Bitdefender? 57
11.3. Làm cách nào tôi có thể khôi phục tệp được mã hóa theo cách thủ công khi quá trình khôi phục không thành công? 58

12. Thông tin trợ giúp 59
12.1. Làm cách nào để kiểm tra giải pháp bảo mật? 59
12.2. Làm thế nào để gỡ bỏ Bitdefender? 59
12.3. Tôi làm cách nào để xóa Bitdefender VPN? 60
12.4. Làm cách nào để xóa tiện ích mở rộng Bitdefender Chống theo dõi 61
12.5. Làm thế nào để tự động tắt máy tính sau khi quá trình quét kết thúc? 62
12.6. Làm thế nào để cấu hình Bitdefender để sử dụng kết nối proxy Internet? 63
12.7. Tôi đang sử dụng phiên bản Windows 32 bit hay 64 bit? 64
12.8. Làm thế nào để hiển thị các đối tượng ẩn trong Windows? 65

12.9. Làm thế nào để gỡ bỏ các giải pháp bảo mật khác? 66
12.10. Làm thế nào để khởi động vào chế độ An toàn? 67

Quản lý An ninh của bạn 69

13. Bảo vệ chống virus 70
13.1. Quét lúc truy cập (bảo vệ thời gian thực) 71
13.1.1. Bật hoặc tắt chế độ bảo vệ thời gian thực 71
13.1.2. Cấu hình các thiết lập bảo vệ theo thời gian thực 71
13.1.3. Khôi phục Cấu hình mặc định 75
13.2. Quét theo yêu cầu 75
13.2.1. Quét một tập tin hoặc thư mục để tìm phần mềm độc hại 76
13.2.2. Chạy một Quét nhanh 76
13.2.3. Chạy một Quét Hệ thống 76
13.2.4. Cấu hình một Quét tùy chỉnh 77
13.2.5. Trình Thuật sĩ quét virus 80
13.2.6. Kiểm tra nhật kí quét 83
13.3. Tự động quét các phương tiện tháo lắp 84
13.3.1. Chúng làm việc như thế nào? 84
13.3.2. Quản lý quét thiết bị tháo lắp 85
13.4. Quét các tập tin hosts 86
13.5. Cấu hình loại trừ quét 86
13.5.1. Loại trừ tập tin và thư mục khỏi quét 86
13.5.2. Loại trừ phần mở rộng tập tin khỏi quét 87
13.5.3. Cấu hình loại trừ quét 88
13.6. Quản lý những tệp tin cách ly 88

14. Phòng chống tấn công nâng cao 90
14.1. Bật hoặc tắt Chế độ Advanced Threat Defense 90
14.2. Kiểm tra các cuộc tấn công độc hại đã phát hiện 90
14.3. Thêm quy trình để loại trừ 91
14.4. Khai thác được phát hiện 91

15. Ngăn chặn mối đe dọa trên mạng 92
15.1. Bitdefender cảnh báo trong trình duyệt 93

16. Lỗ hổng 95
16.1. Quét hệ thống của bạn để tìm các lỗ hổng bảo mật 95
16.2. Sử dụng Tự động giám sát lỗ hổng bảo mật 96
16.3. Cố vấn An ninh Wi-Fi 98
16.3.1. Bật hoặc tắt các thông báo Cố Vấn An Ninh Wifi 99
16.3.2. Cấu hình mạng Wifi gia đình 99
16.3.3. Cấu hình mạng Wifi văn phòng 100
16.3.4. Wi-Fi công cộng 100
16.3.5. Kiểm tra thông tin về mạng Wifi 101

17. Tập Tin An Toàn 103
17.1. Bật hoặc tắt Tập Tin An Toàn 103
17.2. Bảo vệ tập tin cá nhân từ các cuộc tấn công ransomware 104
17.3. Định cấu hình quyền truy cập ứng dụng 104
17.4. Bảo vệ lúc khởi động 105

18. Khắc phục Ransomware 106
18.1. Bật hoặc tắt chức năng Khắc phục Ransomware 106
18.2. Bật hoặc tắt tính năng khôi phục tự động 106
18.3. Xem các tệp đã được khôi phục tự động 106
18.4. Khôi phục các tệp được mã hóa theo cách thủ công 107
18.5. Thêm ứng dụng vào ngoại lệ 107
19. Quản lý mật khẩu bảo vệ tài khoản của bạn 109
19.1. Tạo một cơ sở dữ liệu Ví mới 110
19.2. Nhập một cơ sở dữ liệu có sẵn 110
19.3. Xuất khẩu cơ sở dữ liệu Ví bảo mật 111
19.4. Đồng bộ hóa các ví mình trong đám mây 111
19.5. Quản lý tài khoản với Ví bảo mật 111
19.6. Bật hoặc tắt chức năng bảo vệ Quản lý mật khẩu 112
19.7. Quản lý các thiết lập Quản lý mật khẩu 112
20. Chống theo dõi 116
20.1. Giao diện Chống theo dõi 116
20.2. Tắt Bitdefender Chống theo dõi 117
20.3. Cho phép một trang web được theo dõi 117
21. VPN 119
21.1. Cài đặt VPN 119
21.2. Mở VPN 120
21.3. Giao diện VPN 120
21.4. Các dịch vụ 121
22. Safepay bảo mật các giao dịch trực tuyến 122
22.1. Sử dụng Bitdefender Safepay™ 123
22.2. Thiết lập cấu hình 124
22.3. Quản lý đánh dấu trang 125
22.4. Tắt thông báo Safepay 126
22.5. Sử dụng VPN với Safepay 126
23. Bảo vệ Dữ liệu 127
23.1. Xóa Tệp tin vĩnh viễn 127
24. Miễn dịch USB 128
Tối ưu hóa hệ thống 129
25. Hồ sơ 130
25.1. Hồ sơ Công việc 131
25.2. Hồ sơ Xem phim 132
25.3. Hồ sơ Chơi 133
25.4. Hồ sơ Wi-Fi công cộng 134
25.5. Chế độ Pin Hồ sơ 135
25.6. Tối ưu theo thời gian thực 136
Sửa lỗi 137

26. Giải quyết các vấn đề phổ biến 138
26.1. Hệ thống của tôi chạy chậm 138
26.2. Quét chưa khởi động 139
26.3. Tôi không thể sử dụng ứng dụng nữa 142
26.4. Phải làm gì khi Bitdefender chặn trang web, tên miền, địa chỉ IP hoặc ứng dụng trực tuyến an toàn 143
26.5. Phải làm gì nếu Bitdefender phát hiện một ứng dụng an toàn lại là mã độc tống tiền. 143
26.6. Làm thế nào để cập nhật Bitdefender trên một đường truyền Internet chậm .. 144
26.7. Các dịch vụ của Bitdefender không phản hồi 144
26.8. Tính năng Tự động điền thông tin trong Ví bảo mật của tôi không làm việc ... 145
26.9. Gỡ bỏ Bitdefender không thực hiện được 146
26.10. Hệ thống của tôi không khởi động sau khi cài đặt Bitdefender 147

27. Loại bỏ phần mềm độc hại khỏi hệ thống của bạn 151
27.1. Bitdefender Chế độ cứu hộ (Cứu hộ trong môi trường Windows 10) 151
27.2. Phải làm gì khi Bitdefender tìm thấy các mối đe dọa trên máy tính của bạn? 155
27.3. Làm thế nào để làm sạch virus trong một tập tin nén? 156
27.4. Làm thế nào để làm sạch mã độc trong một e-mail nén? 157
27.5. Phải làm gì nếu tôi nghi ngờ một tập tin là nguy hiểm? 158
27.6. Các tập tin có mật khẩu bảo vệ trong các bản ghi lịch sử quét là gì? 159
27.7. Các đối tượng bị bỏ qua được lưu trong các bản ghi lịch sử quét là gì? 159
27.8. Các tập tin nén quá nhiều lớp trong các bản ghi lịch sử quét là gì? 159
27.9. Tại sao Bitdefender tự động xóa một tập tin bị nhiễm? 160

Liên hệ chúng tôi 161

28. Muốn được giúp 162

29. Nguồn thông tin trực tuyến 164
29.1. Trung tâm hỗ trợ Bitdefender 164
29.2. Diễn đàn Hỗ trợ Bitdefender 164
29.3. Cổng thông tin HOTforSecurity 165

30. Thông tin Liên hệ 166
30.1. Các địa chỉ Web 166
30.2. Các nhà phân phối địa phương 166
30.3. Văn phòng của Bitdefender 167

Sổ tay thuật ngữ 169

CÁC BƯỚC CÀI ĐẶT

1. CHUẨN BỊ CHO CÀI ĐẶT

Trước khi cài đặt Bitdefender Antivirus Plus, hoàn thành công tác chuẩn bị để đảm bảo quá trình cài đặt sẽ diễn ra suôn sẻ:

- Đảm bảo rằng máy tính nơi bạn định cài đặt Bitdefender đáp ứng các yêu cầu hệ thống. Nếu máy tính không đáp ứng tất cả các yêu cầu hệ thống, Bitdefender sẽ không được cài đặt hoặc nếu được cài đặt, nó sẽ không hoạt động đúng và nó sẽ gây chậm hệ thống và mất ổn định. Danh sách đầy đủ các yêu cầu hệ thống có tại "*Yêu cầu hệ thống*" (p. 3).
- Đăng nhập vào máy tính bằng tài khoản Administrator.
- Loại bỏ mọi phần mềm tương tự khỏi máy tính. Nếu phát hiện bất kỳ trong quá trình cài đặt Bitdefender, bạn sẽ được thông báo để gỡ cài đặt. Chạy hai chương trình bảo mật đồng thời có thể ảnh hưởng đến hoạt động của chúng và gây ra vấn đề nghiêm trọng với hệ thống. Windows Defender sẽ bị vô hiệu hóa trong khi cài đặt.
- Bạn nên kết nối với máy tính của mình với internet trong khi cài đặt, ngay cả khi cài đặt từ đĩa CD/DVD. Nếu có phiên bản mới hơn trong gói cài đặt, Bitdefender có thể tải về và cài đặt chúng.

2. YÊU CẦU HỆ THỐNG

Bạn có thể cài đặt Bitdefender Antivirus Plus trên các máy tính đang chạy một trong các hệ điều hành dưới đây:

- Windows 7 Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

- 2.5 GB ổ cứng trống (ít nhất còn trống 800MB trên ổ đĩa hệ thống)
- Intel CORE 2 Duo (2 GHz) hoặc tương đương
- 2 GB bộ nhớ (RAM)

Ghi chú

Để tìm hiểu hệ điều hành Windows máy tính của bạn đang chạy và các thông tin phần cứng:

- Trong **Windows 7**, nhấp chuột phải vào biểu tượng**My Computer** và sau đó chọn **Properties** từ trình đơn.
- Trong **Windows 8**, từ màn hình Start của Windows, xác định vị trí **máy tính** (ví dụ, bạn có thể gõ "Computer" trực tiếp vào ô Start), và sau đó nhấp chuột phải vào biểu tượng của nó. Trong **Windows 8.1** , xác định vị trí **PC này** .

  Chọn **Thuộc tính** từ trình đơn phía dưới. Tìm trong khu vực **Hệ thống** để tìm thông tin về loại hình hệ thống của bạn.
- Trong **Windows 10** , gõ **System** trong hộp tìm kiếm từ thanh tác vụ và nhấp vào biểu tượng của nó. Tìm trong khu vực **Hệ thống** để tìm thông tin về loại hình hệ thống của bạn.

2.1. Yêu cầu phần mềm

Để có thể sử dụng Bitdefender với tất cả các tính năng, máy tính của bạn cần phải đáp ứng các yêu cầu phần mềm sau đây:

- Microsoft Edge 40 hoặc cao hơn
- Internet Explorer 10 trở lên
- Mozilla Firefox 51 trở lên
- Google Chrome 34 trở lên

3. ĐANG CÀI ĐẶT SẢN PHẨM BITDEFENDER

Bạn có thể cài đặt Bitdefender từ đĩa cài đặt, hoặc bằng cách sử dụng các trình cài đặt được tải về từ Bitdefender Central.

Nếu bạn mua sản phẩm dùng cho nhiều máy tính (ví dụ, bạn mua Bitdefender Antivirus Plus cho 3 máy tính), lặp lại quá trình cài đặt và kích hoạt sản phẩm của bạn với cùng tài khoản trên từng máy tính. Các tài khoản bạn cần sử dụng là một trong đó có chứa Bitdefender của bạn đăng ký hoạt động.

3.1. Cài đặt từ Bitdefender Central

Từ Bitdefender Central bạn có thể tải về bộ cài đặt tương ứng bản quyền đã mua. Một khi quá trình cài đặt hoàn tất, Bitdefender Antivirus Plus được kích hoạt.

Để tải về Bitdefender Antivirus Plus từ Bitdefender Central:

1. Truy cập Bitdefender Central.
2. Trong của sổ **Các Thiết Bị Của Tôi** nhấp **Cài đặt bảo vệ**.
3. Chọn một trong hai tùy chọn có sẵn:

   - **Bảo vệ thiết bị này**

     a. Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.

     b. Lưu tập tin cài đặt.

   - **Bảo vệ các thiết bị khác**

     a. Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.

     b. Nhấn **GỬI LIÊN KẾT TẢI XUỐNG**.

     c. Nhập địa chỉ e-mail trong các trường tương ứng, và nhấn **GỬI EMAIL**.

     Lưu ý rằng liên kết tải xuống được tạo chỉ hợp lệ trong 24 giờ tiếp theo. Nếu liên kết hết hạn, bạn sẽ phải tạo một liên kết mới bằng cách làm theo các bước tương tự.

     d. Trên thiết bị bạn muốn cài đặt sản phẩm Bitdefender của bạn, hãy kiểm tra tài khoản email bạn đã nhập, sau đó nhấp vào nút tải xuống tương ứng.

4. Đợi tải về để hoàn thành, sau đó chạy trình cài đặt.

Xác nhận việc cài đặt

Bitdefender đầu tiên sẽ kiểm tra hệ thống của bạn để xác nhận việc cài đặt.

Nếu hệ thống của bạn không đáp ứng các yêu cầu hệ thống để cài đặt Bitdefender, bạn sẽ được thông báo về các yêu cầu cần đáp ứng trước khi bạn có thể tiến hành.

Nếu một giải pháp chống virus không tương thích hoặc một phiên bản Bitdefender cũ được phát hiện, bạn sẽ được thông báo để loại bỏ chúng khỏi hệ thống. Hãy làm theo hướng dẫn để gỡ bỏ phần mềm khỏi hệ thống của bạn, nhằm tránh vấn đề xảy ra sau này. Bạn có thể cần khởi động lại máy tính để hoàn thành việc gỡ bỏ các chương trình chống virus được phát hiện.

Gói cài đặt Bitdefender Antivirus Plus được cập nhật liên tục.

Ghi chú

Tải về các tập tin cài đặt có mất một khoảng thời gian, nhất là khi kết nối Internet bị chậm.

Khi cài đặt được xác nhận, hướng dẫn cài đặt xuất hiện. Thực hiện các bước tiếp theo để cài đặt Bitdefender Antivirus Plus.

Bước 1 - Cài đặt Bitdefender

Trước khi tiến hành cài đặt, bạn phải đồng ý với Thỏa thuận Đăng ký. Vui lòng dành chút thời gian để đọc Thỏa thuận đăng ký vì nó chứa các điều khoản và điều kiện mà bạn có thể sử dụng Bitdefender Antivirus Plus.

Nếu bạn không đồng ý với các điều khoản, hãy đóng cửa sổ cài đặt. Quá trình cài đặt sẽ chấm dứt và bạn sẽ thoát khỏi chương trình cài đặt.

Hai nhiệm vụ bổ sung có thể được thực hiện tại bước này:

- Giữ **Gửi báo cáo sản phẩm** tùy chọn kích hoạt. Bằng cách cho phép tùy chọn này, các báo cáo có chứa thông tin về cách bạn sử dụng sản phẩm được gửi đến máy chủ Bitdefender. Thông tin này là cần thiết để hoàn thiện sản phẩm và có thể cung cấp cho chúng tôi kinh nghiệm tốt hơn cho tương lai. Lưu ý rằng các báo cáo này không chứa các dữ liệu bí mật, chẳng hạn như tên hoặc địa chỉ IP của bạn, và sẽ không được sử dụng cho mục đích thương mại.
- Chọn ngôn ngữ bạn muốn cài đặt sản phẩm tại.

Nhấp vào **CÀI ĐẶT** để khởi chạy quá trình cài đặt sản phẩm Bitdefender của bạn.

Bước 2: Đang trong tiến trình cài đặt.

Vui lòng đợi cho quá trình cài đặt hoàn tất. Thông tin chi tiết về tiến trình được hiển thị.

Bước 3 - Cài đặt hoàn thành

Sản phẩm Bitdefender của bạn đã được cài đặt thành công.

Một bản tóm tắt quá trình cài đặt được hiển thị. Nếu có bất kỳ phần mềm độc hại nào được phát hiện và loại bỏ trong quá trình cài đặt, có thể phải khởi động lại máy tính. Nhấn **BẮT ĐẦU SỬ DỤNGBitdefender** để tiếp tục.

Bước 4 - Bắt đầu

Trong cửa sổ **Bắt đầu**, bạn có thể xem chi tiết về đăng ký hoạt động của mình.

Nhấn vào **Finish** để truy cập giao diện Bitdefender Antivirus Plus.

3.2. Cài đặt từ đĩa cài đặt

Để cài đặt Bitdefender từ đĩa cài đặt, cho đĩa vào ổ đĩa quang.

Một màn hình cài đặt sẽ được hiển thị ngay sau đó Thực hiện theo các hướng dẫn để bắt đầu cài đặt.

Nếu màn hình cài đặt không xuất hiện, sử dụng Windows Explorer để duyệt đến thư mục gốc của đĩa và nhấp đúp vào nó tập tin autorun.Exe.

Nếu tốc độ Internet của bạn chậm, hoặc hệ thống của bạn không được kết nối với Internet, nhấp vào nút **Cài đặt từ đĩa CD/DVD** . Trong trường hợp này, các sản phẩm Bitdefender có sẵn trên đĩa sẽ được cài đặt và phiên bản mới hơn sẽ được tải về từ các máy chủ Bitdefender thông qua cập nhật sản phẩm.

Xác nhận việc cài đặt

Bitdefender đầu tiên sẽ kiểm tra hệ thống của bạn để xác nhận việc cài đặt.

Nếu hệ thống của bạn không đáp ứng các yêu cầu hệ thống để cài đặt Bitdefender, bạn sẽ được thông báo về các yêu cầu cần đáp ứng trước khi bạn có thể tiến hành.

Nếu một giải pháp chống virus không tương thích hoặc một phiên bản Bitdefender cũ được phát hiện, bạn sẽ được thông báo để loại bỏ chúng khỏi hệ thống. Hãy làm theo hướng dẫn để gỡ bỏ phần mềm khỏi hệ thống của bạn, nhằm tránh vấn đề xảy ra sau này. Bạn có thể cần khởi động lại máy tính để hoàn thành việc gỡ bỏ các chương trình chống virus được phát hiện.

Ghi chú

Tải về các tập tin cài đặt có mất một khoảng thời gian, nhất là khi kết nối Internet bị chậm.

Khi cài đặt được xác nhận, hướng dẫn cài đặt xuất hiện. Thực hiện các bước tiếp theo để cài đặt Bitdefender Antivirus Plus.

Bước 1 - Cài đặt Bitdefender

Trước khi tiến hành cài đặt, bạn phải đồng ý với Thỏa thuận Đăng ký. Vui lòng dành chút thời gian để đọc Thỏa thuận đăng ký vì nó chứa các điều khoản và điều kiện mà bạn có thể sử dụng Bitdefender Antivirus Plus.

Nếu bạn không đồng ý với các điều khoản, hãy đóng cửa sổ cài đặt. Quá trình cài đặt sẽ chấm dứt và bạn sẽ thoát khỏi chương trình cài đặt.

Hai nhiệm vụ bổ sung có thể được thực hiện tại bước này:

- Giữ **Gửi báo cáo sản phẩm** tùy chọn kích hoạt. Bằng cách cho phép tùy chọn này, các báo cáo có chứa thông tin về cách bạn sử dụng sản phẩm được gửi đến máy chủ Bitdefender. Thông tin này là cần thiết để hoàn thiện sản phẩm và có thể cung cấp cho chúng tôi kinh nghiệm tốt hơn cho tương lai. Lưu ý rằng các báo cáo này không chứa các dữ liệu bí mật, chẳng hạn như tên hoặc địa chỉ IP của bạn, và sẽ không được sử dụng cho mục đích thương mại.
- Chọn ngôn ngữ bạn muốn cài đặt sản phẩm tại.

Nhấp vào **CÀI ĐẶT** để khởi chạy quá trình cài đặt sản phẩm Bitdefender của bạn.

Bước 2: Đang trong tiến trình cài đặt.

Vui lòng đợi cho quá trình cài đặt hoàn tất. Thông tin chi tiết về tiến trình được hiển thị.

Bước 3 - Cài đặt hoàn thành

Một bản tóm tắt quá trình cài đặt được hiển thị. Nếu có bất kỳ phần mềm độc hại nào được phát hiện và loại bỏ trong quá trình cài đặt, có thể phải khởi động lại máy tính. Nhấn **BẮT ĐẦU SỬ DỤNGBitdefender** để tiếp tục.

Bước 4 - Bitdefender tài khoản

Sau khi bạn hoàn thành thiết lập ban đầu, cửa sổ Tài khoản Bitdefender sẽ xuất hiện. Một tài khoản Bitdefender được yêu cầu để kích hoạt sản phẩm và sử dụng các tính năng trực tuyến. Để biết thêm thông tin, hãy chuyển đến "*Bitdefender Central*" (p. 29).

Tiến hành tùy theo tình hình của bạn.

- **Tôi muốn tạo một tài khoản Bitdefender**

  1. Nhập các thông tin cần thiết vào các trường tương ứng. Các dữ liệu bạn cung cấp tại đây sẽ được giữ bí mật. Mật khẩu phải dài ít nhất 8 ký tự, bao gồm ít nhất một số hoặc ký tự đặc biệt và bao gồm các ký tự chữ thường và chữ hoa.
  2. Trước khi tiếp tục, bạn phải đồng ý với Điều khoản sử dụng. Truy cập Điều khoản sử dụng và đọc chúng cẩn thận vì chúng chứa các điều khoản và điều kiện mà bạn có thể sử dụng Bitdefender.

     Ngoài ra, bạn có thể truy cập và đọc Chính sách bảo mật.
  3. Nhấp vào **TẠO TÀI KHOẢN**.

  > **Ghi chú**
  > Khi tài khoản được tạo, bạn có thể sử dụng địa chỉ email và mật khẩu được cung cấp để đăng nhập vào tài khoản của mình tại https://central.bitdefender.com hoặc trong ứng dụng Bitdefender Central miễn là ứng dụng được cài đặt trên một trong các thiết bị Android của bạn hoặc thiết bị iOS. Để cài đặt ứng dụng Bitdefender Central trên Android, bạn phải truy cập Google Play, tìm kiếm Bitdefender Central, sau đó chạm vào tùy chọn cài đặt tương ứng. Để cài đặt ứng dụng Bitdefender Central trên iOS, bạn phải truy cập App Store, tìm kiếm Bitdefender Central, sau đó chạm vào tùy chọn cài đặt tương ứng.

- **Tôi đã có tài khoản Bitdefender**

  1. Nhấp vào **Đăng nhập**.
  2. Nhập địa chỉ email vào trường tương ứng, sau đó nhấp vào **TIẾP THEO**.

3. Nhập mật khẩu của bạn và sau đó nhấp vào **ĐĂNG KÝ**.

   Nếu bạn quên mật khẩu cho tài khoản của mình hoặc bạn chỉ muốn đặt lại mật khẩu bạn đã đặt:

   a. Nhấp vào **Quên mật khẩu?**.

   b. Nhập địa chỉ email của bạn, sau đó nhấp vào **TIẾP THEO**.

   c. Kiểm tra tài khoản email của bạn, nhập mã bảo mật bạn đã nhận được và sau đó nhấp vào **TIẾP THEO**.

      Ngoài ra, bạn có thể nhấp vào **Thay đổi mật khẩu** trong email mà chúng tôi đã gửi cho bạn.

   d. Nhập mật khẩu mới bạn muốn đặt, sau đó nhập lại mật khẩu. Nhấp chuột vào **Lưu**.

   Ghi chú
   Nếu bạn đã có tài khoản MyBitdefender, bạn có thể sử dụng nó để đăng nhập vào tài khoản Bitdefender của bạn. Nếu bạn quên mật khẩu của bạn, trước tiên bạn cần phải https://my.bitdefender.com đặt lại mật khẩu. Sau đó, sử dụng các thông tin cập nhật để đăng nhập vào tài khoản Bitdefender của bạn.

- **Tôi muốn đăng nhập dùng tài khoản Microsoft, Facebook hoặc Google**

  Để đăng nhập tài khoản với Microsoft, Facebook hoặc Google

  1. Chọn dịch vụ mà bạn muốn sử dụng. Bạn sẽ được chuyển đến trang đăng nhập của dịch vụ đó.
  2. Thực hiện theo hướng dẫn được cung cấp bởi dịch vụ để liên kết tài khoản của bạn đến Bitdefender.

  Ghi chú
  Bitdefender không thể truy cập vào những thông tin bí mật như mật khẩu của tài khoản bạn sử dụng để đăng nhập, hoặc các thông tin cá nhân của bạn bè và địa chỉ liên lạc của bạn.

Bước 5 - Kích hoạt sản phẩm của bạn

> **Ghi chú**
> Bước này xuất hiện nếu bạn đã chọn để tạo ra tài khoản Bitdefender mới trong bước trước, hoặc nếu bạn đăng nhập bằng một tài khoản với một thuê bao đã hết hạn.

Cần kết nối Internet để hoàn thành quá trình đăng ký sản phẩm.

Tiến hành tùy theo tình hình của bạn:

- Tôi có mã kích hoạt

  Trong trường hợp này, đăng ký sản phẩm theo các bước sau:

  1. Nhập mã kích hoạt trong **Tôi có mã kích hoạt** , và sau đó nhấp vào **TIẾP TỤC**.

     > **Ghi chú**
     > Bạn có thể tìm thấy mã kích hoạt của bạn:
     > - Trên tem dán trên đĩa CD.
     > - trên thẻ đăng ký mã số bản quyền.
     > - trong e-mail mua hàng trực tuyến.

  2. **Tôi muốn đánh giá Bitdefender**

     Trong trường hợp này, bạn có thể sử dụng sản phẩm trong thời gian 30 ngày. Để bắt đầu giai đoạn thử nghiệm, chọn **tôi không có bản quyền, tôi muốn dùng thử sản phẩm miễn phí** , và sau đó nhấp vào **TIẾP TỤC**.

Bước 6 - Bắt đầu

Trong cửa sổ **Bắt đầu** bạn có thể xem chi tiết về bản quyền đang hoạt động của mình.

Nhấn vào **Finish** để truy cập giao diện Bitdefender Antivirus Plus.

BẮT ĐẦU

4. NHỮNG ĐIỀU CƠ BẢN

Một khi bạn đã cài đặt Bitdefender Antivirus Plus, máy tính của bạn đã được bảo vệ chống lại tất cả các loại phần mềm độc hại (như mã độc, phần mềm gián điệp, ransomware, khai thác, botnet và trojans).

Ứng dụng sử dụng công nghệ Photon để nâng cao tốc độ và hiệu suất cho việc quét các phần mềm độc hại. Nó hoạt động bằng cách học hỏi các mô hình sử dụng các ứng dụng của hệ thống để biết khi nào tiến hành quét virus, do đó giảm thiểu tác động đến hiệu năng hệ thống.

Kết nối với mạng không dây công cộng thuộc sân bay, trung tâm mua sắm, quán cà phê hoặc khách sạn mà không được bảo vệ có thể gây nguy hiểm cho thiết bị và dữ liệu của bạn. Điều này chủ yếu là do những kẻ lừa đảo có thể đang theo dõi hoạt động của bạn và tìm thời điểm tốt nhất để đánh cắp dữ liệu cá nhân, nhưng cũng vì mọi người đều có thể thấy địa chỉ IP của bạn, do đó biến máy của bạn trở thành nạn nhân của các cuộc tấn công mạng trong tương lai. Để tránh những tình huống không may như vậy, hãy cài đặt và sử dụng ứng dụng "*VPN*" (p. 119).

Bạn có thể theo dõi mật khẩu và tài khoản trực tuyến bằng cách lưu trữ chúng "*Quản lý mật khẩu bảo vệ tài khoản của bạn*" (p. 109) trong ví Với một mật khẩu chính duy nhất, bạn có thể bảo vệ sự riêng tư của bạn khỏi những kẻ xâm nhập đang cố gắng lấy tiền của bạn.

Để bảo vệ bạn khỏi những kẻ xấu và gián điệp tiềm ẩn khi thiết bị của bạn được kết nối với mạng không dây không an toàn, Bitdefender phân tích mức độ bảo mật khi cần thiết, đi kèm với các đề xuất để tăng cường sự an toàn cho các hoạt động trực tuyến của bạn. Để biết hướng dẫn về an toàn dữ liệu cá nhân của bạn, hãy tham khảo "*Cố vấn An ninh Wi-Fi*" (p. 98).

Các tập tin cá nhân của bạn được lưu trữ trên đĩa cứng như tài liệu, ảnh hoặc phim ảnh cũng như các tệp tin lưu trữ trong đám mây có thể tránh xa phần mềm độc hại nguy hiểm hiện nay là ransomware. Để biết thông tin về cách xử lý các tệp cá nhân sao cho an toàn, vui lòng tham khảo "*Tập Tin An Toàn*" (p. 103).

Các tập tin được mã hóa bởi phần mềm ransomware bây giờ có thể được phục hồi mà không cần phải chi tiền cho bất kỳ khoản tiền chuộc yêu cầu nào. Để biết thông tin về cách khôi phục các tệp được mã hóa, hãy tham khảo "*Khắc phục Ransomware*" (p. 106).

Trong khi bạn làm việc, chơi game hoặc xem phim, Bitdefender để cho người dùng trải nghiệm liên tục bằng cách trì hoãn nhiệm vụ bảo dưỡng, loại bỏ gián đoạn và điều chỉnh hiệu ứng hình ảnh thích hợp. Bạn có thể hưởng lợi từ tất cả bằng cách kích hoạt và cấu hình "*Hồ sơ*" (p. 130).

Bitdefender sẽ đưa ra những quyết định liên quan đến an ninh tốt nhất cho bạn và sẽ hiếm khi hiển thị cửa sổ cảnh báo. Thông tin chi tiết về các thao tác và các thông tin về hoạt động chương trình có sẵn trong cửa sổ thông báo. Để biết thêm thông tin, hãy chuyển đến "*Thông báo*" (p. 14).

Theo thời gian, bạn nên mở Bitdefender và sửa chữa bất kỳ vấn đề hiện tại. Bạn có thể có cấu hình cụ thể những thành phần Bitdefender hoặc có những hành động phòng ngừa để bảo vệ máy tính và dữ liệu của bạn.

Để sử dụng các tính năng trực tuyến của Bitdefender Antivirus Plus và quản lý thuê bao và thiết bị của bạn, truy cập tài khoản Bitdefender của bạn. Để biết thêm thông tin, hãy chuyển đến "*Bitdefender Central*" (p. 29).

Phần "Làm thế nào" (p. 41) là nơi mà bạn sẽ tìm thấy hướng dẫn từng bước về cách thực hiện các tác vụ thông thường. Nếu bạn gặp vấn đề trong khi sử dụng Bitdefender, kiểm tra phần "*Giải quyết các vấn đề phổ biến*" (p. 138) để tìm giải pháp khả thi cho các vấn đề phổ biến nhất.

4.1. Mở cửa sổ Bitdefender

Để truy cập vào giao diện chính của Bitdefender Antivirus Plus, hãy theo các bước dưới đây:

- Trong **Windows 7**:
  1. Nhấp **Bắt đầu** và tới **Tất cả các chương trình**.
  2. Nhấp **Bitdefender**.
  3. Nhấp **Bitdefender Antivirus Plus** hoặc nhanh hơn, nhấn đúp biểu tượng Bitdefender tại khay hệ thống.
- Trong **Windows 8 and Windows 8.1**:

  Xác định vị trí Bitdefender từ màn hình Start của Windows (ví dụ, bạn có thể bắt đầu gõ "Bitdefender" trực tiếp vào màn hình Start), và sau đó nhấp vào biểu tượng của nó. Ngoài ra, có thể mở ứng dụng từ màn hình máy tính và sau đó kích đúp vào biểu tượng Bitdefender trong khay hệ thống.
- Trong **Windows 10**:

Loại "Bitdefender" trong hộp tìm kiếm trên thanh tác vụ và sau đó nhấp vào biểu tượng của nó. Ngoài ra, nhấp double chuột vào Bitdefender biểu tượng trong thanh hệ thống.

Để biết thêm thông tin về tính năng và biểu tượng trong khay hệ thống của Bitdefender, vui lòng tham khảo "*Giao diện Bitdefender*" (p. 18).

4.2. Thông báo

Bitdefender giữ một bản ghi chi tiết các sự kiện liên quan đến hoạt động của nó trên máy tính của bạn. Bất cứ khi nào có vấn đề liên quan đến sự an toàn của hệ thống hoặc dữ liệu của bạn xảy ra, một sự kiện mới được thêm vào mục vùng thông báoBitdefender, theo một cách tương tự như một e-mail mới xuất hiện trong hộp thư của bạn.

Các thông báo là một công cụ quan trọng trong việc giám sát và quản lý việc bảo vệ của Bitdefender. Chẳng hạn, bạn sẽ dễ dạng kiểm tra các lần cập nhật được thực hiện thành công, hay tìm thấy virus lây nhiễm trên máy của bạn, v.v... Ngoài ra, bạn có thể có thêm hành động nếu cần thiết hoặc thay đổi hành động của Bitdefender.

Để truy cập nhật ký Thông báo, hãy nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender. Mỗi khi một sự kiện quan trọng xảy ra, một truy cập có thể được nhận thấy trên biểu tượng 2.

Tùy thuộc vào loại và mức độ nghiêm trọng, thông báo được nhóm lại trong:

- Sự kiện **Quan trọng** cho biết những vấn đề quan trọng. Bạn nên kiểm tra ngay lập tức.
- Sự kiện **Cảnh báo** cho biết những vấn đề ít quan trọng. Bạn nên kiểm tra và sửa chữa chúng khi có thời gian.
- Sự kiện **Thông tin** cho biết những hoạt động thành công.

Nhấn vào mỗi tab để tìm thêm thông tin chi tiết về các sự kiện được tạo. Giới thiệu tóm tắt các chi tiết được hiển thị khi nhấp chuột trên mỗi tiêu đề sự kiện, cụ thể là: một mô tả ngắn, hành động Bitdefender vào nó khi nó đã xảy ra, và ngày và thời gian khi nó xảy ra. Tùy chọn có thể được cung cấp để có thêm hành động nếu cần.

Để giúp bạn dễ dàng quản lý các sự kiện, cửa sổ Thông báo cung cấp tùy chọn để xóa hoặc đánh dấu là đã đọc tất cả các sự kiện trong phần đó.

4.3. Hồ sơ

Một số hoạt động máy tính, chẳng hạn như trò chơi trực tuyến hay thuyết trình video, đòi hỏi tăng cường hệ thống, hiệu suất cao và không bị gián đoạn. Khi máy tính xách tay của bạn đang chạy bằng pin, tốt nhất là tạm hoãn lại các hoạt động không cần thiết có tiêu thụ năng lượng cho đến khi máy tính xách tay được kết nối trở lại nguồn điện.

Bitdefender Hồ sơ sẽ gán nhiều tài nguyên hệ thống hơn cho các ứng dụng đang chạy bằng cách tạm thời sửa đổi cài đặt bảo vệ và điều chỉnh cấu hình hệ thống. Do đó, tác động vào hệ thống đang hoạt động của bạn được giảm thiểu.

Để thích ứng với các hoạt động khác nhau, Bitdefender đi kèm với các Hồ sơ sau:

Hồ sơ Công việc
: Tối ưu hóa hiệu quả công việc của bạn bằng cách xác định và điều chỉnh các cài đặt cho sản phẩm và hệ thống.

Hồ sơ Xem phim
: Tăng cường hiệu ứng hình ảnh và loại bỏ gián đoạn khi xem phim.

Hồ sơ Chơi
: Tăng cường hiệu ứng hình ảnh và loại bỏ gián đoạn khi chơi trò chơi.

Hồ sơ Wi-Fi công cộng
: Xác nhận cài đặt sản phẩm để được hưởng lợi từ việc bảo vệ đầy đủ trong khi kết nối với một mạng không dây không an.

Chế độ Pin Hồ sơ
: Xác nhận cài đặt sản phẩm và giữ hoạt động nền để tiết kiệm pin.

4.3.1. Cấu hình tự động kích hoạt các hồ sơ

Để dễ sử dụng, bạn có thể cấu hình chế độ Bitdefender để quản lý chế độ làm việc. Trong trường hợp này, Bitdefender tự động phát hiện các hoạt động bạn thực hiện và hệ thống và tối ưu hóa sản phẩm ứng dụng cài đặt.

Để cho phép Bitdefender để kích hoạt hồ sơ:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. Sử dụng nút chuyển đổi tương ứng để bật **Kích hoạt hồ sơ tự động** .

Nếu bạn không muốn Hồ sơ được tự động kích hoạt, tắt công tắc.

Để kích hoạt hồ sơ cá nhân, bật nút tương ứng. Trong ba cấu hình đầu tiên, chỉ một cấu hình có thể được kích hoạt bằng tay cùng một lúc.

Để biết thêm thông tin, tham khảo "*Hồ sơ*" (p. 130)

4.4. Mật khẩu bảo vệ thiết lập Bitdefender

Nếu bạn không phải là người duy nhất có quyền Admin sử dụng máy tính này thì chúng tôi khuyên bạn nên bảo vệ các phần cài đặt Bitdefender của mình bằng một mật khẩu.

Để cấu hình bảo vệ mật khẩu cho các Bitdefender cài đặt:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **Chung**, hãy bật **Bảo vệ bằng mật khẩu**.
3. Nhập mật khẩu vào hai lần sau đó bấm **OK**. Mật khẩu dài tối thiểu 8 ký tự.

Một khi bạn đã thiết lập một mật khẩu, bất cứ ai cố gắng thay đổi thiết lập Bitdefender trước tiên sẽ phải cung cấp mật khẩu.

Quan trọng

Hãy ghi nhớ mật khẩu của bạn hoặc lưu giữ nó tại một nơi an toàn. Nếu bạn quên mật khẩu, bạn sẽ phải cài đặt lại chương trình hoặc liên hệ với hỗ trợ Bitdefender.

Để gỡ bỏ mật khẩu bảo vệ:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **Chung**, hãy tắt **Bảo vệ bằng mật khẩu**.
3. Nhập mật khẩu sau đó bấm **OK**.

Ghi chú

Để thay đổi mật khẩu cho sản phẩm của bạn, nhấp vào **Thay đổi mật khẩu**. Nhập mật khẩu của bạn sau đó bấm **OK**. Trong cửa sổ mới xuất hiện nhập mật khẩu mới mà bạn muốn sử dụng từ bây giờ để hạn chế quyền truy cập vào cài đặt Bitdefender của bạn.

4.5. Báo cáo sản phẩm

Báo cáo sản phẩm chứa thông tin về cách bạn sử dụng sản phẩm Bitdefender bạn đã cài đặt. Thông tin này là cần thiết để cải thiện sản phẩm và có thể giúp chúng tôi đem tới cho bạn một trải nghiệm sản phẩm tốt hơn trong tương lai.

Lưu ý rằng các báo cáo này không chứa các dữ liệu bí mật, chẳng hạn như tên hoặc địa chỉ IP của bạn, và không được sử dụng cho mục đích thương mại.

Nếu trong quá trình cài đặt bạn đã chọn gửi các báo cáo đó đến các máy chủ Bitdefender và bây giờ muốn dừng quá trình này:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Advanced**.
3. Tắt **Báo cáo sản phẩm** .

4.6. Thông báo khuyến mãi đặc biệt

Khi có khuyến mãi, sản phẩm Bitdefender sẽ thiết lập một cửa sổ thông báo. Điều này sẽ cho bạn cơ hội hưởng lợi từ giá rẻ và giúp thiết bị của bạn được bảo vệ thêm một thời gian dài hơn.

Để bật hoặc tắt khuyến mại đặc biệt và các thông báo:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **Chung**, bật hoặc tắt chuyển đổi tương ứng.

Các thông báo khuyến mãi được bật theo mặc định.

5. GIAO DIỆN BITDEFENDER

Bitdefender Antivirus Plus thích hợp với người mới làm quen sử dụng máy tính cũng như những người dùng yêu thích kỹ thuật. Giao diện đồ họa người sử dụng của sản phẩm được thiết kế phù hợp với từng kiểu người sử dụng khác nhau.

Để mở giao diện Bitdefender, trình hướng dẫn giới thiệu chi tiết về cách tương tác với sản phẩm và cách cấu hình được hiển thị ở phía trên bên trái. Chọn khung góc bên phải để tiếp tục được hướng dẫn, hoặc **Bỏ Qua** để đóng trình hướng dẫn.

Biểu tượng khay hệ thống Bitdefender có sẵn bất kỳ lúc nào, bất kể bạn có muốn mở cửa sổ chính hay không, chạy cập nhật sản phẩm hoặc xem thông tin về phiên bản đã cài đặt.

Cửa sổ chính cung cấp cho bạn thông tin về trạng thái bảo mật của bạn. Dựa trên mức sử dụng thiết bị và nhu cầu của bạn, Autopilot hiển thị ở đây các loại đề xuất khác nhau để giúp bạn cải thiện hiệu suất và bảo mật thiết bị của mình. Hơn nữa, bạn có thể thêm các hành động nhanh chóng mà bạn sử dụng nhiều nhất, để bạn có thể có chúng trong tầm tay bất cứ khi nào bạn cần.

Từ menu điều hướng ở bên trái, bạn có thể truy cập tài khoản Bitdefender, khu vực cài đặt, thông báo và các phần Bitdefender để biết cấu hình chi tiết và các tác vụ quản trị nâng cao. Ngoài ra, bạn có thể liên hệ với chúng tôi để được hỗ trợ trong trường hợp bạn có câu hỏi hoặc điều gì đó bất ngờ xuất hiện.

Nếu bạn muốn giữ theo dõi liên tục về các thông tin bảo mật cần thiết và truy cập nhanh chóng đến các thiết lập quan trọng, đưa Trình thao tác nhanh ra màn hình của bạn.

5.1. Biểu tượng tại khay hệ thống

Để quản lý toàn bộ sản phẩm nhanh hơn, bạn có thể sử dụng biểu tượng Bitdefender trong khay hệ thống.

Ghi chú

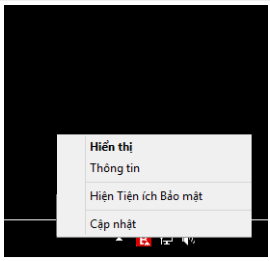
Các biểu tượng Bitdefendercó thể không được nhìn thấy ở tất cả mọi lúc. Để làm cho các biểu tượng xuất hiện vĩnh viễn:

- Trong **Windows 7, Windows 8 và Windows 8.1**:

1. Nhấp vào mũi tên ở góc dưới bên phải màn hình.
2. Nhấp **Tùy chỉnh...** để mở cửa sổ thông tin về biểu tượng.
3. Chọn tùy chọn **Hiển thị biểu tượng và thông báo** cho biểu tượng **Bitdefender agent**.

- Trong **Windows 10**:
  1. Nhấp chuột phải vào thanh tác vụ và chọn **Cài đặt thanh tác vụ** .
  2. Cuộn xuống và nhấp vào liên kết **Chọn biểu tượng nào xuất hiện trên thanh tác vụ** dưới**Khu vực thông báo**.
  3. Kích hoạt tính năng chuyển đổi để **Bitdefender Agent**.

Nếu bạn kích đúp vào biểu tượng này, Bitdefender sẽ mở ra. Ngoài ra, bằng cách kích chuột phải vào biểu tượng, một menu ngữ cảnh sẽ cho phép bạn nhanh chóng quản lý sản phẩm Bitdefender.



Biểu tượng tại khay

- **Hiển thị** - Mở cửa sổ chính của Bitdefender.
- **Giới thiệu** - mở ra một cửa sổ nơi bạn có thể xem thông tin về Bitdefender, nơi cần tìm trợ giúp trong trường hợp có điều gì đó không mong muốn xuất hiện, nơi để truy cập xem xét Thỏa thuận đăng ký, Chính sách bảo mật và thành phần của bên thứ ba.
- **Ẩn / hiển thị Trình thao tác nhanh** - kích hoạt / vô hiệu hóa Trình thao tác nhanh.
- **Cập nhật ngay** - tiến hành cập nhật ngay lập tức.
  Bạn có thể theo dõi trạng thái cập nhật trong bảng cập nhật của cửa sổ chính Bitdefender.

Biểu tượng Bitdefender trên khay hệ thống báo hiệu cho bạn khi tồn tại các vấn đề ảnh hưởng đến máy tính hoặc sản phẩm hoạt động như thế nào bằng cách hiển thị một biểu tượng đặc biệt, như sau:

Không có vấn đề nào ảnh hưởng tới sự bảo mật hệ thống
vấn đề quan trọng có ảnh hưởng đến sự an toàn của hệ thống của bạn. Chúng đòi hỏi sự chú ý của bạn ngay lập tức và phải được sửa càng sớm càng tốt.

Nếu Bitdefender không hoạt động, biểu tượng sản phẩm trên khay hệ thống sẽ có màu xám: . Điều này thường xảy ra khi các thuê bao hết hạn. Điều

này cũng có thể xảy ra khi dịch vụ Bitdefender không hoạt động hoặc khi các lỗi khác ảnh hưởng đến hoạt động bình thường của Bitdefender.

5.2. Chức năng điều hướng

Ở bên trái trên giao diện Bitdefender là menu điều hướng, cho phép bạn truy cập nhanh các tính năng và công cụ của Bitdefender bạn cần để xử lý sản phẩm của mình. Các tab có trong khu vực này là:

- **Trang tổng quan**. Từ đây, bạn có thể nhanh chóng khắc phục sự cố bảo mật, xem các đề xuất theo nhu cầu và mẫu sử dụng hệ thống của bạn và thực hiện các hành động nhanh.
- **Bảo vệ** . Từ đây, bạn có thể khởi động và cấu hình quét virus, truy cập cài đặt Tường lửa, bảo vệ tệp và ứng dụng khỏi các cuộc tấn công ransomware, khôi phục dữ liệu trong trường hợp nó được mã hóa bằng ransowmware và cấu hình bảo vệ trong khi lướt trên internet.
- **Riêng tư**. Từ đây, bạn có thể tạo trình quản lý mật khẩu cho tài khoản trực tuyến của mình, bảo vệ quyền truy cập vào webcam của bạn từ sự tò mò không mong muốn, thực hiện thanh toán trực tuyến trong môi trường an toàn và mở ứng dụng VPN.
- **Thông báo**. Từ đây, bạn có quyền truy cập vào các thông báo được tạo ra.
- **Tài khoản của tôi**. Từ đây, có thể truy cập Bitdefender của bạn để kiểm tra đăng ký của bạn và thực hiện các nhiệm vụ an ninh trên các thiết bị bạn quản lý. Thông tin chi tiết về tài khoản Bitdefender và sử dụng thuê bao cũng có sẵn.
- **Thiết lập**. Từ đây, bạn có quyền truy cập vào các thiết lập chung.
- **Hỗ trợ**. Từ đây, bất cứ khi nào bạn cần hỗ trợ trong việc giải quyết một tình huống với Bitdefender Antivirus Plus của bạn, bạn có thể liên hệ với các bộ phận hỗ trợ kỹ thuật Bitdefender.

5.3. Bảng Điều Khiển

Cửa sổ tổng quan cho phép bạn thực hiện các tác vụ thông thường, nhanh chóng xử lý các vấn đề an ninh, xem thông tin hoạt động của sản phẩm và truy cập từ cửa của sổ cài đặt sản phẩm.

Tất cả mọi việc chỉ cần vài cú nhấp chuột.

Các cửa sổ được tổ chức trong ba vùng chính:

Khu vực trạng thái bảo mật
: Đây là nơi bạn có thể kiểm tra trạng thái bảo mật của máy tính.

Tự động
: Đây là nơi bạn có thể kiểm tra các khuyến nghị Autopilot để đảm bảo chức năng phù hợp của hệ thống.

Hành động nhanh
: Đây là nơi bạn có thể chạy các nhiệm vụ khác nhau để giữ cho hệ thống của bạn được bảo vệ.

5.3.1. Khu vực trạng thái bảo mật

Bitdefender sử dụng một hệ thống theo dõi để phát hiện và thông báo cho bạn những vấn đề có thể ảnh hưởng đến sự an toàn của máy tính và dữ liệu của bạn. Các vấn đề được phát hiện có thể là các thiết lập bảo vệ quan trọng đã bị bỏ qua và các điều kiện khác có thể đại diện cho một nguy cơ bảo mật.

Bất cứ khi nào sự cố ảnh hưởng đến bảo mật máy tính của bạn, trạng thái xuất hiện ở phía trên của giao diện Bitdefender sẽ chuyển thành màu đỏ. Trạng thái được hiển thị cho biết bản chất của các sự cố ảnh hưởng đến hệ thống của bạn. Ngoài ra, biểu tượng khay hệ thống thay đổi thành và nếu bạn di chuyển con trỏ chuột qua biểu tượng, cửa sổ bật lên sẽ xác nhận sự tồn tại của các sự cố đang chờ xử lý.

Vì các vấn đề được phát hiện có thể ngăn cản Bitdefender bảo vệ bạn chống lại các mối đe dọa hoặc đại diện cho một nguy cơ bảo mật lớn, chúng tôi khuyên bạn nên chú ý và khắc phục chúng càng sớm càng tốt. Để khắc phục sự cố, hãy nhấp vào nút bên cạnh sự cố đã phát hiện.

5.3.2. Tự động

Để cung cấp cho bạn một hoạt động hiệu quả và tăng cường bảo vệ trong khi thực hiện các hoạt động khác nhau, Bitdefender Autopilot sẽ hoạt động như một cố vấn bảo mật cá nhân của bạn. Tùy thuộc vào hoạt động bạn thực hiện, bạn làm việc, thanh toán trực tuyến, xem phim hoặc chơi trò chơi Bitdefender Tự động lái sẽ đưa ra các đề xuất theo ngữ cảnh dựa trên nhu cầu sử dụng thiết bị của bạn. Các đề xuất được đề xuất cũng có thể liên quan đến các hành động mà bạn cần thực hiện để giữ cho sản phẩm của bạn hoạt động hết công suất.

Để bắt đầu sử dụng tính năng được đề xuất hoặc thực hiện các cải tiến cho sản phẩm của bạn, hãy nhấp vào nút tương ứng.

Tắt thông báo Autopilot

Để thu hút sự chú ý của bạn đến các khuyến nghị Autopilot, sản phẩm Bitdefender được thiết lập để thông báo cho bạn thông qua một cửa sổ bật lên.

Để tắt thông báo Autopilot:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **Chung**, hãy tắt **thông báo đề xuất**.

5.3.3. Hành động nhanh

Sử dụng các hành động nhanh chóng, bạn có thể nhanh chóng khởi chạy các tác vụ mà bạn cho là quan trọng để giữ cho hệ thống của bạn được bảo vệ và cải thiện cách bạn làm việc.

Theo mặc định, Bitdefender đi kèm với một số hành động nhanh có thể được thay thế bằng những hành động bạn biết bạn chủ yếu sử dụng. Để thay thế một hành động nhanh chóng:

1. Nhấp vào biểu tượng + ở góc trên bên phải của thẻ bạn muốn xóa.
2. Trỏ nhiệm vụ bạn muốn thêm vào giao diện chính, sau đó bấm **ADD** .

Các tác vụ bạn có thể thêm vào giao diện chính là:

- **Quét nhanh**. Chạy quét nhanh để kịp thời phát hiện các mối đe dọa có thể xuất hiện trên máy tính của bạn.
- **Quét hệ thống**. Chạy quét hệ thống để đảm bảo máy tính của bạn sạch các mối đe dọa.
- **Quét lỗ hổng bảo mật**. Quét các lỗ hổng để đảm bảo rằng tất cả các ứng dụng được cài đặt, cùng với các hệ điều hành, được cập nhật và hoạt động đúng.
- **Kiểm tra an toàn Wi-Fi**. Mở Trình cố vấn bảo mật Wi-Fi để kiểm tra xem mạng gia đình không dây bạn đang kết nối có an toàn hay không và nếu nó có lỗ hổng bảo mật.
- **Ví tiền**. Xem và quản lý ví của bạn.
- **Mở Safepay**. Mở Bitdefender Safepay ™ để bảo vệ dữ liệu nhạy cảm của bạn khi thực hiện các giao dịch trực tuyến.

- **Mở VPN**. Mở Bitdefender VPN để thêm một lớp bảo vệ bổ sung khi kết nối internet.
- **Hủy Dữ Liệu**. Khởi chạy công cụ Trình hủy tệp để xóa các dấu vết dữ liệu nhạy cảm khỏi máy tính của bạn.
-

Để bắt đầu bảo vệ các thiết bị bổ sung với Bitdefender:

1. Nhấp vào **Cài đặt trên một thiết bị khác**.

   Một cửa sổ mới xuất hiện trên màn hình của bạn.

2. Nhấp vào **CHIA SẺ LIÊN KẾT TẢI XUỐNG** .

3. Thực hiện theo các bước trên màn hình để cài đặt Bitdefender.

Tùy thuộc vào sự lựa chọn của bạn, các sản phẩm Bitdefender sau sẽ được cài đặt:

- Bitdefender Antivirus Plus trên các thiết bị chạy Windows.
- Bitdefender Antivirus dành cho Mac trên thiết bị có nền tảng macOS
- Bitdefender Mobile Security cho thiết bị Android.
- Bitdefender Bảo mật Di động trên thiết bị chạy iOS.

5.4. Phần Bitdefender

Sản phẩm Bitdefender đi kèm với hai thành phần được chia thành các tính năng hữu ích để bảo vệ trong khi bạn làm việc, lướt web, chơi trò chơi, hoặc thanh toán trực tuyến.

Bất cứ khi nào bạn muốn truy cập các tính năng cho một phần cụ thể hoặc để bắt đầu định cấu hình sản phẩm của mình, hãy truy cập các biểu tượng sau nằm trên menu điều hướng trên giao diện Bitdefender:

- Bảo vệ
- Riêng tư

5.4.1. Bảo vệ

Trong phần Bảo vệ, bạn có thể cấu hình các thiết lập bảo mật nâng cao, thiết lập các tính năng Tệp tin an toàn và Ngăn chặn đe dọa trực tuyến, kiểm tra và sửa các lỗ hổng hệ thống tiềm năng và đánh giá tính bảo mật của các mạng không dây mà bạn kết nối.

Các tính năng bạn có thể quản lý trong phần Bảo vệ:

ANTIVIRUS

Chống virus là nền tảng của an ninh của bạn. Bitdefender bảo vệ bạn theo thời gian thực và theo yêu cầu đối với tất cả các loại phần mềm độc hại như mã độc, trojan, gián điệp, quảng cáo...

Từ tính năng của Antivirus, bạn có thể dễ dàng truy cập các tác vụ quét sau đây:

- Quét nhanh
- Quét hệ thống
- Quản lý tác vụ quét
- Chế độ cứu hộ (Cứu hộ trong môi trường Windows 10)

Để biết thêm thông tin về các tác vụ quét và làm thế nào để cấu hình bảo vệ chống virus, vui lòng tham khảo "*Bảo vệ chống virus*" (p. 70).

Ngăn chặn mối đe dọa trên mạng

Ngăn chặn mối đe dọa trực tuyến giúp bạn được bảo vệ chống lại các tấn công lừa đảo, gian lận và rò rỉ dữ liệu cá nhân trong lúc truy cập Internet.

Để biết thêm thông tin về cách cấu hình Bitdefender để bảo vệ các hoạt động web của bạn, vui lòng tham khảo "*Ngăn chặn mối đe dọa trên mạng*" (p. 92).

Phòng chống tấn công nâng cao

Tính năng Phòng chống Nâng Cao bảo vệ hệ thống của bạn chống lại phần mềm độc hại như ransomware, spyware và trojans bằng cách phân tích hành vi của tất cả các ứng dụng đã cài đặt Các quy trình đáng ngờ được xác định và chặn khi cần thiết.

Để biết thêm thông tin giúp hệ thống của bạn tránh khỏi phần mềm độc hại,vui lòng tham khảo "*Phòng chống tấn công nâng cao*" (p. 90).

DỄ TỔN THƯƠNG

Mô đun Lỗ hổng bảo mật giúp bạn duy trì hệ điều hành và các ứng dụng mà bạn thường xuyên sử dụng cũng như xác định mạng không dây không an toàn mà bạn kết nối.

Nhấp vào **Quét lỗ hổng** trong tính năng Lỗ hổng bảo mật để bắt đầu xác định các cập nhật quan trọng của Windows, cập nhật ứng dụng, mật khẩu yếu thuộc tài khoản Windows và mạng không dây không an toàn.

Nhấn **An ninh Wifi** để xem danh sách các mạng không dây mà bạn kết nối, cùng với việc đánh giá của chúng tôi cho mỗi mạng và các hành động mà bạn có thể làm để giữ an toàn từ các nguy cơ mất an toàn.

Để biết thêm thông tin về cấu hình Phát hiện lỗ hổng bảo mật, vui lòng tham khảo "*Lỗ hổng*" (p. 95).

TẬP TIN AN TOÀN

Tính năng Tập Tin An Toàn đảm bảo rằng các tập tin cá nhân của bạn được bảo vệ khỏi các cuộc tấn công ransomware.

Để biết thêm thông tin về cách cấu hình các Tập Tin An Toàn để bảo vệ dữ liệu cá nhân của bạn khỏi các cuộc tấn công ransomware, hãy tham khảo "*Tập Tin An Toàn*" (p. 103).

Khắc phục ransomware

Tính năng Khắc phục Ransomware giúp bạn khôi phục các tập tin trong trường hợp chúng được mã hóa bởi ransomware.

Để biết thêm thông tin về cách khôi phục các tệp được mã hóa, hãy tham khảo "*Khắc phục Ransomware*" (p. 106).

5.4.2. Riêng tư

Trong phần Bảo mật, bạn có thể mở ứng dụng Bitdefender VPN, bảo vệ các giao dịch trực tuyến của bạn và giữ cho trải nghiệm duyệt web của bạn an toàn.

Các tính năng bạn có thể quản lý trong phần Bảo mật là:

VPN

VPN bảo vệ hoạt động trực tuyến của bạn và ẩn địa chỉ IP mỗi lần bạn kết nối với mạng không dây không an toàn khi ở các sân bay, trung tâm mua sắm, quán cà phê hoặc khách sạn. Thêm vào đó, bạn có thể truy cập nội dung thông thường bị hạn chế ở một số khu vực nhất định.

Để biết thêm thông tin về tính năng này, hãy tham khảo "*VPN*" (p. 119).

QUẢN LÝ MẬT KHẨU

Quản lý mật khẩu Bitdefender giúp bạn theo dõi các mật khẩu của mình, bảo vệ sự riêng tư của bạn và cung cấp một trải nghiệm duyệt web an toàn.

Để biết thêm thông tin về cấu hình tính năng Quản lý mật khẩu, vui lòng tham khảo "*Quản lý mật khẩu bảo vệ tài khoản của bạn*" (p. 109).

SAFEPAY

Trình duyệt Bitdefender Safepay™ giúp bạn thực hiện ngân hàng trực tuyến, mua sắm điện tử và giao dịch trực tuyến được đảm bảo riêng tư và an toàn.

Để biết thêm thông tin về Bitdefender Safepay™, vui lòng tham khảo "*Safepay bảo mật các giao dịch trực tuyến*" (p. 122).

BẢO VỆ DỮ LIỆU

Tính năng Bảo vệ Dữ liệu cho phép bạn xóa các tập tin vĩnh viễn. Nhấp vào **Hủy tập tin** trong Bảo vệ dữ liệu để bắt đầu một trình thủ thuật cho phép bạn loại bỏ hoàn toàn các tệp tin khỏi hệ thống của bạn.

Để biết thêm thông tin về cấu hình bảo vệ dữ liệu, vui lòng tham khảo "*Bảo vệ Dữ liệu*" (p. 127).

Chống theo dõi

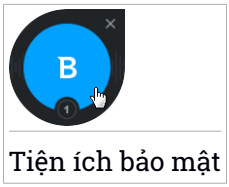
Tính năng Anti-tracker giúp bạn tránh theo dõi, để dữ liệu của bạn được giữ riêng tư trong khi bạn duyệt trực tuyến, đồng thời giảm thời gian tải trang web.

Để biết thêm thông tin về tính năng Chống theo dõi, hãy tham khảo "*Chống theo dõi*" (p. 116).

5.5. Tiện ích bảo mật

Trình tiện ích bảo mật là cách nhanh chóng, dễ dàng để theo dõi và kiểm soát Bitdefender Antivirus Plus. Thêm tiện ích nhỏ và không quấy rầy này vào màn hình làm việc của bạn cho phép bạn xem thông tin quan trọng và thực hiện các nhiệm vụ trọng tâm mọi lúc:

- mở cửa sổ chính của Bitdefender.
- giám sát hoạt động quét theo thời gian thực.
- theo dõi tình trạng an ninh của hệ thống và sửa chữa các vấn đề hiện tại.
- quan sát khi một bản cập nhật được tiến hành.
- xem các thông báo và truy cập vào các sự kiện mới nhất được báo cáo bởi Bitdefender.
- quét các tập tin hoặc thư mục bằng cách kéo và thả một hoặc nhiều đối tượng vào Trình tiện ích.



Tình trạng an ninh tổng thể của máy tính được hiển thị **tại trung tâm** của Trình tiện ích. Tình trạng được chỉ ra bởi màu sắc và hình dạng của các biểu tượng được hiển thị trong khu vực này.

Vấn đề nghiêm trọng ảnh hưởng đến an toàn của hệ thống.

Nó đòi hỏi sự chú ý ngay lập tức và phải được xử lý càng sớm càng tốt. Nhấp vào biểu tượng trạng thái để bắt đầu sửa chữa các vấn đề trong báo cáo.

Vấn đề quan trọng vừa phải ảnh hưởng đến an toàn của hệ thống. Bạn nên kiểm tra và sửa chữa chúng khi có thời gian. Nhấp vào biểu tượng trạng thái để bắt đầu sửa chữa các vấn đề trong báo cáo.

Hệ thống của bạn đã được bảo vệ.

Khi một nhiệm vụ quét theo yêu cầu đang diễn ra, biểu tượng hoạt hình này được hiển thị.

Khi vấn đề được báo cáo, nhấp vào biểu tượng trạng thái để khởi động Trình thuật sĩ xử lý vấn đề.

Phía dưới của tiện ích hiển thị số lượng các sự kiện mới (số sự kiện nổi bật được báo cáo bởi Bitdefender, nếu có). Nhấp vào số lượng sự kiện, ví dụ 1 cho một sự kiện mới, để mở cửa sổ Thông báo. Để biết thêm thông tin, hãy chuyển đến "*Thông báo*" (p. 14).

5.5.1. Quét các tập tin và thư mục

Bạn có thể sử dụng Trình tiện ích bảo mật để nhanh chóng quét các tập tin và thư mục. Kéo bất kỳ tập tin hoặc thư mục bạn muốn quét và thả chúng vào **Trình tiện ích bảo mật**.

Trình Thuật sĩ quét virus sẽ xuất hiện và hướng dẫn bạn quá trình quét. Các tùy chọn quét được cấu hình trước cho các kết quả phát hiện tốt nhất và không thể thay đổi. Nếu file bị nhiễm được phát hiện, Bitdefender sẽ cố gắng

làm sạch chúng (loại bỏ các mã phần mềm độc hại). Nếu việc làm sạch bị thất bại, trình thuật sĩ quét virus sẽ cho phép bạn chỉ định hành động được thực hiện trên các tập tin bị nhiễm virus.

5.5.2. Ẩn / hiện Trình tiện ích bảo mật

Khi bạn không muốn thấy Trình tiện ích bảo mật, nhấp .

Để khôi phục Trình tiện ích bảo mật, sử dụng một trong những phương pháp sau đây:

- Từ khay hệ thống:
  1. Nhấp chuột phải vào biểu tượng Bitdefender trong khay hệ thống .
  2. Nhấp **Hiển thị Trình tiện ích bảo mật** trong trình đơn ngữ cảnh xuất hiện.
- Từ giao diện Bitdefender:
  1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
  2. Trong cửa sổ **Chung**, hãy bật **Tiện ích bảo mật**.

Hiển thị thông tin bảo mật Bitdefender bị vô hiệu theo mặc định.

5.6. Thay đổi ngôn ngữ sản phẩm

Giao diện Bitdefender có sẵn nhiều ngôn ngữ và có thể được thay đổi bằng cách thực hiện theo các bước sau:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **Chung**, nhấp vào **Thay đổi ngôn ngữ**.
3. Chọn ngôn ngữ bạn muốn từ danh sách, sau đó nhấp vào **Lưu** .
4. Đợi một lát cho đến khi các cài đặt được áp dụng.

6. BITDEFENDER CENTRAL

Bitdefender Central là nền tảng nơi bạn có quyền truy cập vào các tính năng và dịch vụ trực tuyến của sản phẩm và từ xa có thể thực hiện các tác vụ quan trọng trên thiết bị Bitdefender được cài đặt trên đó. Bạn có thể đăng nhập vào tài khoản Bitdefender của mình từ bất kỳ máy tính nào được kết nối với internet bằng cách truy cập https://central.bitdefender.com hoặc trực tiếp từ ứng dụng Bitdefender Central trên thiết bị Android và iOS.

Để cài đặt ứng dụng Bitdefender Central trên thiết bị của bạn:

- **Trên Android** - tìm kiếm Bitdefender Central trên Google Play, sau đó tải xuống và cài đặt ứng dụng. Làm theo các bước cần thiết để hoàn tất cài đặt.
- **Trên iOS** - tìm kiếm Bitdefender Central trên App Store, sau đó tải xuống và cài đặt ứng dụng. Làm theo các bước cần thiết để hoàn tất cài đặt.

Khi bạn đã đăng nhập, bạn có thể bắt đầu thực hiện các thao tác sau:

- Tải xuống và cài đặt Bitdefender trên hệ điều hành Windows, macOS, iOS và Android. Các sản phẩm có sẵn để tải về được:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus cho hệ điều hành Mac
  - Bitdefender Mobile Security cho Android
  - Bitdefender Mobile Security dành cho iOS
- Quản lý và đổi mới Bitdefender đăng ký.
- Thêm thiết bị mới vào mạng của bạn và quản lý chúng bất cứ nơi nào bạn có thể.

6.1. Truy cập Bitdefender Central.

Có một số cách để truy cập Bitdefender Central:

- Từ giao diện chính Bitdefender:
  1. Nhấp vào **Tài khoản của tôi** trên menu điều hướng trên giao diện Bitdefender.
  2. Nhấp vào **Chuyển đến Bitdefender Trung tâm** .

3. Đăng nhập vào tài khoản Bitdefender của bạn bằng địa chỉ email và mật khẩu của bạn.

- Từ trình duyệt web của bạn:

  1. Mở trình duyệt web trên các thiết bị có truy cập Internet.
  2. Đi tới: https://central.bitdefender.com.
  3. Đăng nhập vào tài khoản Bitdefender của bạn bằng địa chỉ email và mật khẩu của bạn.

- Từ thiết bị chạy Android hoặc iOS của bạn:

  Mở ứng dụng Bitdefender Central bạn đã cài đặt.

Ghi chú
Trong tài liệu này, bạn được cung cấp các tùy chọn và hướng dẫn có sẵn trên nền tảng web.

6.2. Xác thực hai yếu tố

Phương thức Xác thực 2 yếu tố thêm một lớp bảo mật bổ sung vào tài khoản Bitdefender của bạn, bằng cách yêu cầu mã xác thực cùng với thông tin đăng nhập của bạn. Bằng cách này, bạn sẽ ngăn chặn việc chiếm đoạt tài khoản và tránh xa các loại các vấn đề về tấn công mạng, chẳng hạn như keylogger, brute-force hoặc cố gắng đăng nhập theo cách dự đoán mật khẩu

Đang bật xác thực 2 yếu tố

Bằng cách bật Xác thực 2 yếu tố, bạn sẽ làm cho tài khoản Bitdefender của mình an toàn hơn nhiều. Danh tính của bạn sẽ được xác minh mỗi khi bạn đăng nhập từ các thiết bị khác nhau, để cài đặt một trong những sản phẩm của Bitdefender, kiểm tra trạng thái đăng ký của bạn hoặc chạy các tác vụ từ xa trên thiết bị của bạn.

Để bật xác thực 2 yếu tố

1. Truy cập Bitdefender Central.
2. Nhấp vào biểu tượng ở phía trên bên phải của màn hình.
3. Nhấp vào **BitdefenderTài khoản** trong menu trượt.
4. Chọn thẻ **Mật khẩu và bảo mật** .
5. Nhấp vào **2- Xác thực nhân tố**.

6. Nhấp vào **BẮT ĐẦU**.

   Chọn một trong các phương thức sau:

   - **Ứng dụng Authenticator** - sử dụng ứng dụng xác thực để tạo mã mỗi lần bạn muốn đăng nhập vào tài khoản Bitdefender của mình.

     Nếu bạn muốn sử dụng một ứng dụng xác thực, nhưng bạn không chắc chắn nên chọn gì, một danh sách với các ứng dụng xác thực mà chúng tôi đề xuất có sẵn.

     a. Nhấp vào **SỬ DỤNG ỨNG DỤNG AUTHENTICATOR** để bắt đầu.

     b. Để đăng nhập trên thiết bị chạy Android hoặc iOS, hãy sử dụng thiết bị của bạn để quét mã QR.

        Để đăng nhập trên máy tính xách tay hoặc máy tính bàn, bạn có thể thêm mã được hiển thị theo cách thủ công.

        Nhấp **Tiếp tục**.

     c. Chèn mã được cung cấp bởi ứng dụng hoặc mã được hiển thị ở bước trước và sau đó nhấp vào **HOẠT ĐỘNG**.

   - **E-mail** - mỗi lần bạn đăng nhập vào tài khoản Bitdefender, mã xác minh sẽ được gửi đến hộp thư đến email của bạn. Kiểm tra tài khoản email của bạn và nhập mã được cung cấp.

     a. Nhấp vào **SỬ DỤNG EMAIL** để bắt đầu.

     b. Kiểm tra tài khoản email của bạn và nhập mã được cung cấp.

        Lưu ý rằng bạn có năm phút để kiểm tra tài khoản email của mình và nhập mã được tạo. Nếu hết thời gian, bạn sẽ phải tạo mã mới bằng cách làm theo các bước tương tự.

     c. Nhấp vào **HOẠT ĐỘNG**.

     d. Bạn được cung cấp mười mã kích hoạt. Bạn có thể sao chép, tải xuống hoặc in danh sách và sử dụng nó trong trường hợp bạn mất địa chỉ email hoặc sẽ không thể đăng nhập. Mỗi mã chỉ có thể được sử dụng một lần.

     e. Nhấp vào **XONG**.

Trong trường hợp bạn muốn ngừng sử dụng Xác thực 2 yếu tố:

1. Nhấp vào **TẮT 2- Yếu tố Xác Thực Tự Động** .

2. Kiểm tra ứng dụng hoặc tài khoản email của bạn và nhập mã bạn đã nhận được.

   Trong trường hợp bạn đã chọn nhận mã xác thực qua email, bạn có năm phút để kiểm tra tài khoản email của mình và nhập mã được tạo. Nếu hết thời gian, bạn sẽ phải tạo mã mới bằng cách làm theo các bước tương tự.

3. Xác nhận lựa chọn của bạn.

6.2.1. Thêm thiết bị đáng tin cậy

Để đảm bảo rằng chỉ bạn mới có thể truy cập tài khoản Bitdefender của mình, trước tiên chúng tôi có thể yêu cầu mã bảo mật. Nếu bạn muốn bỏ qua bước này mỗi khi bạn kết nối từ cùng một thiết bị, chúng tôi khuyên bạn nên chỉ định nó như một thiết bị đáng tin cậy.

Để thêm thiết bị làm thiết bị đáng tin cậy:

1. Truy cập Bitdefender Central.
2. Nhấp vào biểu tượng ở phía trên bên phải của màn hình.
3. Nhấp vào **BitdefenderTài khoản** trong menu trượt.
4. Chọn thẻ **Mật khẩu và bảo mật** .
5. Nhấp vào **Thiết bị đáng tin cậy**.
6. Danh sách các thiết bị được cài đặt Bitdefender. Nhấp vào thiết bị mong muốn.

Bạn có thể thêm bao nhiêu thiết bị tùy thích, miễn là chúng đã cài đặt Bitdefender và đăng ký của bạn hợp lệ.

6.3. Các Dịch vụ của tôi

Nền tảng Bitdefender Central cho bạn khả năng để dễ dàng quản lý các thuê bao cho tất cả các thiết bị của bạn.

6.3.1. Kiểm tra các thuê bao có sẵn

Để kiểm tra các thuê bao có sẵn của bạn:

1. Truy cập Bitdefender Central.
2. Chọn bảng**Các thuê bao**.

Ở đây bạn có thông tin về các thuê bao bạn sở hữu và số lượng thiết bị sử dụng.

Bạn có thể thêm một thiết bị mới với một thuê bao hoặc ra hạn mới bằng cách chọn một thẻ đăng ký.

Ghi chú
Bạn có thể có một hoặc nhiều đăng ký trong tài khoản của bạn miễn là chúng dành cho các nền tảng khác nhau (Windows, macOS, iOS hoặc Android)

6.3.2. Thêm một thiết bị mới

Nếu thuê bao của bạn bao gồm nhiều hơn một thiết bị, bạn có thể thêm một thiết bị mới và cài đặt sản phẩm Bitdefender Antivirus Plus trên đó , như sau:

1. Truy cập Bitdefender Central.
2. Trong của sổ **Các Thiết Bị Của Tôi** nhấp **Cài đặt bảo vệ**.
3. Chọn một trong hai tùy chọn có sẵn:
   - **Bảo vệ thiết bị này**

     Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.
   - **Bảo vệ các thiết bị khác**

     Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.

     Nhấn **GỬI LIÊN KẾT TẢI XUỐNG**. Nhập địa chỉ e-mail trong các trường tương ứng, và nhấn **GỬI EMAIL**. Lưu ý rằng liên kết tải xuống được tạo chỉ hợp lệ trong 24 giờ tiếp theo. Nếu liên kết hết hạn, bạn sẽ phải tạo một liên kết mới bằng cách làm theo các bước tương tự.

     Trên thiết bị bạn muốn cài đặt sản phẩm Bitdefender của bạn, hãy kiểm tra tài khoản email bạn đã nhập, sau đó nhấp vào nút tải xuống tương ứng.
4. Đợi tải về để hoàn thành, sau đó chạy trình cài đặt.

6.3.3. Gia hạn đăng ký

Nếu bạn đã tắt tự động gia hạn đăng ký Bitdefender của mình, bạn có thể gia hạn thủ công bằng cách thực hiện theo các bước sau:

1. Truy cập Bitdefender Central.

2. Chọn bảng**Các thuê bao**.
3. Chọn thẻ thuê bao mong muốn.
4. Nhấp **Ra hạn mới** để tiếp tục.

Một trang web mở ra trong trình duyệt web của bạn, nơi bạn có thể gia hạn Bitdefender thuê bao.

6.3.4. Kích hoạt đăng ký

Một thuê bao có thể được kích hoạt trong quá trình cài đặt bằng cách sử dụng tài khoản Bitdefender của bạn. Cùng với quá trình kích hoạt, tính hợp lệ của nó bắt đầu để đếm ngược.

Nếu bạn đã mua một mã kích hoạt từ một trong những đại lý của chúng tôi hoặc bạn đã nhận nó như là một món quà, sau đó bạn có thể thêm các tiện ích choác các bản quyền Bitdefender hiện có trong tài khoản, được cung cấp cho cùng một sản phẩm.

Kích hoạt đăng ký bằng một mã kích hoạt:

1. Truy cập Bitdefender Central.
2. Chọn bảng**Các thuê bao**.
3. Nhấp vào nút **MÃ KÍCH HOẠT**, sau đó nhập mã số trong trường tương ứng.
4. Nhấp vào **Kích Hoạt** để tiếp tục.

Các bản quyền hiện đang kích hoạt. Tới bảng điều khiển **Thiết bị của tôi** , và chọn **Cài đặt bảo vệ** để cài đặt sản phẩm trên một trong các thiết bị của bạn.

6.4. Các thiết bị của tôi

Ở khu vực **Các Thiết Bị Của Tôi** trong Bitdefender Central cung cấp cho bạn khả năng cài đặt, quản lý và có những hành động từ xa trên sản phẩm Bitdefender của bạn trên bất kỳ thiết bị được bật và kết nối với Internet. Các thẻ điện thoại hiển thị tên thiết bị, trạng thái bảo vệ và sẵn có còn lại trên thuê bao của bạn.

Để xem danh sách các thiết bị của bạn được sắp xếp theo trạng thái hoặc người dùng, hãy nhấp vào mũi tên thả xuống ở góc trên bên phải của màn hình.

Để dễ dàng xác định các thiết bị của bạn , bạn có thể tùy chỉnh tên thiết bị:

1. Truy cập Bitdefender Central.

2. Chọn bảng **Thiết bị**.
3. Nhấp vào thẻ thiết bị mong muốn và sau đó nhấp vào biểu tượng ⋮ ở góc trên bên phải của màn hình.
4. Chọn **Cài đặt** .
5. Nhập tên mới vào mục **Tên thiết bị** , sau đó nhấp vào **SAVE** .

Bạn có thể tạo ra và gán một chủ sở hữu để mỗi thiết bị của bạn được quản lý tốt hơn:

1. Truy cập Bitdefender Central.
2. Chọn bảng **Thiết bị**.
3. Nhấp vào thẻ thiết bị mong muốn và sau đó nhấp vào biểu tượng ⋮ ở góc trên bên phải của màn hình.
4. Chọn **hồ sơ** .
5. Nhấp vào **Thêm chủ nhân**, sau đó điền vào các trường tương ứng. Tùy chỉnh tiểu sử bằng cách thêm ảnh và chọn ngày sinh.
6. Nhấn vào **Thêm** để lưu hồ sơ.
7. Chọn chủ sở hữu mong muốn từ danh sách các **chủ sở hữu thiết bị** , sau đó nhấp vào **Gán**.

Để cập nhật từ xa Bitdefender trên một thiết bị Windows:

1. Truy cập Bitdefender Central.
2. Chọn bảng **Thiết bị**.
3. Nhấp vào thẻ thiết bị mong muốn và sau đó nhấp vào biểu tượng ⋮ ở góc trên bên phải của màn hình.
4. Chọn **Cập nhật** .

Đối với những hành động từ xa và các thông tin liên quan đến sản phẩm của bạn Bitdefender trên một thiết bị cụ thể, nhấp vào thẻ điện thoại mong muốn.

Khi bạn nhấp chuột vào một thẻ điện thoại, các tab sau:

- **Bảng Điều Khiển**. Trong cửa sổ này bạn có thể xem thông tin chi tiết về thiết bị đã chọn, kiểm tra trạng thái bảo vệ, trạng thái của Bitdefender VPN và số lượng các mối đe dọa đã bị chặn trong bảy ngày qua. Tình trạng bảo vệ có thể là màu xanh lá cây, khi không có sự cố nào ảnh hưởng đến thiết

bị của bạn, màu vàng khi thiết bị cần sự chú ý của bạn hoặc màu đỏ khi thiết bị gặp nguy hiểm. Khi có sự cố ảnh hưởng đến thiết bị của bạn, hãy nhấp vào mũi tên thả xuống trong khu vực trạng thái trên để tìm hiểu thêm chi tiết. Từ đây bạn có thể tự sửa chữa các vấn đề đang ảnh hưởng đến sự an toàn của các thiết bị của bạn.

- **Bảo vệ**. Từ cửa sổ này, bạn có thể từ xa chạy Quick Scan hoặc System Scan trên thiết bị của bạn. Nhấn vào nút **QUÉT** để bắt đầu quá trình. Bạn cũng có thể kiểm tra khi lần quét cuối cùng được thực hiện trên các thiết bị và báo cáo của lần quét mới nhất với các thông tin quan trọng nhất có sẵn.Để biết thêm thông tin về hai tiến trình quét, vui lòng tham khảo "*Chạy một Quét Hệ thống*" (p. 76) và "*Chạy một Quét nhanh*" (p. 76)..
- **Lỗ hổng bảo mật**. Để kiểm tra một thiết bị cho các lỗ hổng bảo mật như thiếu cập nhật Windows, các ứng dụng đã lỗi thời, hoặc mật khẩu yếu nhấn nút**QUÉT** trong các bảng lỗ hổng bảo mật. Lỗ hổng không thể được giải quyết từ xa. Trong trường hợp có bất kỳ lỗ hổng bảo mật được tìm thấy, bạn cần phải chạy quét mới trên thiết bị và sau đó có những hành động khuyến cáo. Nhấn**Thêm các chi tiết** để truy cập vào một báo cáo chi tiết về các vấn đề được tìm thấy. Để biết thêm chi tiết về tính năng này, hãy tham khảo "*Lỗ hổng*" (p. 95).

6.5. Thông báo

Để giúp bạn luôn được thông báo về những gì đang xảy ra trên các thiết bị được liên kết với tài khoản của bạn, biểu tượng ở trên tay Một khi bạn nhấp vào nó, bạn sẽ có một hình ảnh tổng thể bao gồm thông tin về hoạt động của các sản phẩm Bitdefender được cài đặt trên thiết bị của bạn.

7. GIỮ BITDEFENDER ĐƯỢC CẬP NHẬT

Các chương trình nguy hiểm mới được phát hiện và xác định hàng ngày. Đây là lý do tại sao việc cập nhật Bitdefender với cơ sở dữ liệu mới nhất là rất quan trọng.

Nếu bạn đang kết nối với Internet thông qua băng thông rộng hoặc DSL, Bitdefender sẽ tự thực hiện việc cập nhật. Theo mặc định, nó sẽ kiểm tra các bản cập nhật khi bạn bật máy tính và **từng giờ** sau đó. Nếu một bản cập nhật được phát hiện, nó sẽ tự động tải về và cài đặt trên máy tính của bạn.

Quá trình cập nhật được thực hiện ngay lập tức, có nghĩa là các tệp tin cần cập nhật được thay thế dần. Bằng cách này, quá trình cập nhật sẽ không ảnh hưởng đến hoạt động của sản phẩm và đồng thời, mọi lỗ hổng sẽ bị loại trừ.

Quan trọng
Để được bảo vệ chống lại các mối đe dọa mới nhất, cần bật chế độ tự động cập nhật.

Trong một số trường hợp đặc biệt, sự can thiệp của bạn là cần thiết để giữ cho Bitdefender được cập nhật:

- Nếu máy tính của bạn kết nối với Internet thông qua một máy chủ proxy, bạn phải thiết lập cấu hình proxy như mô tả trong "*Làm thế nào để cấu hình Bitdefender để sử dụng kết nối proxy Internet?*" (p. 63).
- Nếu bạn kết nối với Internet bằng cách quay số dial-up, bạn nên chủ động cập nhật Bitdefender thường xuyên. Để biết thêm thông tin, hãy chuyển đến "*Thực hiện một cập nhật*" (p. 38).

7.1. Kiểm tra xem Bitdefender đã cập nhật chưa

Để kiểm tra thời gian cập nhật cuối cùng của Bitdefender của bạn:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.
2. Trong Tab**Tất cả**, chọn thông báo về cập nhật mới nhất.

Bạn có thể biết khi tiến trình cập nhật bắt đầu và thông tin về nó (cập nhật thành công hay không, có yêu cầu khởi động lại máy tính để hoàn tất cài đặt không). Nếu được yêu cầu, khởi động lại hệ thống sớm nhất có thể.

7.2. Thực hiện một cập nhật

Để thực hiện cập nhật, kết nối Internet là cần thiết.

để bắt đầu cập nhật, chuột phải vào biểu tượng Bitdefender trong khay hệ thống và sau đó chọn **Cập nhật ngay**.

Tính năng Cập nhật sẽ kết nối với máy chủ cập nhật Bitdefender và nó sẽ kiểm tra các bản cập nhật. Nếu một bản cập nhật được phát hiện, bạn sẽ được yêu cầu xác nhận hoặc cập nhật sẽ được thực hiện tự động, tùy thuộc vào các thiết lập cập nhật.

Quan trọng
Có thể cần phải khởi động lại máy tính sau khi cập nhật thành công. Chúng tôi khuyên bạn nên làm như vậy càng sớm càng tốt.

Bạn cũng có thể thực hiện cập nhật từ xa trên thiết bị của bạn, miễn là chúng được bật và kết nối với internet.

Để cập nhật từ xa Bitdefender trên một thiết bị Windows:

1. Truy cập Bitdefender Central.
2. Chọn bảng **Thiết bị**.
3. Nhấp vào thẻ thiết bị mong muốn và sau đó nhấp vào biểu tượng ở góc trên bên phải của màn hình.
4. Chọn **Cập nhật** .

7.3. Bật hoặc tắt chế độ tự động cập nhật

Bật hoặc tắt chế độ tự động cập nhật

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Cập nhật**.
3. Bật hoặc tắt công tắc tương ứng.
4. Một cửa sổ cảnh báo xuất hiện. Bạn phải xác nhận lựa chọn của bạn bằng cách chọn từ trình đơn bạn muốn vô hiệu hóa chế độ tự động cập nhập trong bao lâu. Bạn có thể tắt cập nhật tự động trong 5, 15 hoặc 30 phút, trong một giờ hoặc cho đến khi hệ thống khởi động lại.

Cảnh báo
Đây là một lỗi bảo mật nguy hiểm. Chúng tôi khuyến cáo nên tắt Cập nhật tự động càng ngắn càng tốt. Nếu Bitdefender không được cập nhật thường xuyên, nó sẽ không thể bảo vệ bạn chống lại các mối đe dọa mới nhất.

7.4. Điều chỉnh các thiết lập cập nhật

Có thể cập nhật từ mạng nội bộ, thông qua Internet, trực tiếp hoặc qua proxy. Mặc định, Bitdefender sẽ kiểm tra việc cập nhập hàng giờ, qua Internet và cài đặt những cập nhập có sẵn mà không cần nhắc bạn.

Các thiết lập cập nhật mặc định thích hợp cho hầu hết người dùng và bạn thường không cần phải thay đổi chúng.

Để điều chỉnh các thiết lập cập nhật:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab**Cập nhật** và điều chỉnh các thiết lập theo sở thích của bạn.

Tần suất cập nhật

Bitdefender được cấu hình để kiểm tra các bản cập nhật mỗi giờ. Để thay đổi tần số cập nhật, kéo thanh trượt dọc theo độ để đặt thời gian mong muốn thời gian khi cập nhật nên thực hiện.

Quy tắc tiến hành cập nhật

Mỗi khi có bản cập nhật, Bitdefender sẽ tự động tải xuống và triển khai bản cập nhật mà không hiển thị thông báo. Tắt tùy chọn **Cập nhật thầm lặng** nếu bạn muốn được thông báo mỗi khi có bản cập nhật mới.

Một số cập nhật cần phải khởi động lại để hoàn tất cài đặt.

Theo mặc định, nếu cập nhật đòi hỏi khởi động lại, Bitdefender sẽ tiếp tục làm việc với các tập tin cũ cho đến khi người sử dụng tự nguyện khởi động lại máy tính. Điều này là để ngăn chặn quá trình cập nhật Bitdefender hưởng đến công việc của người dùng.

Nếu bạn muốn được nhắc khi bản cập nhật yêu cầu khởi động lại, hãy bật **Khởi động lại thông báo**.

7.5. Cập nhật liên tục

Để đảm bảo rằng bạn đang sử dụng phiên bản mới nhất, Bitdefender của bạn sẽ tự động kiểm tra các bản cập nhật sản phẩm. Các bản cập nhật này có thể mang lại các tính năng và cải tiến mới, khắc phục sự cố sản phẩm hoặc tự động nâng cấp lên phiên bản mới. Khi phiên bản Bitdefender mới xuất hiện thông qua bản cập nhật, các cài đặt tùy chỉnh sẽ được lưu và thủ tục bỏ cài đặt và cài đặt lại bị bỏ qua.

Các bản cập nhật này yêu cầu hệ thống khởi động lại để bắt đầu cài đặt các dữ liệu mới. Khi một cập nhật sản phẩm hoàn tất, một cửa sổ pop-up sẽ thông báo cho bạn để khởi động lại hệ thống. Nếu bạn bỏ lỡ thông báo này, bạn có thể nhấp vào **KHỞI ĐỘNG LẠI NGAY** trong cửa sổ Thông báo nơi cập nhật gần đây nhất được đề cập hoặc bằng tay Khởi động lại hệ thống.

Ghi chú

Bản cập nhật bao gồm các tính năng và cải tiến mới sẽ chỉ được phân phối cho người dùng đã cài đặt Bitdefender 2019.

LÀM THẾ NÀO

8. CÁC BƯỚC CÀI ĐẶT

8.1. Làm thế nào để cài đặt Bitdefender trên một máy tính thứ hai?

Nếu bản quyền bạn đã mua bao gồm nhiều hơn một máy tính, bạn có thể sử dụng tài khoản Bitdefender để kích hoạt một máy tính thứ hai.

Để cài đặt Bitdefender trên một máy tính thứ hai?

1. Nhấp vào **CÀI ĐẶT TRÊN THIẾT BỊ KHÁC** ở góc dưới bên phải của giao diện Bitdefender.

   Một cửa sổ mới xuất hiện trên màn hình của bạn.

2. Nhấp vào **CHIA SẺ LIÊN KẾT TẢI XUỐNG** .
3. Làm theo các hướng dẫn trên màn hình để cài đặt Bitdefender.

Các thiết bị mới mà bạn đã cài đặt sản phẩm Bitdefender sẽ xuất hiện trong bảng điều khiển Bitdefender Central.

8.2. Làm cách nào để cài đặt lại Bitdefender?

Tình huống điển hình khi bạn sẽ cần phải cài đặt lại Bitdefender gồm:

- bạn cài đặt lại hệ điều hành.
- Bạn muốn khắc phục các vấn đề có thể gây ra sự chậm trễ và sự cố.
- Sản phẩm Bitdefender của bạn không được chạy hoặc hoạt động bình thường.

Trong trường hợp của bạn, hãy làm theo các bước sau:

- Trong **Windows 7**:
  1. Nhấp **Bắt đầu** và tới **Tất cả các chương trình**.
  2. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  3. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
  4. Bạn sẽ cần phải khởi động lại máy tính để hoàn tất quá trình.
- Trong **Windows 8 and Windows 8.1**:

1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
4. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
5. Bạn sẽ cần phải khởi động lại máy tính để hoàn tất quá trình.

- Trong **Windows 10**:

1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
2. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **Ứng dụng và các đặc tính** .
3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
5. Nhấp vào **CÀI ĐẶT LẠI** .
6. Bạn sẽ cần phải khởi động lại máy tính để hoàn tất quá trình.

Ghi chú
Bằng cách làm theo thủ tục cài đặt lại này, các cài đặt tùy chỉnh được lưu và có sẵn trong sản phẩm được cài đặt mới. Các cài đặt khác có thể được chuyển trở lại cấu hình mặc định của chúng.

8.3. Tôi có thể tải về sản phẩm Bitdefender từ đâu?

Bạn có thể cài đặt Bitdefender từ đĩa cài đặt, hoặc bằng cách sử dụng các trình cài đặt bạn có thể tài về trên máy tính từ Bitdefender Central.

Ghi chú
Trước khi cài đặt, bạn nên loại bỏ những giải pháp chống virus khác đang có trên hệ thống. Khi bạn sử dụng nhiều hơn một giải pháp bảo mật trên cùng một máy tính, hệ thống sẽ trở nên không ổn định.

Để cài đặt Bitdefender từ Bitdefender Central:

1. Truy cập Bitdefender Central.
2. Trong của sổ **Các Thiết Bị Của Tôi** nhấp **Cài đặt bảo vệ**.
3. Chọn một trong hai tùy chọn có sẵn:

- **Bảo vệ thiết bị này**

  Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.

- **Bảo vệ các thiết bị khác**

  Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.

  Nhấn **GỬI LIÊN KẾT TẢI XUỐNG**. Nhập địa chỉ e-mail trong các trường tương ứng, và nhấn **GỬI EMAIL**. Lưu ý rằng liên kết tải xuống được tạo chỉ hợp lệ trong 24 giờ tiếp theo. Nếu liên kết hết hạn, bạn sẽ phải tạo một liên kết mới bằng cách làm theo các bước tương tự.

  Trên thiết bị bạn muốn cài đặt sản phẩm Bitdefender của bạn, hãy kiểm tra tài khoản email bạn đã nhập, sau đó nhấp vào nút tải xuống tương ứng.

4. Chạy sản phẩm Bitdefender bạn đã tải về.

8.4. Làm thế nào tôi có thể thay đổi ngôn ngữ của Bitdefender sản phẩm?

Giao diện Bitdefender có sẵn nhiều ngôn ngữ và có thể được thay đổi bằng cách thực hiện theo các bước sau:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **Chung**, nhấp vào **Thay đổi ngôn ngữ**.
3. Chọn ngôn ngữ bạn muốn từ danh sách, sau đó nhấp vào **Lưu** .
4. Đợi một lát cho đến khi các cài đặt được áp dụng.

8.5. Làm thế nào để sử dụng bản quyền Bitdefender sau khi nâng cấp Windows?

Tình huống này xuất hiện khi bạn nâng cấp hệ điều hành và bạn muốn tiếp tục sử dụng bản quyền Bitdefender của bạn.

Nếu đang sử dụng phiên bản bạn cũ Bitdefender, bạn có thể nâng cấp miễn phí lên Bitdefender mới nhất như sau:

- Từ phiên bản trước của Bitdefender Antivirus lên phiên bản mới nhất Bitdefender Antivirus.

- Từ phiên bản trước của Bitdefender Internet Security lên phiên bản mới nhất Bitdefender Internet Security.
- Từ phiên bản trước của Bitdefender Total Security lên phiên bản mới nhất Bitdefender Total Security.

Có hai trường hợp có thể xuất hiện:

- Bạn đã nâng cấp hệ điều hành bằng cách sử dụng Windows Update và bạn nhận thấy Bitdefender không còn làm việc.

  Trong trường hợp này, bạn cần phải cài đặt lại sản phẩm bằng cách làm theo các bước sau:

  - Trong **Windows 7**:

    1. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
    2. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
    3. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
    4. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

       Mở giao diện của sản phẩm Bitdefender đã cài đặt mới để có quyền truy cập vào các tính năng của nó.

  - Trong **Windows 8 and Windows 8.1**:

    1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
    2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
    3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
    4. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
    5. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

       Mở giao diện của sản phẩm Bitdefender đã cài đặt mới để có quyền truy cập vào các tính năng của nó.

  - Trong **Windows 10**:

    1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.

2. Nhấp vào biểu tượng **Hệ thống** trong khu vực Cài đặt, sau đó chọn **Ứng dụng**.
3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
5. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
6. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

   Mở giao diện của sản phẩm Bitdefender đã cài đặt mới để có quyền truy cập vào các tính năng của nó.

Ghi chú
Bằng cách làm theo thủ tục cài đặt lại này, các cài đặt tùy chỉnh được lưu và có sẵn trong sản phẩm được cài đặt mới. Các cài đặt khác có thể được chuyển trở lại cấu hình mặc định của chúng.

- Bạn đã thay đổi hệ thống của bạn và bạn muốn tiếp tục sử dụng Bitdefender. Vì vậy, bạn cần phải cài đặt lại sản phẩm sử dụng phiên bản mới nhất.

  Để giải quyết tình trạng này:

  1. Tải về các tập tin cài đặt:
     a. Truy cập Bitdefender Central.
     b. Trong của sổ **Các Thiết Bị Của Tôi** nhấp **Cài đặt bảo vệ**.
     c. Chọn một trong hai tùy chọn có sẵn:
        - **Bảo vệ thiết bị này**

          Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.
        - **Bảo vệ các thiết bị khác**

          Chọn tùy chọn này và sau đó chọn chủ sở hữu của thiết bị. Nếu thiết bị thuộc về người khác, nhấp vào nút tương ứng.

          Nhấn **GỬI LIÊN KẾT TẢI XUỐNG**. Nhập địa chỉ e-mail trong các trường tương ứng, và nhấn **GỬI EMAIL**. Lưu ý rằng liên kết tải xuống được tạo chỉ hợp lệ trong 24 giờ tiếp theo. Nếu liên kết hết hạn,

bạn sẽ phải tạo một liên kết mới bằng cách làm theo các bước tương tự.

Trên thiết bị bạn muốn cài đặt sản phẩm Bitdefender của bạn, hãy kiểm tra tài khoản email bạn đã nhập, sau đó nhấp vào nút tải xuống tương ứng.

2. Chạy sản phẩm Bitdefender bạn đã tải về.

Để biết thêm thông tin về quá trình cài đặt Bitdefender, vui lòng tham khảo "*Đang cài đặt sản phẩm Bitdefender*" (p. 4).

8.6. Làm cách nào để nâng cấp lên phiên bản Bitdefender mới nhất?

Từ bây giờ, bạn có thể nâng cấp lên phiên bản mới nhất mà không cần thực hiện quy trình gỡ cài đặt thủ công và cài đặt lại. Chính xác hơn, sản phẩm mới bao gồm các tính năng mới và các cải tiến sản phẩm được phân phối thông qua việc cập nhật sản phẩm và nếu bạn đã đăng ký sản phẩm Bitdefender đang hoạt động thì sản phẩm sẽ tự động được kích hoạt.

Nếu bạn đang sử dụng phiên bản 2019, bạn có thể nâng cấp lên phiên bản mới nhất bằng cách làm theo các bước sau:

1. Nhấp vào **KHỞI ĐỘNG LẠI NGAY** trong thông báo bạn nhận được với thông tin nâng cấp. Nếu bạn bỏ lỡ nó, hãy truy cập cửa sổ Thông báo, trỏ đến bản cập nhật gần đây nhất và sau đó nhấp vào nút **KHỞI ĐỘNG LẠI NGAY**. Đợi cho máy tính khởi động lại.

   Cửa sổ **Có gì mới** với thông tin về các tính năng được cải tiến mới.

2. Nhấp vào liên kết **Đọc thêm** để được chuyển hướng đến trang dành riêng của chúng tôi với nhiều chi tiết hơn và các bài viết hữu ích.

3. Đóng cửa sổ **Có gì mới** để truy cập vào giao diện của phiên bản cài đặt mới.

Người dùng muốn nâng cấp miễn phí từ Bitdefender 2016 hoặc phiên bản thấp hơn sang phiên bản Bitdefender mới nhất, phải gỡ bỏ phiên bản hiện tại từ Control Panel, và sau đó tải tập tin cài đặt mới nhất từ Bitdefender tại địa chỉ sau: https://www.bitdefender.com/taive/. Kích hoạt chỉ có thể thành công với đăng ký hợp lệ

9. BITDEFENDER CENTRAL

9.1. Làm cách nào để tôi đăng nhập vào tài khoản Bitdefender bằng tài khoản khác?

Bạn tạo một tài khoản Bitdefender mới và bạn muốn sử dụng nó từ bây giờ.

Để đăng nhập thành công bằng tài khoản Bitdefender khác:

1. Nhấp vào **Tài khoản của tôi** trên menu điều hướng trên giao diện Bitdefender.
2. Nhấp vào **Chuyển tài khoản** ở góc trên bên phải của màn hình để thay đổi tài khoản được liên kết với máy tính.
3. Nhập địa chỉ email vào trường tương ứng, sau đó nhấp vào **TIẾP THEO**.
4. Nhập mật khẩu của bạn và sau đó nhấp vào **ĐĂNG KÝ**.

Ghi chú
Các sản phẩm Bitdefender từ thiết bị của bạn sẽ tự động thay đổi theo thuê bao liên quan đến tài khoản mới Bitdefender.
Nếu không có thuê bao có sẵn liên quan đến Bitdefender tài khoản mới, hoặc bạn muốn chuyển nó từ các tài khoản trước đây, bạn có thể liên hệ với Bitdefendercần hỗ trợ như mô tả trong phần *"Muốn được giúp"* (p. 162) .

9.2. Làm thế nào để tắt tin nhắn trợ giúp Bitdefender Central?

Để giúp bạn hiểu từng tùy chọn gì trong Bitdefender Central là hữu ích, giúp thông báo được hiển thị trong bảng điều khiển.

Nếu bạn muốn dừng lại khi nhìn thấy các tin nhắn này:

1. Truy cập Bitdefender Central.
2. Nhấp vào biểu tượng ở phía trên bên phải của màn hình.
3. Nhấn **Tài khoản của tôi**.
4. Nhấp vào **Cài đặt** trong menu trượt.
5. Vô hiệu hoá các tùy chọn **Bật/tắt thông báo trợ giúp**.

9.3. Tôi quên mật khẩu tôi đặt cho tài khoản Bitdefender của tôi. Làm thế nào để thiết lập lại nó?

Có hai khả năng đặt mật khẩu mới cho tài khoản Bitdefender của bạn:

- Từ giao diện Bitdefender.
  1. Nhấp vào **Tài khoản của tôi** trên menu điều hướng trên giao diện Bitdefender.
  2. Nhấp vào **Chuyển tài khoản** ở góc trên bên phải của màn hình.

     Một cửa sổ mới xuất hiện.
  3. Nhấp vào **Quên mật khẩu?**.
  4. Nhập tài khoản email của bạn và nhấp vào **TIẾP THEO**.
  5. Kiểm tra tài khoản email của bạn, nhập mã bảo mật bạn đã nhận được và sau đó nhấp vào **TIẾP THEO**.

     Ngoài ra, bạn có thể nhấp vào **Thay đổi mật khẩu** trong email mà chúng tôi đã gửi cho bạn.
  6. Nhập mật khẩu mới bạn muốn đặt, sau đó nhập lại mật khẩu. Nhấp chuột vào **Lưu**.
- Từ trình duyệt web của bạn:
  1. Đi tới: https://central.bitdefender.com.
  2. Nhấp vào **ĐĂNG KÝ**.
  3. Nhập địa chỉ email của bạn, sau đó nhấp vào **TIẾP THEO**.
  4. Nhấp vào **Quên mật khẩu?**.
  5. Kiểm tra tài khoản e-mail của bạn và làm theo hướng dẫn để thiết lập một mật khẩu mới cho Bitdefender tài khoản của bạn.

Để truy cập tài khoản Bitdefender của bạn từ bây giờ, gõ địa chỉ e-mail và mật khẩu mới mà bạn vừa thiết lập.

9.4. Làm cách nào để quản lý các phiên đăng nhập được kết hợp với tài khoản Bitdefender của tôi?

Trong tài khoản Bitdefender của bạn, bạn có thể xem phiên đăng nhập không hoạt động và hoạt động mới nhất đang chạy trên các thiết bị được liên kết

với tài khoản của bạn. Hơn nữa, bạn có thể đăng xuất từ xa bằng cách làm theo các bước sau:

1. Truy cập Bitdefender Central.
2. Nhấp vào biểu tượng ở phía trên bên phải của màn hình.
3. Nhấn **Tài khoản của tôi**.
4. Nhấp vào **Quản lý phiên** trong menu trượt.
5. Trong phần **Các phiên đang hoạt động** , chọn tùy chọn **ĐĂNG XUẤT** bên cạnh thiết bị bạn muốn kết thúc phiên đăng nhập.

10. QUÉT VỚI BITDEFENDER

10.1. Làm thế nào để quét một tập tin hoặc một thư mục?

Cách dễ nhất để quét một tập tin hoặc thư mục là bấm chuột phải vào đối tượng bạn muốn quét, trỏ đến Bitdefender và chọn **Quét với Bitdefender** từ trình đơn.

Để hoàn thành quá trình quét, hãy làm theo Trình thuật sĩ Quét virus. Bitdefender sẽ tự động có những hành động được đề nghị về tập tin được phát hiện nghi vấn.

Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý.

Tình huống điển hình khi bạn sẽ sử dụng phương pháp quét này bao gồm:

- Bạn nghi ngờ một tập tin hoặc thư mục cụ thể bị nhiễm virus.
- Bất cứ khi nào bạn tải xuống các tệp từ internet mà bạn cho là có thể nguy hiểm.
- Quét một ổ chia sẻ qua mạng trước khi sao chép tập tin vào máy tính của bạn.

10.2. Làm thế nào để quét hệ thống?

Để thực hiện việc quét toàn bộ trên hệ thống:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Quét hệ thống** .
3. Thực hiện theo Thuật sĩ quét Hệ thống để hoàn tất quá trình quét. Bitdefender sẽ tự động có những hành động được đề nghị về tập tin được phát hiện nghi vấn.

   Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý. Để biết thêm thông tin, hãy chuyển đến "*Trình Thuật sĩ quét virus*" (p. 80).

10.3. Làm thế nào để lập lịch quét?

Bạn có thể thiết lập sản phẩm Bitdefender của bạn để bắt đầu quét các vị trí hệ thống quan trọng khi bạn đang không ở phía trước của máy tính.

Để lên lịch quét:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Quản lý quét** .
3. Nhấp vào bên cạnh phương thức quét mà bạn muốn lên lịch, Quét hệ thống hoặc Quét nhanh.

   Ngoài ra, bạn có thể tạo loại quét phù hợp với nhu cầu của mình bằng cách nhấp vào **Tạo mới tác vụ quét**.
4. Kích hoạt tùy chọn **Lịch quét**.

   Chọn một trong các tùy chọn tương ứng để thiết lập một lịch trình:

   - Tại lúc hệ thống khởi động
   - Hàng ngày
   - hàng tuần
   - hàng tháng

   Nếu bạn chọn Hàng ngày, Hàng tháng hoặc Hàng tuần, hãy kéo thanh trượt dọc theo tỷ lệ để đặt khoảng thời gian mong muốn khi quá trình quét theo lịch sẽ bắt đầu.

Nếu bạn chọn tạo quét tùy chỉnh mới, cửa sổ **Tác vụ Quét** sẽ xuất hiện. Từ đây bạn có thể chọn các vị trí bạn muốn được quét.

10.4. Làm thế nào để tạo ra một tác vụ quét tùy chỉnh?

Nếu bạn muốn quét các vùng cụ thể trên máy tính của bạn hoặc để cấu hình các tùy chọn quét, hãy cấu hình và chạy một nhiệm vụ quét tùy chỉnh.

Để tạo ra một tác vụ quét tùy chỉnh, tiến hành như sau:

1. Trong phần **CHỐNG VIRUS** , nhấp **Quản lý quét** .
2. Nhấp vào **Tạo tác vụ quét mới** .
3. Trong trường **Tên tác vụ** , nhập tên cho quá trình quét, sau đó chọn các vị trí bạn muốn quét và sau đó nhấp vào **TIẾP** .

4. Cấu hình các tùy chọn chung:
   - **Chỉ quét các ứng dụng** . Bạn có thể đặt Bitdefender để chỉ quét các ứng dụng đã truy cập.
   - **Tác vụ quét ưu tiên** . Bạn có thể chọn tác động mà quá trình quét nên có đối với hiệu suất hệ thống của bạn.
     - Tự động - Ưu tiên của quá trình quét sẽ phụ thuộc vào hoạt động của hệ thống. Để đảm bảo rằng quá trình quét sẽ không ảnh hưởng đến hoạt động của hệ thống, Bitdefender sẽ quyết định liệu quy trình quét nên được chạy với mức độ ưu tiên cao hay thấp.
     - Cao - Mức độ ưu tiên của quá trình quét sẽ cao. Bằng cách chọn tùy chọn này, bạn sẽ cho phép các chương trình khác chạy chậm hơn và giảm thời gian cần thiết để quá trình quét kết thúc.
     - Thấp - Mức độ ưu tiên của quá trình quét sẽ thấp. Bằng cách chọn tùy chọn này, bạn sẽ cho phép các chương trình khác chạy nhanh hơn và tăng thời gian cần thiết để quá trình quét kết thúc.
   - **Hành động quét bài** . Chọn hành động nào Bitdefender sẽ thực hiện trong trường hợp không tìm thấy mối đe dọa nào:
     - Hiện cửa sổ Tổng Quát
     - Tắt thiết bị
     - Đóng cửa sổ Quét
5. Nếu bạn muốn định cấu hình chi tiết các tùy chọn quét, hãy nhấp vào **Hiển thị tùy chọn nâng cao** .

   Nhấp vào **TIẾP THEO** .
6. Bật **Tác vụ quét định kỳ** , sau đó chọn thời điểm quét tùy chỉnh bạn đã tạo sẽ bắt đầu.
   - Tại lúc hệ thống khởi động
   - Hàng ngày
   - hàng tháng
   - hàng tuần

   Nếu bạn chọn Hàng ngày, Hàng tháng hoặc Hàng tuần, hãy kéo thanh trượt dọc theo tỷ lệ để đặt khoảng thời gian mong muốn khi quá trình quét theo lịch sẽ bắt đầu.

7. Nhấp vào **LƯU** để lưu cài đặt và đóng cửa sổ cấu hình.

   Tùy thuộc vào địa điểm được quét, quá trình quét có thể mất một thời gian. Nếu các mối đe dọa sẽ được tìm thấy trong quá trình quét, bạn sẽ được nhắc chọn các hành động được thực hiện trên các dữ liệu được phát hiện.

Nếu muốn, bạn có thể nhanh chóng chạy lại một tác vụ quét tùy chỉnh trước đó bằng cách nhấn vào mục tương ứng trong danh sách có sẵn.

10.5. Làm thế nào để loại trừ một thư mục khỏi bị quét?

Bitdefender cho phép loại trừ các tập tin, thư mục hoặc phần mở rộng tập tin cụ thể khỏi bị quét.

Ngoại lệ sẽ được sử dụng bởi người dùng có kiến thức máy tính nâng cao và chỉ trong các trường hợp sau:

- Bạn có một thư mục lớn trên hệ thống, nơi bạn lưu giữ các bộ phim và âm nhạc.
- Bạn có một kho lưu trữ lớn trên hệ thống, nơi bạn cất nhiều dữ liệu khác nhau.
- Bạn giữ một thư mục nơi bạn cài đặt các loại phần mềm và ứng dụng khác nhau cho mục đích thử nghiệm. Quét các thư mục có thể dẫn đến mất một số dữ liệu.

Để thêm thư mục vào Danh sách loại trừ.

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Nhấp vào tab **Ngoại lệ** .
4. Nhấp vào danh sách các tệp và thư mục **Danh sách tệp và thư mục ngoại trừ quét** , sau đó **Thêm** .
5. Nhấp vào **BROWSE** , chọn thư mục mà bạn muốn được loại trừ khỏi quá trình quét và sau đó chọn loại quét cần được loại trừ.
6. Nhấp **Thêm** để lưu lại các thay đổi và đóng cửa sổ lại.

10.6. Phải làm gì khi Bitdefender phát hiện một tập tin sạch mà coi như bị nhiễm virus?

Có khả năng Bitdefender nhầm lẫn đánh dấu một tập tin hợp pháp là mối đe dọa (một phát hiện sai). Để khắc phục lỗi này, thêm các tập tin vào Khu vực loại trừ của Bitdefender:

1. Tắt chế độ bảo vệ theo thời gian thực của Bitdefender:
   a. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
   b. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
   c. Trong cửa sổ **Shield** , tắt **Bitdefender Shield** .

   Một cửa sổ cảnh báo xuất hiện. Bạn phải xác nhận muốn tạm thời vô hiệu hóa chế độ bảo vệ theo thời gian thực trong bao lâu. Bạn có thể vô hiệu hóa tạm thời sự bảo vệ trong 5,15 hoặc phút, một giờ, vĩnh viễn hoặc cho đến khi nào hệ thống khởi động lại.
2. Hiển thị các đối tượng ẩn trong Windows. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để hiển thị các đối tượng ẩn trong Windows?*" (p. 65).
3. Khôi phục các tập tin từ Vùng cách ly:
   a. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
   b. Trong phần **CHỐNG VIRUS** , nhấp **Cách Ly** .
   c. Chọn tập tin và sau đó nhấn **Khôi phục**.
4. Thêm tệp vào danh sách Ngoại lệ. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để loại trừ một thư mục khỏi bị quét?*" (p. 54).
5. Bật chế độ bảo vệ theo thời gian thực của Bitdefender.
6. Liên hệ với đại diện hỗ trợ của chúng tôi để chúng tôi có thể xóa bỏ các cập nhật. Để hiểu cách thực hiện việc này, hãy tham khảo "*Muốn được giúp*" (p. 162).

10.7. Làm thế nào để kiểm tra Bitdefender đã phát hiện mã độc gì?

Mỗi lần quét được thực hiện, một hồ sơ quét được tạo ra và Bitdefender ghi lại các vấn đề được phát hiện.

Bản ghi (Scan log) chứa thông tin chi tiết về quá trình quét, như là lựa chọn quét, đích quét, hiểm họa tìm thấy và hành động dã thực hiện đối với hiểm họa.

Bạn có thể mở nhật ký quét trực tiếp từ trình hướng dẫn quét sau khi quá trình quét hoàn tất, bằng cách nhấn **Xem nhật ký**.

Để kiểm tra log quét hay các nhiễm trùng được phát hiện tại một thời gian sau:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.
2. Trong Tab**Tất cả**, chọn thông báo về quét mới nhất.

   Đây là nơi bạn có thể tìm thấy tất cả các sự kiện quét phần mềm độc hại, bao gồm các mối đe dọa được phát hiện bởi Quét khi truy cập, Quét chủ động bởi người sử dụng và những thay đổi trạng thái của quét tự động.
3. Trong danh sách các thông báo, bạn có thể kiểm tra những tác vụ quét đã được thực hiện gần đây. Nhấp vào một thông báo để xem chi tiết về nó.
4. Để mở một hồ sơ quét, nhấn **Xem nhật ký**.

11. BẢO VỆ THÔNG TIN CÁ NHÂN

11.1. Làm thế nào để đảm bảo an toàn giao dịch trực tuyến của tôi?

Để đảm bảo các hoạt động trực tuyến của bạn an toàn, bạn có thể sử dụng trình duyệt được cung cấp bởi Bitdefender để bảo vệ các giao dịch và các ứng dụng ngân hàng.

Bitdefender Safepay là một trình duyệt bảo mật được thiết kế để bảo vệ thông tin thẻ tín dụng, số tài khoản hoặc bất kỳ dữ liệu nhạy cảm khác mà bạn có thể nhập trong khi truy cập vào các giao dịch trực tuyến.

Để giữ cho hoạt động trực tuyến của bạn an toàn và riêng tư:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong ngăn **SAFEPAY**, nhấp vào **Mở Safepay**.
3. Nhấp nút để mở **Bàn phím ảo**.

   Sử dụng **Bàn phím ảo** khi gõ thông tin nhạy cảm như mật khẩu của bạn.

11.2. Làm thế nào để loại bỏ một tập tin vĩnh viễn với Bitdefender?

Nếu bạn muốn xóa một tập tin vĩnh viễn khỏi hệ thống, bạn cần phải xóa các dữ liệu vật lý từ đĩa cứng của bạn.

Chức năng Hủy tệp tin của Bitdefender sẽ giúp bạn nhanh chóng xóa sạch tập tin hoặc thư mục từ máy tính của bạn bằng cách sử dụng trình đơn ngữ cảnh Windows bằng cách làm theo các bước sau:

1. Bấm chuột phải vào tập tin hoặc thư mục mà bạn muốn xóa vĩnh viễn, chỉ vào Bitdefender và chọn **Hủy tập tin**.
2. Nhấp vào **XÓA VĨNH VIỄN** và sau đó xác nhận rằng bạn muốn tiếp tục quá trình.

   Đợi đến khi Bitdefender hoàn tất hủy các tập tin.
3. Các kết quả được hiển thị. Nhấp **HOÀN THÀNH** để thoát khỏi tiện ích.

11.3. Làm cách nào tôi có thể khôi phục tệp được mã hóa theo cách thủ công khi quá trình khôi phục không thành công?

Trong trường hợp các tệp được mã hóa không thể được khôi phục tự động, bạn có thể khôi phục chúng theo cách thủ công bằng cách làm theo các bước sau:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.
2. Trong tab **Tất cả**, chọn thông báo liên quan đến hành vi ransomware mới nhất được phát hiện và sau đó nhấp vào **Tệp được mã hóa**.
3. Danh sách với các tập tin được mã hóa được hiển thị.

   Nhấp vào **FILOVER FILES** để tiếp tục.
4. Trong trường hợp toàn bộ hoặc một phần của quá trình khôi phục không thành công, bạn phải chọn vị trí lưu các tệp đã giải mã. Nhấp vào **RESTORE LOCATION** , sau đó chọn vị trí trên PC của bạn.
5. Một cửa sổ xác nhận xuất hiện.

   Nhấp vào **HOÀN THÀNH** để kết thúc quá trình khôi phục.

Các tệp có các phần mở rộng sau có thể được khôi phục trong trường hợp chúng được mã hóa:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

12. THÔNG TIN TRỢ GIÚP

12.1. Làm cách nào để kiểm tra giải pháp bảo mật?

Để đảm bảo Bitdefender là hoạt động tốt, chúng tôi khuyên bạn sử dụng kiểm tra Eicar.

Bài thử Eicar cho phép bạn kiểm tra khả năng chống virus của sản phẩm bằng việc sử dụng một tập tin an toàn được phát triển cho mục đích kiểm thử.

Để kiểm tra giải pháp bảo mật của bạn:

1. Tải về thử nghiệm từ trang web chính thức của tổ chức EICAR http://www.eicar.org/.
2. Nhấp vào **Tập tin kiểm tra chương trình Chống mã độc**.
3. Nhấp **Tải về** từ bên trái trình đơn.
4. Từ **Khu vực Tải về sử dụng giao thức http** nhấp vào tập tin thử nghiệm **eicar.com**.
5. Bạn sẽ được thông báo trang web mà bạn đang truy cập chứa tập tin kiểm tra EICAR (không phải là một mã độc).

   Nếu bạn nhấp vào **Tôi hiểu những rủi ro, hãy đưa tôi đi tiếp**, việc tải xuống tập tin thử nghiệm sẽ bắt đầu và một cửa sổ Bitdefender thông báo tới bạn rằng một virus đã được phát hiện.

   Nhấp **Thêm chi tiết** để tìm hiểu thêm thông tin về hành động này.

Nếu bạn không nhận được bất kỳ cảnh báo nào từ Bitdefender, chúng tôi đề nghị bạn liên hệ với hỗ trợ Bitdefender như mô tả trong phần *"Muốn được giúp"* (p. 162).

12.2. Làm thế nào để gỡ bỏ Bitdefender?

Nếu bạn muốn xóa Bitdefender Antivirus Plus của bạn:

- Trong **Windows 7**:
  1. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
  2. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  3. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.

4. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

- Trong **Windows 8 and Windows 8.1**:

1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
4. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
5. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

- Trong **Windows 10**:

1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
2. Nhấp vào biểu tượng **Hệ thống** trong khu vực Cài đặt, sau đó chọn **Ứng dụng**.
3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
5. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
6. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

Ghi chú
Thủ tục cài đặt lại này sẽ xóa vĩnh viễn các cài đặt tùy chỉnh.

12.3. Tôi làm cách nào để xóa Bitdefender VPN?

Thủ tục xóa VPN Bitdefender tương tự như thủ tục mà bạn sử dụng để xóa các chương trình khác khỏi máy tính của bạn:

- Trong **Windows 7**:

1. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
2. Tìm **Bitdefender VPN** và chọn **Gỡ cài đặt**.

   Đợi đến khi quá trình gỡ bỏ hoàn tất.

- Trong **Windows 8 and Windows 8.1**:
  1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
  2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
  3. Tìm **Bitdefender VPN** và chọn **Gỡ cài đặt**.

     Đợi đến khi quá trình gỡ bỏ hoàn tất.
- Trong **Windows 10**:
  1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
  2. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **cài đặt các ứng dụng** .
  3. Tìm **Bitdefender VPN** và chọn **Gỡ cài đặt**.
  4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.

     Đợi đến khi quá trình gỡ bỏ hoàn tất.

12.4. Làm cách nào để xóa tiện ích mở rộng Bitdefender Chống theo dõi

Tùy thuộc vào trình duyệt web bạn đang sử dụng, hãy làm theo các bước sau để gỡ cài đặt tiện ích mở rộng Trình theo dõi Bitdefender:

- Internet Explorer
  1. Nhấp vào bên cạnh thanh tìm kiếm, sau đó chọn Quản lý tiện ích bổ sung.

     Một danh sách với các phần mở rộng được cài đặt xuất hiện.
  2. Nhấp vào Bitdefender Chống theo dõi.
  3. Nhấp vào **Tắt** ở dưới cùng bên phải.
- Google Chrome
  1. Nhấp vào bên cạnh thanh tìm kiếm.
  2. Chọn **Công cụ khác** và sau đó **Tiện ích** .

     Một danh sách với các phần mở rộng được cài đặt xuất hiện.

3. Nhấp vào **Xóa bỏ** trong thẻ Bitdefender Chống theo dõi
4. Nhấp vào **Xóa bỏ** trong cửa sổ hiện lên.

- Mozilla Firefox

1. Nhấp vào ☰ bên cạnh thanh tìm kiếm.
2. Chọn **Tiện ích** và sau đó **Tiện ích mở rộng** .

   Một danh sách với các phần mở rộng được cài đặt xuất hiện.
3. Nhấp vào **Xóa bỏ** trong thẻ Bitdefender Chống theo dõi

12.5. Làm thế nào để tự động tắt máy tính sau khi quá trình quét kết thúc?

Bitdefender có khả năng quét đa tác vụ mà bạn có thể sử dụng để đảm bảo hệ thống của bạn không bị nhiễm phần mềm độc hại. Quét toàn bộ máy tính có thể mất thời gian lâu hơn để hoàn thành tùy thuộc vào cấu hình phần cứng và phần mềm hệ thống.

Vì lý do này, Bitdefender cho phép bạn cấu hình để tắt hệ thống ngay sau khi quá trình quét kết thúc.

Hãy xem xét ví dụ này: bạn đã hoàn thành công việc của bạn với máy tính và bạn muốn đi ngủ. Bạn muốn kiểm tra toàn bộ hệ thống của bạn bởi Bitdefender.

Để tắt máy tính khi Quét nhanh hoặc Quét hệ thống kết thúc:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Quản lý quét** .
3. Nhấp vào ✎ bên cạnh Quét nhanh hoặc Quét hệ thống.
4. Từ danh sách **Hành động quét cổng**, chọn **Tắt thiết bị** , sau đó nhấp vào **TIẾP THEO** .
5. Bật **Tác vụ quét theo lịch** , sau đó chọn thời điểm bắt đầu tác vụ.

   Nếu bạn chọn Hàng ngày, Hàng tháng hoặc Hàng tuần, hãy kéo thanh trượt dọc theo tỷ lệ để đặt khoảng thời gian mong muốn khi quá trình quét theo lịch sẽ bắt đầu.

Để tắt máy tính khi quá trình quét tùy chỉnh kết thúc:

1. Nhấp vào bên cạnh bản quét tùy chỉnh bạn đã tạo.
2. Trong cửa sổ **Tác vụ quét** , nhấp vào **TIẾP THEO** .
3. Từ danh sách **Hành động quét cổng**, chọn **Tắt thiết bị** .
4. Nhấp vào **TIẾP THEO** , sau đó nhấp vào **LƯU** .

Nếu không có mối đe dọa nào được tìm thấy, máy tính sẽ tắt.

Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý. Để biết thêm thông tin, hãy chuyển đến "*Trình Thuật sĩ quét virus*" (p. 80).

12.6. Làm thế nào để cấu hình Bitdefender để sử dụng kết nối proxy Internet?

Nếu máy tính của bạn kết nối với Internet thông qua một máy chủ proxy, bạn phải cấu hình Bitdefender với các thiết lập proxy. Thông thường, Bitdefender tự động phát hiện và nhập khẩu các thiết lập proxy từ hệ thống của bạn.

> **!** **Quan trọng**
> Kết nối Internet tại nhà thường không sử dụng máy chủ proxy. Như một quy luật, kiểm tra và cấu hình các thiết lập kết nối proxy Bitdefender của bạn khi chương trình cập nhật không làm việc. Nếu Bitdefender được cập nhật, có nghĩa nó đã được cấu hình để kết nối Internet.

Để quản lý các thiết lập proxy:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Advanced**.
3. Bật **máy chủ proxy** .
4. Nhấp vào **Thay đổi proxy** .
5. Có hai tùy chọn để thiết lập các cài đặt proxy:
   - **Nhập khẩu thiết lập proxy từ trình duyệt mặc định** - Thiết lập proxy của người dùng hiện tại theo trình duyệt mặc định. Nếu máy chủ proxy yêu cầu tên người dùng và mật khẩu, bạn bắt buộc phải cung cấp chúng trong trường tương ứng.

> **Ghi chú**
> Bitdefender có thể đem các thiết lập proxy từ các trình duyệt phổ biến nhất, bao gồm các phiên bản mới nhất của Microsoft Edge, Internet Explorer, Mozilla Firefox và Google Chrome.

- **Thiết lập proxy tùy chỉnh** - Thiết lập proxy mà bạn có thể tự cấu hình. Các thiết lập sau cần được chọn:
  - **Địa chỉ** - gõ IP của máy chủ proxy.
  - **Cổng** - Gõ số hiệu cổng mà Bitdefender dùng để nối với máy chủ proxy.
  - **Người dùng** - hãy vào tên người sử dụng mà proxy nhận biết được.
  - **Mật khẩu** - đưa vào mật khẩu của người dùng.

6. Nhấp **OK** để lưu lại các thay đổi và đóng cửa sổ lại.

Bitdefender sẽ sử dụng các cài đặt proxy có sẵn cho đến khi nó có thể kết nối với Internet.

12.7. Tôi đang sử dụng phiên bản Windows 32 bit hay 64 bit?

Để tìm ra nếu bạn có một hệ điều hành 32bit hoặc 64 bit:

- Trong **Windows 7**:
  1. Nhấp **Bắt đầu**.
  2. Tìm đến **Máy tính** trên trình đơn **Bắt đầu**.
  3. Kích chuột phải vào **Máy tính** và chọn **Thuộc tính**.
  4. Nhìn vào bên dưới **Hệ thống** để kiểm tra các thông tin về hệ thống của bạn.
- Trong **Windows 8**:
  1. Từ màn hình Bắt đầu của Windows, xác định vị trí **Máy tính** (ví dụ, bạn có thể gõ "máy tính" trực tiếp vào màn hình Bắt đầu) và sau đó kích chuột phải vào biểu tượng của nó .

     Trong **Windows 8.1** , xác định vị trí **PC này** .
  2. Chọn **Thuộc tính** từ trình đơn phía dưới.
  3. Tìm trong khu vực hệ thống để xem loại hệ thống của bạn.
- Trong **Windows 10**:

1. Loại "Hệ thống" trong ô tìm kiếm trên thanh tác vụ và nhấp vào biểu tượng của nó.
2. Tìm trong vùng hệ thống để tìm kiếm thông tin về loại hình hệ thống.

12.8. Làm thế nào để hiển thị các đối tượng ẩn trong Windows?

Bước này rất hữu ích trong những trường hợp mà bạn đang đối phó với tình huống lây nhiễm phần mềm độc hại mà bạn cần phải tìm và loại bỏ các file bị nhiễm có thể được ẩn đi.

Thực hiện theo các bước sau để hiển thị các đối tượng ẩn trong Windows:

1. Nhấp **Bắt đầu**, đi đến **Bảng điều khiển**.

   Trong **Windows 8 và Windows 8. 1**: Từ màn hình Start của Windows, xác định vị trí **Control Panel** (ví dụ, bạn có thể bắt đầu gõ "Control Panel" trực tiếp trên màn hình Start) và sau đó nhấp chuột vào biểu tượng của nó.
2. Chọn **Lựa chọn thư mục**.
3. Tới **Xem**.
4. Chọn **Hiển thị tập tin và thư mục ẩn** .
5. Bỏ **Ẩn đuôi mở rộng của các tập tin**.
6. Bỏ **Ẩn các tập tin hệ thống**.
7. Nhấn **Apply**, sau đó bấm **OK**.

Trong **Windows 10**:

1. Loại "Show hidden files and folders" trong hộp tìm kiếm trên thanh tác vụ và nhấp vào biểu tượng của nó.
2. Chọn **Hiển thị các tập tin ẩn,thư mục,và ổ đĩa**.
3. Bỏ **Ẩn đuôi mở rộng của các tập tin**.
4. Bỏ **Ẩn các tập tin hệ thống**.
5. Nhấn **Apply**, sau đó bấm **OK**.

12.9. Làm thế nào để gỡ bỏ các giải pháp bảo mật khác?

Lý do chính để sử dụng một giải pháp bảo mật là để bảo vệ an toàn cho dữ liệu của bạn. Nhưng điều gì xảy ra khi bạn có nhiều hơn một sản phẩm bảo mật trên cùng một hệ thống?

Khi bạn sử dụng nhiều hơn một giải pháp bảo mật trên cùng một máy tính, hệ thống sẽ trở nên không ổn định. Cài đặt Bitdefender Antivirus Plus tự động phát hiện các chương trình bảo mật khác và cho bạn tùy chọn gỡ bỏ chúng.

Nếu bạn không loại bỏ các giải pháp bảo mật khác vào lúc bắt đầu cài đặt

- Trong **Windows 7**:
  1. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
  2. Chờ một vài phút cho đến khi danh sách các phần mềm cài đặt được hiển thị.
  3. Tìm tên của chương trình mà bạn muốn loại bỏ và chọn **Gỡ cài đặt**.
  4. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
- Trong **Windows 8 and Windows 8.1**:
  1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
  2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
  3. Chờ một vài phút cho đến khi danh sách các phần mềm cài đặt được hiển thị.
  4. Tìm tên của chương trình mà bạn muốn loại bỏ và chọn **Gỡ cài đặt**.
  5. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
- Trong **Windows 10**:
  1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
  2. Nhấp vào biểu tượng **Hệ thống** trong khu vực Cài đặt, sau đó chọn **Ứng dụng**.
  3. Tìm tên của chương trình mà bạn muốn loại bỏ và chọn **Gỡ cài đặt**.

4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
5. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

Nếu bạn không thể gỡ bỏ các giải pháp bảo mật khác khỏi hệ thống, hãy tìm công cụ gỡ bỏ cài đặt từ trang web của nhà cung cấp hoặc liên hệ trực tiếp để được hướng dẫn gỡ bỏ cài đặt.

12.10. Làm thế nào để khởi động vào chế độ An toàn?

Chế độ An toàn là một chế độ hoạt động chẩn đoán, sử dụng chủ yếu để khắc phục sự cố các vấn đề ảnh hưởng đến hoạt động bình thường của Windows. Những vấn đề như vậy bao gồm từ các trình điều khiển xung đột đến các mối đe dọa ngăn Windows khởi động bình thường. Trong chế độ An toàn, chỉ có một vài ứng dụng làm việc và Windows chỉ tải các trình điều khiển cơ bản tối thiểu của hệ điều hành. Đây là lý do tại sao hầu hết các virus không thể hoạt động khi sử dụng Windows ở chế độ An toàn và chúng có thể dễ dàng bị loại bỏ.

Để khởi động Windows vào chế độ An toàn:

- Trong **Windows 7**:
  1. Khởi động lại máy tính.
  2. Nhấn **F8** vài lần trước khi Windows khởi động để truy cập trình đơn khởi động.
  3. Chọn **Safe Mode** trong trình đơn khởi động hoặc **Safe Mode with Networking** nếu bạn muốn truy cập Internet.
  4. Nhấn **Enter** và chờ đợi trong khi Windows được nạp trong chế độ An toàn.
  5. Quá trình này kết thúc với một thông báo xác nhận. Nhấp **OK** để xác nhận.
  6. Để khởi động Windows bình thường, chỉ cần khởi động lại hệ thống.
- Trong **Windows 8, Windows 8.1 và Windows 10**:
  1. Bắt đầu **Cấu hình hệ thống** trong các cửa sổ đồng thời nhấn phím **Windows + R** trên bàn phím của bạn.
  2. Viết **msconfig** trong hộp thoại**Open**, sau đó bấm **OK**.
  3. Chọn trình đơn **Boot**

4. Trong khu vực **Tùy chọn Boot**, chọn **Safe boot**
5. Nhấn**Mạng**, và sau đó **OK**.
6. Nhấn **OK**trong cửa sổ **System Configuration** thông báo cho bạn việc hệ thống cần phải được khởi động lại để có thể thực hiện các thay đổi mà bạn thiết lập .

   Hệ thống của bạn khởi động lại trong chế độ Safe Mode with Mạng.

Để khởi động lại trong chế độ bình thường, chuyển đổi lại các thiết lập bằng cách bắt đầu lại **Hoạt động hệ thống** và xóa thiết lập **Safe boot**. Nhấn **OK**, và sau đó**Khởi động lại**. Chờ cho các thiết lập mới được áp dụng.

QUẢN LÝ AN NINH CỦA BẠN

13. BẢO VỆ CHỐNG VIRUS

Bitdefender bảo vệ máy tính của bạn khỏi tất cả các loại mã độc (virus, Trojan, spyware, rootkit và nhiều hơn thế.) Các phần bảo vệ do Bitdefender cung cấp được chia ra thành hai loại:

- Quét lúc truy cập - ngăn chặn các mối đe dọa phần mềm độc hại mới xâm nhập vào hệ thống của bạn. Ví dụ Bitdefender sẽ quét một tài liệu Word ngay khi bạn mở nó, và một e-mail khi bạn nhận nó.

  Quét lúc truy cập đảm bảo bạn được bảo vệ theo thời gian thực chống lại phần mềm độc hại, đây là thành phần thiết yếu của bất kỳ chương trình bảo vệ máy tính nào.

  > **Quan trọng**
  > Để ngăn chặn virus lây nhiễm vào máy tính của bạn, hãy luôn kích hoạt **Quét lúc truy cập**.

- Quét theo yêu cầu - cho phép phát hiện và loại bỏ các loại mã độc thường trú từ trước trong hệ thống của bạn. Đây là kiểu quét truyền thống do người sử dụng khởi xướng - bạn chọn ổ đĩa, thư mục hoặc tập tin nào mà Bitdefender phải quét và Bitdefender quét chúng theo yêu cầu.

Bitdefender tự động quét mọi thiết bị lưu trữ di động được gắn vào máy tính để chắc chắn rằng nó có thể được truy cập một cách an toàn. Để biết thêm thông tin, hãy chuyển đến "*Tự động quét các phương tiện tháo lắp*" (p. 84).

Người dùng cao cấp có thể cấu hình loại trừ quét nếu họ không muốn những tập tin cụ thể hoặc tập tin theo phân loại được quét. Để biết thêm thông tin, hãy chuyển đến "*Cấu hình loại trừ quét*" (p. 86).

Khi phát hiện một virus hoặc phần mềm độc hại, Bitdefender sẽ tự động cố gắng loại bỏ các mã phần mềm độc hại khỏi các tập tin bị nhiễm và tái tạo lại tập tin gốc. Hoạt động này được gọi là khử nhiễm. Các tập tin không thể được khử nhiễm được chuyển đến thư mục cách ly. Để biết thêm thông tin, hãy chuyển đến "*Quản lý những tệp tin cách ly*" (p. 88).

Nếu máy tính của bạn đã bị nhiễm phần mềm độc hại, vui lòng tham khảo "*Loại bỏ phần mềm độc hại khỏi hệ thống của bạn*" (p. 151). Để giúp bạn làm sạch máy tính khỏi phần mềm độc hại mà không thể gỡ bỏ được từ bên trong hệ điều hành Windows, Bitdefender cung cấp cho bạn"*Bitdefender Chế độ cứu hộ (Cứu hộ trong môi trường Windows 10)*" (p. 151). Đây là một môi trường an toàn, được thiết kế đặc biệt để loại bỏ phần mềm độc hại, cho phép bạn

khởi động máy tính độc lập với Windows. Khi máy tính chạy trong chế độ Cứu hộ (Môi trường Cứu hộ trong Windows 10), các phần mềm độc hại của Windows không hoạt động, làm cho nó dễ dàng để loại bỏ.

13.1. Quét lúc truy cập (bảo vệ thời gian thực)

Bitdefender cung cấp bảo vệ thời gian thực chống lại một loạt các mối đe dọa từ mã độc bằng cách quét tất cả các tập tin được truy cập và e-mail.

13.1.1. Bật hoặc tắt chế độ bảo vệ thời gian thực

Để bật hoặc tắt bảo vệ thời gian thực chống lại phần mềm độc hại:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Trong cửa sổ **Shield** , bật hoặc tắt **Bitdefender Shield** .
4. Nếu bạn muốn tắt chế độ bảo vệ thời gian thực, một cửa sổ cảnh báo sẽ xuất hiện. Bạn phải xác nhận muốn tạm thời vô hiệu hóa chế độ bảo vệ theo thời gian thực trong bao lâu. Bạn có thể vô hiệu hóa tạm thời sự bảo vệ trong 5,15 hoặc phút, một giờ, vĩnh viễn hoặc cho đến khi nào hệ thống khởi động lại. Bảo vệ thời gian thực sẽ tự động bật khi hết thời gian tạm dừng.

> **Cảnh báo**
> Đây là một lỗi bảo mật nguy hiểm. Chúng tôi khuyến cáo nên tắt chế độ bảo vệ thời gian thực trong khoảng thời gian ngắn nhất có thể. Nếu chế độ bảo vệ theo thời gian thực bị tắt, bạn sẽ không được bảo vệ khỏi các mã độc.

13.1.2. Cấu hình các thiết lập bảo vệ theo thời gian thực

Người dùng thành thạo có thể muốn tận dụng lợi thế của các thiết lập quét do Bitdefender cung cấp. Bạn có thể cấu hình các thiết lập bảo vệ thời gian thực một cách chi tiết bằng cách tạo ra một mức độ bảo vệ tùy ý.

Để cấu hình các thiết lập bảo vệ thời gian thực

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Trong cửa sổ **Shield**, hãy nhấp vào trình đơn **Hiển thị thiết lập nâng cao**.

Một cửa sổ được hiển thị.

4. Cuộn xuống để cấu hình các thiết lập quét khi cần thiết.

Thông tin về các lựa chọn quét

Bạn có thể tìm thấy thông tin này hữu ích:

- **Chỉ quét các ứng dụng.** Bạn có thể đặt Bitdefender để chỉ quét các ứng dụng đã truy cập.
- **Quét các ứng dụng không mong muốn.** Chọn tùy chọn này để chỉ quét các chương trình và các ứng dụng không mong muốn. Một ứng dụng có khả năng không mong muốn (PUA) hoặc chương trình không mong muốn (PUP) là một phần mềm thường đi kèm với phần mềm miễn phí và sẽ hiển thị cửa sổ bật lên hoặc cài đặt thanh công cụ trong trình duyệt mặc định. Một số người trong số họ sẽ thay đổi trang chủ hoặc công cụ tìm kiếm, những người khác sẽ chạy một số quy trình trong nền làm chậm máy tính hoặc sẽ hiển thị nhiều quảng cáo. Các chương trình này có thể được cài đặt mà không có sự đồng ý của bạn (còn được gọi là phần mềm quảng cáo) hoặc sẽ được bao gồm theo mặc định trong bộ cài đặt nhanh (được quảng cáo hỗ trợ).
- **Scan scripts.** Tính năng Quét tập lệnh cho phép Bitdefender quét các tập lệnh powershell và tài liệu văn phòng có thể chứa phần mềm độc hại dựa trên tập lệnh.
- **Quét các chia sẻ qua mạng.** Để truy cập an toàn vào mạng từ xa từ máy tính của bạn, chúng tôi khuyên bạn nên bật tùy chọn chia sẻ mạng Quét.
- **Quét những tệp lưu trữ.** Quét bên trong file nén là một quá trình chậm và tiêu tốn tài nguyên hệ thống, do đó không nên chọn loại file này ở chế độ bảo vệ thời gian thực. Lưu trữ có chứa file bị nhiễm không phải là một mối đe dọa trực tiếp đến an ninh của hệ thống của bạn. Các phần mềm độc hại có thể ảnh hưởng đến hệ thống của bạn chỉ khi các tập tin bị nhiễm được chiết xuất ra từ file nén và hoạt động khi không được bảo vệ ở chế độ thời gian thực.

  Nếu bạn quyết định sử dụng tùy chọn này, hãy bật nó lên, sau đó kéo thanh trượt dọc theo tỷ lệ để loại trừ lưu trữ quét dài hơn một giá trị nhất định tính bằng MB (Megabyte).
- **Quét email.** Để ngăn chặn phần mềm độc hại được tải xuống máy tính của bạn, Bitdefender tự động quét các email được gửi đến và đi.

Mặc dù không được khuyến cáo, bạn vẫn có thể vô hiệu hoá quét virus qua e-mail để tăng hiệu suất hệ thống. Nếu bạn vô hiệu các tùy chọn quét tương ứng, các e-mail và các tập tin nhận được sẽ không được quét, do đó cho phép các tập tin bị nhiễm độc được lưu vào máy tính của bạn. Đây không phải là một mối đe dọa lớn vì bảo vệ thời gian thực sẽ chặn các phần mềm độc hại khi các file bị nhiễm được truy cập (mở ra, di chuyển, sao chép hoặc thực thi).

- **Quét vùng khởi động đĩa cứng.** Bạn có thể thiết lập Bitdefender để quét vùng khởi động của đĩa cứng của bạn. Vùng này của đĩa cứng chứa mã máy tính cần thiết để bắt đầu quá trình khởi động. Khi một virus lây nhiễm khu vực khởi động, ổ đĩa có thể không thể tiếp cận được và bạn không thể khởi động hệ thống và truy cập dữ liệu.
- **Chỉ quét các tệp mới và tệp đã sửa đổi.** Bằng cách chỉ quét các tệp mới và đã sửa đổi, bạn có thể cải thiện đáng kể khả năng phản hồi của hệ thống với sự cân bằng tối thiểu trong bảo mật.
- **Quét keyloggers.** Chọn tùy chọn này khi quét hệ thống để tìm các ứng dụng ghi lại phím gõ. Trình ghi lại phím gõ sẽ ghi lại những gì bạn gõ trên bàn phím của bạn và gửi thông tin này qua Internet cho tin tặc (hacker). Kẻ tấn công có thể dễ dàng tìm thấy các thông tin nhạy cảm từ các chuỗi ký tự lấy cắp được trên máy của bạn, ví dụ như số tài khoản và mật khẩu, sau đó sử dụng nó để ăn cắp tiền của bạn.
- **Quét trước khi khởi động.** Chọn **Tùy chọn quét khởi động sớm** để quét hệ thống của bạn lúc khởi động ngay sau khi tất cả các dịch vụ quan trọng được nạp. Nhiệm vụ của tính năng này là để cải thiện việc phát hiện virus khi khởi động hệ thống và thời gian khởi động của hệ thống.

Hành động của phần mềm độc hại được phát hiện

Bạn có thể cấu hình các hành động được thực hiện bằng cách bảo vệ thời gian thực bằng cách làm theo các bước sau:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Trong cửa sổ **Shield**, hãy nhấp vào trình đơn **Hiển thị thiết lập nâng cao**.

   Một cửa sổ được hiển thị.
4. Cuộn xuống cho đến khi bạn thấy tùy chọn **Hành động đe dọa**.
5. Cấu hình các thiết lập quét cần thiết.

Các tác vụ sau có thể được thực hiện bằng cách bảo vệ thời gian thực trong Bitdefender:

Hành động thích hợp

Bitdefender sẽ đề nghị những hành động tùy thuộc vào loại tập tin được phát hiện:

- **Tệp bị nhiễm.** Các tệp được phát hiện bị nhiễm trùng khớp với cơ sở dữ liệu về mối đe dọa trong Bitdefender Threat Information Database. Bitdefender sẽ cố gắng tự động loại bỏ các mã phần mềm độc hại từ các tập tin bị nhiễm và tái tạo lại tập tin gốc. Hoạt động này được gọi là khử nhiễm.

  Các tập tin không thể được khử nhiễm được chuyển đến thư mục cách ly. Các tệp đã được cách ly sẽ không thể thực thi hoặc mở; do đó, không còn nguy cơ bị lây nhiễm cho toàn bộ máy. Để biết thêm thông tin, hãy chuyển đến "*Quản lý những tệp tin cách ly*" (p. 88).

  > **Quan trọng**
  > Đối với phần mềm độc hại cụ thể, khử nhiễm là không thể vì các tập tin được phát hiện hoàn toàn độc hại. Trong trường hợp này, các tập tin bị nhiễm sẽ bị xóa khỏi đĩa.

- **Những tập tin nghi ngờ.** Các tệp tin bị nghi ngờ bởi chương trình phân tích phỏng đoán. Tập tin đáng ngờ không thể được khử nhiễm, bởi vì không có một quy trình lập sẵn cho trường hợp này. Chúng sẽ được chuyển đến vùng cách ly để ngăn chặn khả năng lây lan.

  Mặc định, tập tin cách ly sẽ được tự động gửi đến Bitdefender để được phân tích bởi các kỹ sư nghiên cứu phần mềm độc hại của Bitdefender. Nếu sự hiện diện của mối đe dọa được xác nhận, bản cập nhật thông tin về mối đe dọa sẽ được phát hành để cho phép loại bỏ chúng.

- **Tập tin nén có chứa tập tin bị nhiễm.**
  - Tập tin nén chỉ chứa các file bị nhiễm sẽ bị tự động xóa.
  - Nếu một tập tin nén chứa cả tập tin bị nhiễm lẫn tập tin sạch sẽ, Bitdefender sẽ cố gắng để xóa các tập tin bị nhiễm miễn là nó có thể tái tạo lại các tập tin nén chứa các tập tin sạch. Nếu tái tạo lại tập tin nén là không thể, bạn sẽ được thông báo rằng không có hành động nào được thực hiện để tránh mất dữ liệu sạch.

Chuyển sang cách ly
Chuyển các tập tin bị nhiễm đến vùng cách ly. Các tệp đã được cách ly sẽ không thể thực thi hoặc mở; do đó, không còn nguy cơ bị lây nhiễm cho toàn bộ máy. Để biết thêm thông tin, hãy chuyển đến "*Quản lý những tệp tin cách ly*" (p. 88).

Từ chối truy cập
Trong trường hợp một tập tin bị nhiễm được phát hiện, việc truy cập tập tin đó sẽ bị từ chối.

13.1.3. Khôi phục Cấu hình mặc định

Các thiết lập mặc định bảo vệ theo thời gian thực đảm bảo một sự bảo vệ hiệu quả chống lại phần mềm độc hại, không ảnh hưởng hiệu năng hệ thống.

Để khôi phục các thiết lập bảo vệ thời gian thực mặc định.

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Trong cửa sổ **Shield**, hãy nhấp vào trình đơn **Hiển thị thiết lập nâng cao**.

   Một cửa sổ được hiển thị.
4. Cuộn xuống cho đến khi bạn thấy tùy chọn **Đặt lại cài đặt** . Chọn tùy chọn này để đặt lại cài đặt chống vi rút thành mặc định.

13.2. Quét theo yêu cầu

Mục tiêu chính của Bitdefender là giữ cho máy tính của bạn không có bất kỳ mã độc nào. Điều này được thực hiện bằng cách giữ cho máy tính của bạn không bị nhiễm virus mới và bằng cách quét e-mail và bất kỳ tập tin được tải về hoặc sao chép vào hệ thống của bạn.

Có một mối nguy hại đã nằm sẵn trong hệ thống của bạn, trước khi bạn cài đặt Bitdefender. Đây là lý do tại sao bạn nên quét máy tính ngay sau khi cài đặt Bitdefender. Và bạn nên thường xuyên quét máy tính để tìm xem liệu có mã độc nào còn tiềm ẩn hay không.

Quét theo yêu cầu là thiết lập cơ bản của các tác vụ quét. Nhiệm vụ quét chỉ rõ các tùy chọn quét và các đối tượng được quét. Bạn có thể quét máy tính bất kì khi nào bạn muốn bằng cách chạy tác vụ mặc định hoặc những tác vụ do bạn định nghĩa. Nếu bạn muốn quét các địa điểm cụ thể trên máy tính hoặc cấu hình các tùy chọn quét, hãy cấu hình và chạy một tác vụ quét tùy chỉnh.

13.2.1. Quét một tập tin hoặc thư mục để tìm phần mềm độc hại

Bạn nên quét các tập tin và thư mục bất cứ khi nào bạn nghi ngờ rằng chúng có thể bị nhiễm virus. Bấm chuột phải vào tập tin hoặc thư mục bạn muốn quét, chọn **Bitdefender** và chọn **Quét với Bitdefender**. Trình Thuật sĩ quét virus sẽ xuất hiện và hướng dẫn bạn quá trình quét. Vào giai đoạn cuối của quá trình quét, bạn sẽ được nhắc nhở để lựa chọn các hành động được thực hiện trên các tập tin phát hiện nghi vấn, nếu có.

13.2.2. Chạy một Quét nhanh

Quét nhanh sử dụng công nghệ đám mây để phát hiện phần mềm độc hại đang chạy trong hệ thống của bạn. Chạy Quét nhanh thường mất ít hơn một phút và sử dụng một phần nhỏ tài nguyên hệ thống cần thiết cho việc quét vi-rút thông thường.

Để chạy Quét nhanh:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Quét nhanh** .
3. Thực hiện theo Thuật sĩ quét virus để hoàn tất quá trình quét. Bitdefender sẽ tự động có những hành động được đề nghị về tập tin được phát hiện nghi vấn. Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý.

13.2.3. Chạy một Quét Hệ thống

Việc Quét Hệ Thống sẽ quét toàn bộ máy tính để tìm tất cả các loại phần mềm độc hại đe dọa an ninh cho bạn, chẳng hạn như mã độc, phần mềm gián điệp, phần mềm quảng cáo, rootkits và nhiều loại khác.

Ghi chú
Vì **Quét hệ thống** thực hiện quét toàn bộ hệ thống, nó có thể mất một thời gian. Vì vậy, bạn nên chạy tác vụ này khi không sử dụng máy tính.

Trước khi chạy một Quét hệ thống, chúng tôi khuyến cáo:

- Đảm bảo Bitdefender được cập nhật với cơ sở dữ liệu về mối đe dọa mới nhất. Quét máy tính sử dụng một cơ sở dữ liệu chữ ký đã cũ có thể ngăn chặn Bitdefender phát hiện phần mềm độc hại mới được tìm thấy kể từ

lần cập nhật mới nhất. Để biết thêm thông tin, hãy chuyển đến *"Giữ Bitdefender được cập nhật"* (p. 37).

- Tắt tất cả các chương trình đang mở.

Nếu bạn muốn quét các địa điểm cụ thể trên máy tính của bạn hoặc để cấu hình các tùy chọn quét, hãy cấu hình và chạy một quét tùy chỉnh. Để biết thêm thông tin, hãy chuyển đến *"Cấu hình một Quét tùy chỉnh"* (p. 77).

Để chạy Quét hệ thống:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Quét hệ thống** .
3. Lần đầu tiên bạn chạy Quét hệ thống, bạn sẽ được giới thiệu về tính năng này. Nhấp **OK, TÔI ĐÃ HIỂU** để tiếp tục.
4. Thực hiện theo Thuật sĩ quét virus để hoàn tất quá trình quét. Bitdefender sẽ tự động có những hành động được đề nghị về tập tin được phát hiện nghi vấn. Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý.

13.2.4. Cấu hình một Quét tùy chỉnh

Trong cửa sổ **Quản lý Quét** , bạn có thể thiết lập Bitdefender để chạy quét bất cứ khi nào bạn cho rằng máy tính của mình cần kiểm tra các mối đe dọa tiềm ẩn. Bạn có thể lên lịch Quét hệ thống hoặc Quét nhanh , hoặc bạn có thể tạo quét tùy chỉnh một cách thuận tiện.

Khi bạn truy cập vào cửa sổ, các biểu tượng sau đây khả dụng:

Tác vụ quét theo lịch trình đã bị tắt.

Tác vụ quét theo lịch trình được bật.

Cấu hình chi tiết có thể được thực hiện ở đây.

Xóa bản quét đã chọn. Tùy chọn này chỉ có sẵn cho quét tùy chỉnh mới.

Để cấu hình quét tùy chỉnh mới một cách chi tiết:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Quản lý quét** .
3. Nhấp vào **Tạo tác vụ quét mới** .
4. Trong trường **Tên tác vụ** , nhập tên cho quá trình quét, sau đó chọn các vị trí bạn muốn quét và sau đó nhấp vào **TIẾP** .

5. Cấu hình các tùy chọn chung:
   - **Chỉ quét các ứng dụng** . Bạn có thể đặt Bitdefender để chỉ quét các ứng dụng đã truy cập.
   - **Tác vụ quét ưu tiên** . Bạn có thể chọn tác động mà quá trình quét nên có đối với hiệu suất hệ thống của bạn.
     - Tự động - Ưu tiên của quá trình quét sẽ phụ thuộc vào hoạt động của hệ thống. Để đảm bảo rằng quá trình quét sẽ không ảnh hưởng đến hoạt động của hệ thống, Bitdefender sẽ quyết định liệu quy trình quét nên được chạy với mức độ ưu tiên cao hay thấp.
     - Cao - Mức độ ưu tiên của quá trình quét sẽ cao. Bằng cách chọn tùy chọn này, bạn sẽ cho phép các chương trình khác chạy chậm hơn và giảm thời gian cần thiết để quá trình quét kết thúc.
     - Thấp - Mức độ ưu tiên của quá trình quét sẽ thấp. Bằng cách chọn tùy chọn này, bạn sẽ cho phép các chương trình khác chạy nhanh hơn và tăng thời gian cần thiết để quá trình quét kết thúc.
   - **Hành động quét bài** . Chọn hành động nào Bitdefender sẽ thực hiện trong trường hợp không tìm thấy mối đe dọa nào:
     - Hiện cửa sổ Tổng Quát
     - Tắt thiết bị
     - Đóng cửa sổ Quét
6. Nếu bạn muốn định cấu hình chi tiết các tùy chọn quét, hãy nhấp vào **Hiển thị tùy chọn nâng cao** . Bạn có thể tìm thấy thông tin về các bản quét được liệt kê ở cuối phần này.

   Nhấp vào **TIẾP THEO** .
7. Bật **Tác vụ quét định kỳ** , sau đó chọn thời điểm quét tùy chỉnh bạn đã tạo sẽ bắt đầu.
   - Tại lúc hệ thống khởi động
   - Hàng ngày
   - hàng tháng
   - hàng tuần

Nếu bạn chọn Hàng ngày, Hàng tháng hoặc Hàng tuần, hãy kéo thanh trượt dọc theo tỷ lệ để đặt khoảng thời gian mong muốn khi quá trình quét theo lịch sẽ bắt đầu.

8. Nhấp vào **LƯU** để lưu cài đặt và đóng cửa sổ cấu hình.

   Tùy thuộc vào địa điểm được quét, quá trình quét có thể mất một thời gian. Nếu các mối đe dọa sẽ được tìm thấy trong quá trình quét, bạn sẽ được nhắc chọn các hành động được thực hiện trên các dữ liệu được phát hiện.

Thông tin về các lựa chọn quét

Bạn có thể tìm thấy thông tin này hữu ích:

- Nếu bạn không quen với một số thuật ngữ, kiểm tra chúng tại thuật ngữ. Bạn cũng có thể tìm thấy thông tin hữu ích bằng cách tìm kiếm trên Internet.
- **Quét các ứng dụng không mong muốn.** Chọn tùy chọn này để chỉ quét các chương trình và các ứng dụng không mong muốn. Một ứng dụng có khả năng không mong muốn (PUA) hoặc chương trình không mong muốn (PUP) là một phần mềm thường đi kèm với phần mềm miễn phí và sẽ hiển thị cửa sổ bật lên hoặc cài đặt thanh công cụ trong trình duyệt mặc định. Một số người trong số họ sẽ thay đổi trang chủ hoặc công cụ tìm kiếm, những người khác sẽ chạy một số quy trình trong nền làm chậm máy tính hoặc sẽ hiển thị nhiều quảng cáo. Các chương trình này có thể được cài đặt mà không có sự đồng ý của bạn (còn được gọi là phần mềm quảng cáo) hoặc sẽ được bao gồm theo mặc định trong bộ cài đặt nhanh (được quảng cáo hỗ trợ).
- **Quét những tệp lưu trữ.** Lưu trữ có chứa file bị nhiễm không phải là một mối đe dọa trực tiếp đến an ninh của hệ thống của bạn. Các phần mềm độc hại có thể ảnh hưởng đến hệ thống của bạn chỉ khi các tập tin bị nhiễm được chiết xuất ra từ file nén và hoạt động khi không được bảo vệ ở chế độ thời gian thực. Tuy nhiên, bạn nên sử dụng tùy chọn này để phát hiện và loại bỏ các mối đe dọa tiềm ẩn, ngay cả khi nó chưa phải là một mối đe dọa ngay lập tức.

  Kéo thanh trượt dọc theo tỷ lệ để loại trừ lưu trữ quét dài hơn một giá trị nhất định tính bằng MB (Megabyte).

Ghi chú
Quét các tập tin nén làm tăng thời gian quét tổng thể và đòi hỏi nhiều tài nguyên hệ thống hơn.

- **Chỉ quét các tệp mới và tệp đã sửa đổi.** Bằng cách chỉ quét các tệp mới và đã sửa đổi, bạn có thể cải thiện đáng kể khả năng phản hồi của hệ thống với sự cân bằng tối thiểu trong bảo mật.
- **Quét vùng khởi động đĩa cứng.** Bạn có thể thiết lập Bitdefender để quét vùng khởi động của đĩa cứng của bạn. Vùng này của đĩa cứng chứa mã máy tính cần thiết để bắt đầu quá trình khởi động. Khi một virus lây nhiễm khu vực khởi động, ổ đĩa có thể không thể tiếp cận được và bạn không thể khởi động hệ thống và truy cập dữ liệu.
- **Quét bộ nhớ.** Chọn tùy chọn này để quét các chương trình đang chạy trong bộ nhớ hệ thống của bạn.
- **Quét thanh ghi.** Chọn tùy chọn này để quét các khóa thanh ghi hệ thống. Windows Registry là một cơ sở dữ liệu lưu trữ các thiết lập cấu hình và các tùy chọn cho các thành phần hệ điều hành Windows cũng như các ứng dụng được cài đặt.
- **Quét cookies.** Chọn tùy chọn này để quét các tập tin cookie được lưu trữ bởi các trình duyệt web trên máy tính của bạn.
- **Quét keyloggers.** Chọn tùy chọn này khi quét hệ thống để tìm các ứng dụng ghi lại phím gõ. Trình ghi lại phím gõ sẽ ghi lại những gì bạn gõ trên bàn phím của bạn và gửi thông tin này qua Internet cho tin tặc (hacker). Kẻ tấn công có thể dễ dàng tìm thấy các thông tin nhạy cảm từ các chuỗi ký tự lấy cắp được trên máy của bạn, ví dụ như số tài khoản và mật khẩu, sau đó sử dụng nó để ăn cắp tiền của bạn.

13.2.5. Trình Thuật sĩ quét virus

Bất cứ khi nào bạn khởi động một tác vụ quét theo yêu cầu (ví dụ, kích chuột phải vào một thư mục, điểm đến Bitdefender và chọn **Quét với Bitdefender**), Trình thuật sĩ quét virus của Bitdefender sẽ xuất hiện. Thực hiện theo các hướng dẫn để hoàn tất quá trình quét.

Ghi chú
Nếu trình hướng dẫn quét không xuất hiện, quá trình quét có thể được cấu hình để chạy âm thầm ở chế độ nền. Tìm biểu tượng tiến trình quét tại khay

hệ thống. Bạn có thể nhấp vào biểu tượng này để mở cửa sổ quét và xem tiến trình quét.

Bước 1 - Tiến hành quét

Bitdefender sẽ bắt đầu quét những đối tượng được chọn. Bạn có thể xem thông tin thời gian thực về tình trạng quét và thống kê (bao gồm cả thời gian trôi qua, ước tính thời gian còn lại và số lượng các mối đe dọa được phát hiện).

Chờ cho Bitdefender hoàn tất quá trình quét. Quá trình quét có thể mất một khoảng thời gian, tuỳ thuộc vào độ phức tạp của lần quét.

Dừng hoặc tạm dừng quá trình quét. Bạn có thể dừng quét bất cứ lúc nào bạn muốn bằng cách nhấp **Dừng**. Bạn sẽ chuyển đến bước cuối cùng của quá trình trợ giúp. Để tạm ngừng quá trình quét, chỉ cần nhấp **Tạm dừng**. Bạn sẽ phải bấm **Tiếp tục** để tiếp tục quét.

Tập tin nén với mật khẩu bảo vệ. Khi một tập tin nén có mật khẩu được phát hiện, tùy thuộc vào các thiết lập quét, bạn có thể được nhắc nhở để cung cấp mật khẩu. Tệp tin nén có mật khẩu nên không thể quét được trừ khi bạn cung cấp mật khẩu. Có những lựa chọn sau:

- **Mật khẩu.** Nếu bạn muốn Bitdefender quét các tập tin nén, chọn tùy chọn này và nhập mật khẩu. Nếu bạn không biết mật khẩu, chọn một trong các tùy chọn khác.
- **Đừng hỏi mật khẩu và bỏ qua đối tượng này.** Chọn tùy chọn này để bỏ qua chức năng quét tập tin nén này.
- **Bỏ qua tất cả các tập tin có mật khẩu bảo vệ mà không cần quét chúng.** Chọn tùy chọn này nếu bạn không muốn bị làm phiền bởi các tập tin nén có mật khẩu. Bitdefender sẽ không thể quét chúng, nhưng một bản ghi sẽ được lưu giữ trong hệ thống lưu dấu.

Chọn tùy chọn mong muốn và nhấn **OK** để tiếp tục quét.

Bước 2 - Chọn hành động

Vào giai đoạn cuối của quá trình quét, bạn sẽ được nhắc nhở để lựa chọn các hành động được thực hiện trên các tập tin phát hiện nghi vấn, nếu có.

Ghi chú

Khi bạn chạy một Quét nhanh hoặc một Quét hệ thống, Bitdefender sẽ tự động thực hiện những hành động được đề nghị đối với tập tin được phát hiện trong

quá trình quét. Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý.

Những đối tượng bị nhiễm được hiển thị theo nhóm dựa trên loại mã độc gây nhiễm. Nhấp vào liên kết tương ứng của mối đe dọa để tìm hiểu thêm thông tin về các đối tượng bị nhiễm virus.

Bạn có thể chọn một hành động chung cho tất cả các nhóm vấn đề hoặc bạn cũng có thể tách riêng từng hành động cho từng nhóm. Một hoặc một số các tùy chọn sau đây có thể xuất hiện trên trình đơn:

Hành động thích hợp

Bitdefender sẽ đề nghị những hành động tùy thuộc vào loại tập tin được phát hiện:

- **Tệp bị nhiễm.** Các tệp được phát hiện bị nhiễm trùng khớp với cơ sở dữ liệu về mối đe dọa trong Bitdefender Threat Information Database. Bitdefender sẽ cố gắng tự động loại bỏ các mã phần mềm độc hại từ các tập tin bị nhiễm và tái tạo lại tập tin gốc. Hoạt động này được gọi là khử nhiễm.

  Các tập tin không thể được khử nhiễm được chuyển đến thư mục cách ly. Các tệp đã được cách ly sẽ không thể thực thi hoặc mở; do đó, không còn nguy cơ bị lây nhiễm cho toàn bộ máy. Để biết thêm thông tin, hãy chuyển đến "*Quản lý những tệp tin cách ly*" (p. 88).

  Quan trọng
  Đối với phần mềm độc hại cụ thể, khử nhiễm là không thể vì các tập tin được phát hiện hoàn toàn độc hại. Trong trường hợp này, các tập tin bị nhiễm sẽ bị xóa khỏi đĩa.

- **Những tập tin nghi ngờ.** Các tệp tin bị nghi ngờ bởi chương trình phân tích phỏng đoán. Tập tin đáng ngờ không thể được khử nhiễm, bởi vì không có một quy trình lập sẵn cho trường hợp này. Chúng sẽ được chuyển đến vùng cách ly để ngăn chặn khả năng lây lan.

  Mặc định, tập tin cách ly sẽ được tự động gửi đến Bitdefender để được phân tích bởi các kỹ sư nghiên cứu phần mềm độc hại của Bitdefender. Nếu sự hiện diện của mối đe dọa được xác nhận, bản cập nhật thông tin về mối đe dọa sẽ được phát hành để cho phép loại bỏ chúng.

- **Tập tin nén có chứa tập tin bị nhiễm.**
  - Tập tin nén chỉ chứa các file bị nhiễm sẽ bị tự động xóa.

- Nếu một tập tin nén chứa cả tập tin bị nhiễm lẫn tập tin sạch sẽ, Bitdefender sẽ cố gắng để xóa các tập tin bị nhiễm miễn là nó có thể tái tạo lại các tập tin nén chứa các tập tin sạch. Nếu tái tạo lại tập tin nén là không thể, bạn sẽ được thông báo rằng không có hành động nào được thực hiện để tránh mất dữ liệu sạch.

Xoá

Loại bỏ các tập tin phát hiện từ đĩa.

Nếu tập tin bị nhiễm được lưu trữ trong một tập tin nén cùng với các tập tin sạch, Bitdefender sẽ cố gắng xóa các file bị nhiễm và tái tạo lại tập tin nén chứa các tập tin sạch. Nếu tái tạo lại tập tin nén là không thể, bạn sẽ được thông báo rằng không có hành động nào được thực hiện để tránh mất dữ liệu sạch.

Không làm gì

Không có hành động nào được tiến hành đối với các tập tin đã nhận diện. Sau khi hoàn tất quá trình quét, bạn có thể kiểm tra lịch sử quét để xem các thông tin đối với các tệp này.

Nhấn **Tiếp tục** để áp dụng hành động đã định.

Bước 3 – Tổng kết

Khi Bitdefender kết thúc quá trình sửa chữa, kết quả quét sẽ xuất hiện ở một cửa sổ mới. Nếu bạn muốn xem thông tin toàn diện về quá trình quét, nhấn **Xem bản ghi** để xem bản ghi quá trình quét.

Quan trọng

Trong đa số trường hợp, Bitdefender khử nhiễm thành công các tệp bị nhiễm mà nó phát hiện ra hoặc sẽ cách ly các tệp này. Tuy nhiên, có những vấn đề không thể được giải quyết tự động. Bạn có thể được yêu cầu khởi động lại hệ thống để hoàn tất quá trình làm sạch hệ thống. Để biết thêm thông tin và hướng dẫn về cách để loại bỏ phần mềm độc hại thủ công, tham khảo "*Loại bỏ phần mềm độc hại khỏi hệ thống của bạn*" (p. 151).

13.2.6. Kiểm tra nhật kí quét

Mỗi lần quét được thực hiện, một bản ghi được tạo ra và Bitdefender lưu hồ sơ các vấn đề phát hiện trong cửa sổ Diệt virus. Bản ghi (Scan log) chứa thông tin chi tiết về quá trình quét, như là lựa chọn quét, đích quét, hiểm họa tìm thấy và hành động dã thực hiện đối với hiểm họa.

Bạn có thể mở nhật ký quét trực tiếp từ trình hướng dẫn quét sau khi quá trình quét hoàn tất, bằng cách nhấn **Xem nhật ký**.

Để kiểm tra log quét hay các nhiễm trùng được phát hiện tại một thời gian sau:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.
2. Trong Tab**Tất cả**, chọn thông báo về quét mới nhất.

   Đây là nơi bạn có thể tìm thấy tất cả các sự kiện quét phần mềm độc hại, bao gồm các mối đe dọa được phát hiện bởi Quét khi truy cập, Quét chủ động bởi người sử dụng và những thay đổi trạng thái của quét tự động.
3. Trong danh sách các thông báo, bạn có thể kiểm tra những tác vụ quét đã được thực hiện gần đây. Nhấp vào một thông báo để xem chi tiết về nó.
4. Để mở nhật ký quét, nhấn **Xem nhật ký**.

13.3. Tự động quét các phương tiện tháo lắp

Bitdefender tự động phát hiện khi bạn kết nối một thiết bị lưu trữ di động với máy tính của bạn và quét nó dưới nền khi bật tùy chọn Autoscan. Đây là khuyến cáo để ngăn chặn phần mềm độc hại lây nhiễm vào máy tính của bạn.

Thiết bị phát hiện rơi vào một trong các loại:

- CD/DVD
- Flash driver, chẳng hạn như bút flash và ổ đĩa cứng gắn ngoài
- ổ đĩa mạng chia sẻ

Bạn có thể cấu hình tự động quét riêng cho từng loại thiết bị lưu trữ. Theo mặc định, Tự động quét các ổ đĩa mạng là tắt.

13.3.1. Chúng làm việc như thế nào?

Khi phát hiện một thiết bị lưu trữ di động, Bitdefender sẽ bắt đầu quét ổ đĩa này để tìm phần mềm độc hại(với điều kiện tính năng quét tự động được kích hoạt cho loại thiết bị đó). Bạn sẽ được thông báo thông qua một cửa sổ hiển thị rằng một thiết bị mới đã được phát hiện và nó đang được quét.

Một biểu tượng quét của Bitdefender sẽ xuất hiện trong khay hệ thống. Bạn có thể nhấp vào biểu tượng này để mở cửa sổ quét và xem tiến trình quét.

Khi quá trình quét hoàn tất, cửa sổ kết quả quét được hiển thị thông báo cho bạn nếu bạn có thể truy cập các tập tin trên thiết bị di động một cách an toàn.

Trong hầu hết các trường hợp, Bitdefender tự động loại bỏ phần mềm độc hại được phát hiện hoặc cô lập các tập tin bị nhiễm vào vùng cách ly. Nếu vẫn còn những mối đe dọa chưa được giải quyết, bạn sẽ được nhắc nhở để lựa chọn các hành động xử lý.

Ghi chú

Cần ý thức rằng không diệt được virus trên các tập tin bị nhiễm hoặc nghi ngờ phát hiện trên đĩa CD / DVD. Tương tự như vậy, không diệt được virus trên các tập tin bị nhiễm hoặc nghi ngờ phát hiện trên ổ đĩa mạng nếu bạn không có các quyền thích hợp.

Thông tin này có thể hữu ích cho bạn:

- Hãy cẩn thận khi sử dụng một đĩa CD/DVD bị nhiễm phần mềm độc hại, vì các phần mềm độc hại không thể được gỡ bỏ khỏi CD/DVD. Hãy chắc chắn bảo vệ thời gian thực được bật để ngăn chặn phần mềm độc hại lây lan sang hệ thống của bạn. Tốt nhất bạn hãy sao chép những dữ liệu có giá trị về hệ thống của bạn, và sau đó hủy đĩa đó đi.
- Trong một số trường hợp, Bitdefender không thể loại bỏ phần mềm độc hại từ các tập tin cụ thể do hạn chế về pháp lý hoặc kỹ thuật. Một ví dụ điển hình là các tập tin nén bằng cách sử dụng công nghệ độc quyền (bởi vì các tập tin nén không thể được tái tạo một cách chính xác).

  Để tìm hiểu cách đối phó với các mối đe dọa, hãy tham khảo "*Loại bỏ phần mềm độc hại khỏi hệ thống của bạn*" (p. 151).

13.3.2. Quản lý quét thiết bị tháo lắp

Để quản lý tự động quét các đĩa di động:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Chọn tab **Ổ đĩa và thiết bị** .

Các tùy chọn quét được cấu hình sẵn cho các kết quả phát hiện tốt nhất. Nếu file bị nhiễm được phát hiện, Bitdefender sẽ cố gắng để khử nhiễm (loại bỏ các mã phần mềm độc hại) hoặc di chuyển chúng đến vùng cách ly. Nếu cả hai hành động thất bại, trình thuật sĩ sẽ cho phép bạn chỉ định các hành

động khác được thực hiện trên các tập tin bị nhiễm virus. Các tùy chọn quét là tiêu chuẩn và bạn không thể thay đổi chúng.

Để bảo vệ tốt nhất, bạn nên chọn **Scan tự động** cho tất cả các loại thiết bị lưu trữ di động.

13.4. Quét các tập tin hosts

Các file host đi theo mặc định với bộ cài đặt hệ điều hành của bạn và được sử dụng để ánh xạ tên máy thành địa chỉ IP mỗi khi bạn truy cập một trang web mới, kết nối với FTP hoặc đến các máy chủ Internet khác. Đây là một tập tin văn bản đơn giản và các chương trình độc hại có thể sửa đổi nó. Người dùng cao cấp biết làm thế nào để sử dụng nó để chặn các quảng cáo gây phiền nhiễu, biểu ngữ, cookie của bên thứ ba, hoặc tin tặc.

Để cấu hình quét tập tin host:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Advanced**.
3. Bật hoặc tắt **Quét tệp máy chủ lưu trữ**.

13.5. Cấu hình loại trừ quét

Bitdefender cho phép loại trừ các tập tin, thư mục hoặc phần mở rộng tập tin cụ thể khỏi bị quét. Tính năng này được thiết kế để tránh làm phiền công việc của bạn và nó cũng có thể giúp cải thiện hiệu suất hệ thống. Loại trừ sẽ được sử dụng bởi người dùng có kiến thức máy tính cao cấp hoặc theo các khuyến nghị của đại diện Bitdefender.

Bạn có thể cấu hình loại trừ để áp dụng cho Quét lúc truy cập hoặc theo yêu cầu, hoặc cả hai. Các đối tượng được bỏ qua trong quá trình quét lúc truy cập sẽ không bị quét, chúng sẽ không được quét khi bạn hoặc chương trình khác truy cập chúng.

Ghi chú

Loại trừ sẽ không áp dụng cho quét theo ngữ cảnh. Quét theo bối cảnh là một loại quét theo yêu cầu: bạn bấm chuột phải vào tập tin hoặc thư mục bạn muốn quét và chọn **Quét với Bitdefender**.

13.5.1. Loại trừ tập tin và thư mục khỏi quét

Để loại trừ các tập tin và thư mục cụ thể từ quét:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Chọn tab **Loại trừ**.
4. Nhấp vào **Danh sách các tập tin và thư mục bị loại khỏi quá trình quét**. Trong cửa sổ hiện ra, bạn có thể quản lý các tập tin và thư mục được bỏ qua khi quét.
5. Thêm loại trừ bằng cách làm theo các bước sau:
   a. Nhấn vào **Thêm**.
   b. Nhấp **Duyệt**, chọn tập tin hoặc thư mục mà bạn muốn bỏ qua khi quét, và sau đó nhấp vào **Thêm**. Ngoài ra, bạn có thể gõ (hoặc chép và dán) đường dẫn đến tập tin hoặc thư mục trong trường lựa chọn.
   c. Theo mặc định, các tập tin hoặc thư mục đã chọn được loại trừ với cả hai kiểu quét theo yêu cầu và quét lúc truy cập. Để thay đổi thời điểm áp dụng ngoại lệ, hãy chọn một trong các tùy chọn khác.
   d. Nhấn vào **Thêm**.

13.5.2. Loại trừ phần mở rộng tập tin khỏi quét

Khi bạn ngoại trừ một phần mở rộng tệp khi quét, Bitdefender sẽ không còn quét các tệp có tiện ích đó nữa, bất kể vị trí của chúng trên máy tính của bạn. Việc loại trừ cũng áp dụng cho các tập tin trên thiết bị tháo lắp, chẳng hạn như đĩa CD, DVD, thiết bị lưu trữ USB hoặc ổ đĩa mạng.

> **!** **Quan trọng**
> Hãy cẩn thận khi loại trừ phần mở rộng tập tin khỏi tác vụ quét vì các ngoại lệ này có thể làm cho máy tính của bạn dễ bị lây nhiễm phần mềm độc hại.

Để loại trừ phần mở rộng tập tin khỏi quét

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Chọn tab **Loại trừ**.
4. Nhấp vào **Danh sách các phần mở rộng bị loại khỏi quá trình quét**. Trong cửa sổ hiện ra, bạn có thể quản lý các phần mở rộng tập tin được bỏ qua khi quét.
5. Thêm loại trừ bằng cách làm theo các bước sau:

a. Nhấn vào **Thêm**.

b. Nhập các phần mở rộng bạn muốn loại trừ khỏi quá trình quét, tách chúng bằng dấu chấm phẩy (;). Đây là một ví dụ:

txt;avi;jpg

c. Theo mặc định, tất cả các file với phần mở rộng chỉ định được loại trừ với cả hai kiểu quét theo yêu cầu và quét theo lúc truy cập. Để thay đổi thời điểm áp dụng ngoại lệ, hãy chọn một trong các tùy chọn khác.

d. Nhấn vào **Thêm**.

13.5.3. Cấu hình loại trừ quét

Nếu loại trừ quét không còn cần thiết, chúng tôi khuyên bạn xóa hoặc vô hiệu hoá loại trừ quét.

Để quản lý loại trừ quét:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
3. Chọn tab **Loại trừ**.
4. Sử dụng các tùy chọn trong **Danh sách các tập tin và thư mục bị loại khỏi quá trình quét** trình đơn quản lý loại trừ quét.
5. Để xóa bỏ hay sửa loại trừ quét, nhấp vào một trong các liên kết có sẵn. Thực hiện các bước dưới đây:
   - Để xóa một mục khỏi danh sách, hãy chọn mục đó và nhấp vào **Xóa**.
   - Để chỉnh sửa một mục trong bảng, kích đúp vào nó (hoặc chọn nó và nhấp vào**Chỉnh sửa**). Một cửa sổ mới xuất hiện khi bạn thay đổi phần mở rộng hoặc đường dẫn và kiểu quét mà bạn muốn chúng được bỏ qua. Thực hiện các thay đổi cần thiết, sau đó bấm **Sửa đổi**.

13.6. Quản lý những tệp tin cách ly

Bitdefender cách ly các tập tin bị nhiễm phần mềm độc hại không thể khử nhiễm và các tập tin đáng ngờ trong một khu vực an toàn. Khi mã độc được cách ly, chúng sẽ không thể gây tác hại được vì chúng sẽ không còn có thể thực thi được các tác vụ hay chạy trong hệ thống nữa.

Mặc định, tập tin cách ly sẽ được tự động gửi đến Bitdefender để được phân tích bởi các kỹ sư nghiên cứu phần mềm độc hại của Bitdefender. Nếu sự

hiện diện của mối đe dọa được xác nhận, bản cập nhật thông tin về mối đe dọa sẽ được phát hành để cho phép loại bỏ chúng.

Ngoài ra, Bitdefender sẽ quét các tập tin đã bị cách ly sau mỗi lần cập nhật mẫu chữ ký mới. Các tập tin được làm sạch sẽ được tự động chuyển trở lại vị trí ban đầu của chúng.

Để kiểm tra và quản lý các tập tin cách ly:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong phần **CHỐNG VIRUS** , nhấp **Cách Ly** .

   Ở đây bạn có thể xem tên của các tệp cách ly, vị trí ban đầu của chúng và tên của các mối đe dọa được phát hiện.
3. Tập tin cách ly được quản lý tự động bởi Bitdefender theo các thiết lập mặc định.

   Mặc dù không được khuyến cáo, nhưng bạn vẫn có thể điều chỉnh các thiết lập cách ly theo nhu cầu của bạn bằng cách nhấp vào **Xem cài đặt** .

   Bấm công tắc để bật hoặc tắt:

   Quét lại tập tin đã cách ly sau khi thông tin cập nhật đe dọa
   Giữ tùy chọn này bật để tự động quét các tập tin cách ly sau mỗi lần cập nhật dữ liệu mới. Các tập tin được làm sạch sẽ được tự động chuyển trở lại vị trí ban đầu của chúng.

   Xóa nội dung trên 30 ngày
   Các tập tin bị cách ly hơn 30 ngày sẽ tự động bị xóa.

   Tạo loại trừ cho các tập tin được khôi phục
   Các tệp mà bạn khôi phục từ vùng cách ly sẽ được di chuyển trở lại vị trí ban đầu của chúng mà không được sửa chữa và sẽ tự động loại trừ khỏi các lần quét trong tương lai.
4. Để xóa một tập tin bị cách ly, chọn nó và nhấn vào nút **Xóa**. Nếu bạn muốn khôi phục lại một tập tin được cách ly về vị trí ban đầu của nó, chọn nó và nhấp vào **Khôi phục**.

14. PHÒNG CHỐNG TẤN CÔNG NÂNG CAO

Bitdefender Advanced Threat Defense là một công nghệ tiên phong sáng tạo phát hiện sử dụng các phương pháp tiên tiến để phát hiện mã độc tống tiền và các mối đe dọa tiềm năng mới khác trong thời gian thực.

PHÒNG CHỐNG TẤN CÔNG NÂNG CAO liên tục giám sát các ứng dụng đang chạy trên máy tính, tìm kiếm các hành động tương tự như phần mềm độc hại Mỗi một trong các hành động được ghi điểm và tổng điểm được tính cho mỗi quá trình.

Như một biện pháp an toàn, bạn sẽ được thông báo mỗi khi các mối đe dọa và các quy trình độc hại có thể được phát hiện và chặn.

14.1. Bật hoặc tắt Chế độ Advanced Threat Defense

Để bật hoặc tắt chế độ Advanced Threat Defense

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **PHÒNG THỦ MỐI ĐE DỌA NÂNG CAO**, bật hoặc tắt chuyển đổi.

> **Ghi chú**
> Để giữ cho hệ thống của bạn được bảo vệ khỏi mã độc tống tiền và các cuộc tấn công phần mềm độc hại khác, chúng tôi khuyên bạn chỉ nên vô hiệu hóa tính năng Advanced Threat Defense trong thời gian ít nhất có thể.

14.2. Kiểm tra các cuộc tấn công độc hại đã phát hiện

Bất cứ khi nào các mối đe dọa hoặc các quy trình độc hại tiềm ẩn được phát hiện, Bitdefender sẽ chặn chúng để ngăn máy tính của bạn không bị nhiễm phần mềm mã hóa hoặc phần mềm độc hại khác. Bạn có thể kiểm tra bất kỳ lúc nào danh sách các cuộc tấn công độc hại được phát hiện bằng cách làm theo các bước sau:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **PHÒNG CHỐNG CÁC MỐI ĐE DỌA**, nhấp **CHỐNG TẤN CÔNG**.
3. Lần đầu tiên bạn truy cập Ransomware Protection, bạn được giới thiệu vào tính năng này. Nhấp **OK, TÔI ĐÃ HIỂU** để tiếp tục.

Các cuộc tấn công được phát hiện trong vòng 90 ngày gần nhất được hiển thị Để xem chi tiết về loại ransomware được phát hiện, đường dẫn của phần mềm độc hại, hoặc đã xử lý đã thành công, chỉ cần nhấp vào nó.

14.3. Thêm quy trình để loại trừ

Bạn có thể cấu hình quy tắc loại trừ cho các ứng dụng mà bạn tin tưởng để tính năng PHÒNG CHỐNG TẤN CÔNG NÂNG CAO không chặn chúng nếu chúng có các hành động tương tự như phần mềm độc hại.

Để bắt đầu thêm các quy trình vào danh sách Loại trừ phòng chống tấn công nâng cao:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **PHÒNG THỦ MỐI ĐE DỌA NÂNG CAO**, nhấp **Thiết lập**.
3. Trong khu vực **Loại trừ**, nhấp vào **Thêm ứng dụng vào loại trừ**.
4. Tìm và chọn ứng dụng bạn muốn loại trừ, sau đó nhấp **OK**.

   Để xóa một mục khỏi danh sách, nhấp vào lựa chọn **Xóa** ở bên cạnh.

14.4. Khai thác được phát hiện

Một cách được các tin tặc sử dụng để xâm nhập hệ thống, là tận dụng các lỗi hoặc lỗ hổng cụ thể có trong phần mềm máy tính (ứng dụng hoặc plugin) và phần cứng. Để đảm bảo rằng máy tính của bạn tránh xa các cuộc tấn công như vậy, thường lan truyền rất nhanh, Bitdefender sử dụng các công nghệ chống khai thác mới nhất.

Bật hoặc tắt phát hiện khai thác

Để bật hoặc tắt phát hiện khai thác:

- Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
- Trong cửa sổ **PHÒNG THỦ MỐI ĐE DỌA NÂNG CAO**, nhấp **Thiết lập**.
- Nhấp vào công tắc bật hoặc tắt tương ứng.

> **Ghi chú**
> Tùy chọn phát hiện Khai thác được bật theo mặc định.

15. NGĂN CHẶN MỐI ĐE DỌA TRÊN MẠNG

Bitdefender Ngăn chặn mối đe dọa trực tuyến đảm bảo duyệt web an toàn bằng cách cảnh báo cho bạn về các trang web độc hại.

Bitdefender cung cấp ngăn chặn mối đe dọa trực tuyến thời gian thực cho:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Để định cấu hình cài đặt Ngăn chặn mối đe dọa trực tuyến:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **NGĂN CHẶN MỐI ĐE DỌA TRỰC TUYẾN**, nhấp **Thiết lập**.

Trong cửa sổ **BẢO VỆ Web**, nhấn vào chuyển để bật hoặc tắt:

- Tính năng Ngăn chặn tấn công web ngăn chặn các mối đe dọa đến từ internet, bao gồm cả ổ đĩa- bằng cách tải xuống.
- Cố vấn tìm kiếm, một thành phần đánh giá mức độ an toàn các kết quả truy vấn tìm kiếm của bạn và các liên kết được đăng trên các trang mạng xã hội bằng cách đặt một biểu tượng bên cạnh mỗi kết quả tìm kiếm:

  Bạn không nên truy cập vào trang web này.

  Trang web này có thể chứa nội dung nguy hiểm. Hãy thận trọng nếu bạn quyết định truy cập vào nó.

  Đây là một trang an toàn để truy cập.

  Cố vấn tìm kiếm đánh giá các kết quả tìm kiếm từ các công cụ tìm kiếm web sau đây:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Cố vấn tìm kiếm đánh giá các liên kết được đăng trên các dịch vụ mạng xã hội trực tuyến sau đây:

- Facebook
- Twitter

- Quét trang web mã hóa.

  Các cuộc tấn công phức tạp hơn có thể sử dụng truy cập web trên giao thức an toàn để đánh lừa nạn nhân của chúng. Do đó, chúng tôi khuyên bạn nên tiếp tục bật tùy chọn quét web được mã hóa.

- Bảo vệ chống gian lận.

- Bảo vệ chống Lừa đảo.

Trong cửa sổ **Ngăn chặn mối đe dọa mạng**, bạn có tùy chọn **Ngăn chặn mối đe dọa mạng** . Để giữ cho máy tính của bạn tránh xa các cuộc tấn công được thực hiện bởi phần mềm độc hại phức tạp (chẳng hạn như ransomware) thông qua việc khai thác lỗ hổng bảo mật, hãy bật tùy chọn này.

Bạn có thể tạo một danh sách các trang web, tên miền và địa chỉ IP sẽ được bỏ qua bởi các công cụ chống đe dọa, chống lừa đảo và chống lừa đảo của Bitdefender. Danh sách chỉ nên chứa các trang web, tên miền và địa chỉ IP mà bạn hoàn toàn tin tưởng.

Để cấu hình và quản lý trang web, tên miền và địa chỉ IP bằng tính năng Ngăn chặn mối đe dọa trực tuyến được cung cấp bởi Bitdefender:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **NGĂN CHẶN MỐI ĐE DỌA TRỰC TUYẾN**, nhấp **Thiết lập**.
3. Nhập vào trường tương ứng tên của trang web, tên miền hoặc địa chỉ IP bạn muốn thêm vào ngoại lệ, sau đó nhấp vào **THÊM** .

   Để xóa khỏi danh sách, chọn mục muốn xoá và sau đó nhấp vào **Xóa** .

   Nhấp **Lưu lại** để lưu các thay đổi và đóng cửa sổ.

15.1. Bitdefender cảnh báo trong trình duyệt

Bất cứ khi nào bạn cố gắng truy cập vào một trang web bị phân loại là không an toàn, trang web sẽ bị chặn và một cảnh báo được hiển thị trong trình duyệt của bạn.

Các trang web có chứa các thông tin như URL của trang web và các mối đe dọa được phát hiện.

Bạn cần quyết định làm gì tiếp theo. Có những lựa chọn sau:

- Điều hướng khỏi trang web bằng cách nhấp vào **hãy để chúng tôi giữ an toàn**
- Tiếp tục với trang web, bất chấp cảnh báo, bằng cách nhấp vào **Tôi hiểu các rủi ro, hãy đưa tôi đến đó bằng mọi cách** .
- Nếu bạn chắc chắn rằng trang web được phát hiện là an toàn, hãy nhấp vào **NHẬP** để thêm nó vào ngoại lệ. Chúng tôi khuyên bạn chỉ nên thêm các trang web mà bạn hoàn toàn tin tưởng.

16. LỖ HỔNG

Một bước quan trọng cần thực hiện để bảo vệ cho máy của bạn khỏi các nguy cơ bị lây nhiễm mã độc là cập nhật thường xuyên các bản vá lỗi mới nhất cho hệ điều hành và ứng dụng của bạn thường xuyên. Hơn nữa, để ngăn chặn truy cập vật lý trái phép vào máy tính của bạn, mật khẩu mạnh (mật khẩu khó đoán được) phải được cấu hình cho mỗi tài khoản người dùng Windows và cũng cho các mạng Wi-Fi mà bạn kết nối.

Bitdefender tự động kiểm tra lỗ hổng hệ thống và đưa ra cảnh báo. Nó quét sau:

- các ứng dụng đã lỗi thời trên máy tính của bạn.
- thiếu bản cập nhật Windows.
- tài khoản người dùng Windows có mật khẩu yếu.
- các mạng không dây và định tuyến không được an toàn.

Bitdefender cung cấp hai cách dễ dàng để sửa chữa các lỗ hổng bảo mật hệ thống của bạn:

- Bạn có thể quét hệ thống để tìm các lỗ hổng bảo mật và sửa chữa chúng từng bước bằng cách sử dụng **Quét lỗ hổng bảo mật**
- Bằng việc giám sát tự động lỗ hổng bảo mật, bạn có thể kiểm tra và sửa chữa lỗ hổng được phát hiện trong cửa sổ Thông báo.

Bạn nên kiểm tra và sửa chữa các lỗ hổng hệ thống mỗi một hoặc hai tuần.

16.1. Quét hệ thống của bạn để tìm các lỗ hổng bảo mật

Để phát hiện các lỗ hổng hệ thống, Bitdefender yêu cầu kết nối internet.

Để quét hệ thống của bạn để tìm các lỗ hổng bảo mật:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **LỖ HỔNG BẢO MẬT**, nhấp vào **Quét lỗ hổng**.
3. Lần đầu tiên bạn truy cập quét lỗ hổng bảo mật, bạn sẽ được giới thiệu tính năng này. Nhấp vào **BẮT ĐẦU QUÉT** để tiếp tục và sau đó đợi Bitdefender kiểm tra lỗ hổng hệ thống của bạn.
   - **Cập nhật các bản vá cho Windows**

Một danh sách các bản cập nhật Windows quan trọng chưa được cài đặt trên máy tính của bạn được hiển thị. Khởi động lại hệ thống có thể được yêu cầu để cho phép Bitdefender hoàn tất cài đặt.

Xin lưu ý rằng có thể mất một lúc để cài đặt các bản cập nhật.

- **Cập nhật ứng dụng**

  Để xem thông tin về ứng dụng cần được cập nhật, nhấp vào tên của nó từ danh sách.

  Nếu một ứng dụng không cập nhật, hãy nhấp vào **TẢI XUỐNG PHIÊN BẢN MỚI** để tải xuống phiên bản mới nhất.

- **Tài khoản Windows không bảo mật**

  Bạn có thể nhìn thấy danh sách các tài khoản đăng nhập Windows đã được tạo trên máy và mức độ bảo mật của mật khẩu tương ứng.

  Bạn có thể lựa chọn giữa yêu cầu người dùng thay đổi mật khẩu ở lần đăng nhập tiếp theo hoặc thay đổi mật khẩu ngay lập tức.

  Để đặt mật khẩu mới cho hệ thống của bạn, chọn **Thay đổi mật khẩu ngay** .

  Để tạo mật khẩu mạnh, chúng tôi khuyên bạn nên sử dụng kết hợp chữ hoa và chữ thường, số và ký tự đặc biệt (chẳng hạn như # , $ hoặc @).

- **Mạng Wi-Fi và bộ định tuyến**

  Để tìm hiểu thêm về mạng không dây và bộ định tuyến bạn đang kết nối, nhấp vào tên của nó từ danh sách. Nếu bạn nên đặt mật khẩu mạnh hơn cho mạng gia đình của mình, hãy đảm bảo rằng bạn làm theo hướng dẫn của chúng tôi để bạn có thể duy trì kết nối mà không phải lo lắng về quyền riêng tư của mình.

  Khi những gợi ý khác đều có sẵn, hãy làm theo các hướng dẫn được cung cấp để đảm bảo mạng gia đình của bạn vẫn an toàn khỏi những nguy cơ rò rỉ thông tin.

16.2. Sử dụng Tự động giám sát lỗ hổng bảo mật

Bitdefender thường xuyên quét hệ thống của bạn để tìm các lỗ hổng bảo mật tại nền và lưu hồ sơ của các vấn đề được phát hiện trong cửa sổ Thông báo.

Để kiểm tra và sửa chữa các vấn đề được phát hiện:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.
2. Trong **Tất cả các** Tab, chọn thông báo về Quét lỗ hổng bảo mật.
3. Bạn có thể xem thông tin chi tiết về các lỗ hổng hệ thống phát hiện. Tùy thuộc vào vấn đề, để sửa chữa một lỗ hổng cụ thể tiến hành như sau:
   - Nếu có bản cập nhật Windows, hãy nhấp vào **Cài đặt**.
   - Nếu tự động cập nhật của Windows bị vô hiệu hóa, kích **Enable**.
   - Nếu một ứng dụng là lỗi thời, hãy chọn **CẬP NHẬT NGAY** để tìm một liên kết đến trang web của nhà cung cấp, nơi bạn có thể cài đặt phiên bản mới nhất của ứng dụng đó.
   - Nếu một tài khoản người dùng Windows có mật khẩu yếu, nhấn **Đổi mật khẩu** để buộc người dùng phải thay đổi mật khẩu ở lần đăng nhập tiếp theo hoặc thay đổi ngay tại chỗ. Để có mật khẩu có độ bảo mật cao, hãy sử dụng kết hợp cả chữ hoa và chữ thường, số và các ký tự đặc biệt (ví dụ như #, $ hoặc @).
   - Nếu tính năng Tự động chạy của Windows được kích hoạt, nhấn **Fix** để vô hiệu hóa nó.
   - Nếu định tuyến bạn đã cấu hình thiết lập một mật khẩu yếu, nhấp **ĐỔI MẬT KHẨU** để truy cập vào giao diện của nó từ nơi mà bạn có thể thiết lập một mật khẩu mạnh.
   - Nếu mạng bạn đang kết nối có lỗ hổng bảo mật đó có thể khiến hệ thống của bạn có nguy cơ, nhấn **ĐỔI CÀI ĐẶT WIFI**.

Để cấu hình các thiết lập theo dõi lỗ hổng bảo mật:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **LỖ HỔNG BẢO MẬT**, nhấp vào **Cài đặt** .

> **!** **Quan trọng**
> Để tự động thông báo về các lỗ hổng hệ bảo mật hệ thống hoặc ứng dụng, bật lựa chọn **Lỗ hổng bảo mật**.

3. Chọn các lỗ hổng hệ thống bạn muốn được kiểm tra thường xuyên bằng cách sử dụng các lựa chọn tương ứng.

   Cập nhật Windows
   Kiểm tra xem hệ điều hành Windows của bạn có các bản cập nhật bảo mật quan trọng mới nhất từ Microsoft chưa.

Cập nhật ứng dụng

Kiểm tra xem các ứng dụng được cài đặt trên hệ thống của bạn có cập nhật không. Ứng dụng lỗi thời có thể bị khai thác bởi phần mềm độc hại, làm cho máy tính của bạn dễ bị tấn công từ bên ngoài.

Mật khẩu người dùng

Kiểm tra xem các mật khẩu của các tài khoản Windows và định tuyến được cấu hình trên hệ thống là dễ đoán hay không. Thiết lập mật khẩu khó đoán (mật khẩu mạnh) làm cho tin tặc rất khó đột nhập vào hệ thống của bạn. Một mật khẩu có độ bảo mật cao sử dụng kết hợp cả chữ hoa và chữ thường, số và các ký tự đặc biệt (ví dụ như #, $ hoặc @).

Tự chạy

Kiểm tra tình trạng của tính năng Tự động chạy trong Windows. Tính năng này cho phép các ứng dụng sẽ được tự động chạy từ đĩa CD, DVD, USB hoặc các thiết bị gắn ngoài khác.

Một số loại phần mềm độc hại sử dụng tính năng chạy Tự động để lây lan tự động từ thiết bị đa phương tiện vào máy tính. Đây là lý do tại sao bạn nên vô hiệu hóa tính năng Windows này.

Cố vấn An ninh Wi-Fi

Kiểm tra nếu các nhà mạng không dây bạn đã kết nối đến là an toàn hay không, và nếu nó có lỗ hổng. Ngoài ra, kiểm tra xem mật khẩu của định tuyến nhà của bạn đủ mạnh, và làm thế nào bạn có thể làm cho nó an toàn hơn.

Hầu hết các mạng không dây không được bảo vệ là không an toàn, do đó tin tặc có thể truy cập đến các hoạt động cá nhân của bạn.

Ghi chú

Nếu bạn tắt giám sát một lỗ hổng cụ thể, các vấn đề liên quan sẽ không còn được ghi nhận trong cửa sổ Thông báo.

16.3. Cố vấn An ninh Wi-Fi

Trong khi trên đường đi, làm việc trong một quán cà phê, hoặc chờ đợi ở sân bay, kết nối với một mạng không dây công cộng để thực hiện thanh toán, kiểm tra e-mail hoặc các tài khoản mạng xã hội có thể là giải pháp nhanh nhất. Các mã độc cố gắng để chiếm quyền điều khiển dữ liệu cá nhân của bạn có thể có mặt ở đó, xem cách rò rỉ thông tin qua mạng.

Dữ liệu cá nhân có nghĩa là các mật khẩu và tên người dùng bạn sử dụng để có được quyền truy cập vào tài khoản trực tuyến của bạn, chẳng hạn như email, tài khoản ngân hàng, tài khoản truyền thông xã hội, mà còn là thông điệp bạn gửi đi.

Thông thường, các mạng không dây công cộng có nhiều khả năng không an toàn vì chúng không yêu cầu mật khẩu lúc đăng nhập, và nếu họ làm, mật mã có thể được cung cấp cho bất kỳ ai muốn kết nối. Hơn nữa, chúng có thể là mạng độc hại hoặc mạo danh, đại diện cho một mục tiêu cho tội phạm mạng.

Để bảo vệ bạn khỏi những mối nguy hiểm của các điểm truy cập không dây không an toàn hoặc không được mã hoá, Bitdefender Wi- Fi Security Advisor phân tích mức độ bảo mật của mạng không dây và khi cần thiết, nó rất khuyến khích bạn sử dụng Bitdefender VPN

Bitdefender Wifi Cố vấn An ninh cung cấp thông tin về:

- mạng Wifi gia đình
- mạng Wifi văn phòng
- mạng Wifi công cộng

16.3.1. Bật hoặc tắt các thông báo Cố Vấn An Ninh Wifi

Để bật hoặc tắt các thông báo của Cố vấn an ninh Wi- Fi:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **LỖ HỔNG BẢO MẬT**, nhấp vào **Cài đặt** .
3. Trong cửa sổ **Cài đặt** , bật hoặc tắt tùy chọn **Cố vấn bảo mật Wi-Fi** .

16.3.2. Cấu hình mạng Wifi gia đình

Để bắt đầu cấu hình mạng gia đình của bạn:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong mô đun**LỖ HỔNG BẢO MẬT**, chọn **Bảo mật Wifi**.
3. Trong tab **Wi-Fi gia đình** , nhấp vào **CHỌN WI-FI gia đình**.

   Một danh sách các mạng không dây, bạn kết nối cho đến khi được hiển thị.
4. Chỉ vào mạng gia đình của bạn, và sau đó nhấp vào **CHỌN**.

Nếu một mạng gia đình được coi là không được bảo mật hoặc không an toàn, khuyến cáo cấu hình không có bảo đảm hoặc không an toàn để cải thiện an ninh của nó được hiển thị.

Để loại bỏ các mạng không dây mà bạn đã thiết lập như là một mạng gia đình, nhấp vào nút **XÓA**.

Để thêm mạng không dây mới làm mạng gia đình, hãy nhấp vào **Chọn mạng gia đình mới** .

16.3.3. Cấu hình mạng Wifi văn phòng

Để bắt đầu cấu hình mạng văn phòng của bạn:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong mô đun**LỖ HỔNG BẢO MẬT**, chọn **Bảo mật Wifi**.
3. Trong tab **Wi-Fi văn phòng** , nhấp vào **CHỌN WI-FI văn phòng**.

   Một danh sách các mạng không dây, bạn kết nối cho đến khi được hiển thị.
4. Trỏ vào mạng văn phòng của bạn, và sau đó nhấp vào **CHỌN**.

Nếu một mạng văn phòng được coi là không bảo mật hoặc không an toàn, các khuyến nghị cấu hình để cải thiện bảo mật của nó sẽ được hiển thị.

Để xóa mạng không dây mà bạn đã đặt làm mạng văn phòng, hãy nhấp vào **XÓA** .

Để thêm mạng không dây mới làm mạng văn phòng, hãy nhấp vào **Chọn mạng văn phòng mới** .

16.3.4. Wi-Fi công cộng

Trong khi kết nối với một mạng không dây không đảm bảo hoặc không an toàn, hồ sơ Wifi công cộng được kích hoạt. Trong khi đang chạy trong hồ sơ này, Bitdefender Antivirus Plus được thiết lập để tự động thực hiện các cài đặt chương trình sau đây:

- Phòng chống tấn công nâng cao được bật
- Các cài đặt sau từ tính năng Ngăn chặn mối đe dọa trực tuyến được bật:
  - Quét trang web mã hóa
  - Bảo vệ khỏi gian lận

- Bảo vệ khỏi lừa đảo
- Một nút mở Bitdefender Safepay™ có sẵn. Trong trường hợp này, việc bảo vệ Hotspot cho mạng không an toàn được kích hoạt theo mặc định.

16.3.5. Kiểm tra thông tin về mạng Wifi

Để kiểm tra thông tin về các mạng không dây, bạn thường kết nối tới:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong mô đun**LỖ HỔNG BẢO MẬT**, chọn **Bảo mật Wifi**.
3. Tùy thuộc vào thông tin bạn cần, chọn một trong ba tab, **Wi-Fi gia đình** , **Wi-Fi văn phòng** hoặc **Wi-Fi công cộng** .
4. Nhấn **Xem chi tiết** bên cạnh mạng bạn muốn tìm thông tin thêm về.

Có ba kiểu mạng không dây được lọc bởi tầm quan trọng của chúng, mỗi loại chỉ định bởi một biểu tượng cụ thể:

Wifi là không an toàn - chỉ ra rằng mức độ bảo mật của mạng là thấp. Điều này có nghĩa rằng có một nguy cơ cao để sử dụng nó, và nó không được khuyến khích để thực hiện thanh toán hoặc kiểm tra tài khoản ngân hàng mà không có thêm sự bảo vệ. Trong tình huống như vậy, chúng tôi khuyên bạn sử dụng Bitdefender Safepay ™ với bảo vệ Hotspot cho các mạng không được bảo đảm kích hoạt.

Wifi là không an toàn - chỉ ra rằng mức độ bảo mật của mạng là vừa phải. Điều này có nghĩa rằng có thể có lỗ hổng bảo mật, và nó không được khuyến khích để thực hiện thanh toán hoặc kiểm tra tài khoản ngân hàng mà không có thêm sự bảo vệ. Trong tình huống như vậy, chúng tôi khuyên bạn sử dụng Bitdefender Safepay ™ với bảo vệ Hotspot cho các mạng không được bảo đảm kích hoạt.

Wifi là an toàn - chỉ ra rằng mạng bạn sử dụng là an toàn. Trong trường hợp này, bạn có thể sử dụng dữ liệu nhạy cảm cho việc thực hiện các hoạt động trực tuyến.

Bằng cách nhấp vào liên kết **Xem chi tiết** trong khu vực của mỗi mạng, các chi tiết sau đây được hiển thị:

- **Bảo vệ** - ở đây bạn có thể xem nếu mạng được chọn có được bảo vệ hay không. Mạng không được mã hóa có thể làm cho dữ liệu bạn sử dụng bị phát tán.
- **Loại Mã hóa** - ở đây bạn có thể xem các loại mã hóa được sử dụng bởi các mạng được chọn. Một số loại mã hóa có thể không an toàn. Vì vậy, chúng

tôi đề nghị bạn kiểm tra thông tin về các loại mã hóa hiển thị để chắc chắn rằng bạn được bảo vệ khi lướt web.

- **Kênh/Tần số** - ở đây bạn có thể xem các kênh tần số được sử dụng bởi các mạng được chọn.
- **Mật khẩu mạnh** - ở đây bạn có thể xem cách mật khẩu mạnh là. Lưu ý rằng các mạng đã đặt mật khẩu yếu là một mục tiêu để tội phạm mạng khai thác.
- **Loại đăng nhập** - ở đây bạn có thể xem nếu mạng được lựa chọn được bảo vệ bằng mật khẩu hay không. Nó là rất khuyến khích để kết nối duy nhất với các mạng đã thiết lập mật khẩu mạnh.
- **Loại Xác Thực** - ở đây bạn có thể xem các loại xác thực được sử dụng bởi các mạng được chọn.

17. TẬP TIN AN TOÀN

Ransomware là một phần mềm độc hại tấn công vào hệ thống dễ bị tổn thương bằng cách khóa chúng, và yêu cầu tiền chuộc để cho phép người dùng lấy lại sự kiểm soát hệ thống của mình. Phần mềm độc hại này hoạt động thông minh bằng cách hiển thị các tin nhắn giả hoảng sợ cho người sử dụng, thúc giục phải tiến hành thanh toán.

Các tập tin nhiễm có thể lây lan qua thư rác điện tử, bằng cách tải file đính kèm, hoặc bằng cách truy cập các trang web bị lây nhiễm và cài đặt các ứng dụng độc hại mà không để cho người dùng biết những gì đang xảy ra trên hệ thống của mình.

Ransomware có thể có một trong các hành vi sau đây ngăn chặn người sử dụng truy cập vào hệ thống của mình:

- Mã hóa các tập tin nhạy cảm và riêng tư mà không đưa ra khả năng giải mã cho đến khi một số tiền chuộc được trả bởi các nạn nhân.
- Khóa màn hình của máy tính và hiển thị một thông báo yêu cầu tống tiền. Trong trường hợp này, không có tập tin được mã hóa, chỉ có người sử dụng buộc phải tiến hành thanh toán tiền chuộc.
- Chặn các ứng dụng đang chạy.

Với Bitdefender Tập Tin An toàn, bạn có thể được bảo vệ khỏi các cuộc tấn công ransomware đến các tập tin cá nhân, như tài liệu, hình ảnh hoặc phim.

Ghi chú
Phòng chống Tấn Công Nâng cao và Tập Tin An Toàn là hai lớp bảo vệ chống lại ransomware. PHÒNG CHỐNG TẤN CÔNG NÂNG CAO là một tính năng ngăn chặn các cuộc tấn công ransomware vào các khu vực quan trọng của hệ thống, trong khi Tập Tin An Toàn đảm bảo không có tệp tin quan trọng trên máy tính của bạn được mã hóa.

17.1. Bật hoặc tắt Tập Tin An Toàn

Để bật hoặc tắt tính năng Tập Tin An Toàn:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **TẬP TIN AN TOÀN**, bật hoặc tắt

Mỗi khi một ứng dụng sẽ cố gắng truy cập vào một tập tin được bảo vệ, một bảng Bitdefender được hiển thị. Bạn có thể cho phép hoặc chặn truy cập

Ghi chú
Tính năng Tập Tin An Toàn sẽ không được bật theo mặc định.

17.2. Bảo vệ tập tin cá nhân từ các cuộc tấn công ransomware

Nếu bạn muốn giải quyết các tập tin cá nhân đến một nơi trú ẩn:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **TẬP TIN AN TOÀN**, nhấp vào **Các thư mục được bảo vệ**
3. Lần đầu tiên bạn truy cập Các thư mục được bảo vệ, bạn sẽ được giới thiệu vào tính năng này. Nhấp vào **BẢO VỆ THƯ MỤC** để tiếp tục.
4. Chọn thư mục bạn muốn bảo vệ, sau đó nhấp **OK**

   Để thêm các thư mục khác, hãy nhấp vào liên kết **Bảo vệ nhiều thư mục hơn**. Cách khác, kéo thư mục vào cửa sổ này.

Theo mặc định, các thư mục Pictures, Videos, Documents và Music được bảo vệ chống lại các cuộc tấn công đe dọa. Dữ liệu cá nhân được lưu trữ trong các dịch vụ lưu trữ trực tuyến như Box, Dropbox, Google Drive và OneDrive cũng được bao gồm trong môi trường được bảo vệ, miễn là các ứng dụng của chúng được cài đặt trên hệ thống.

Để tránh làm chậm hệ thống, chúng tôi khuyên bạn nên thêm tối đa 30 thư mục hoặc lưu nhiều tệp trong một thư mục

Ghi chú
Thư mục tùy chỉnh có thể được bảo vệ chỉ cho người dùng hiện tại. Các tập tin hệ thống và ứng dụng không thể được thêm vào trường hợp ngoại lệ.

17.3. Định cấu hình quyền truy cập ứng dụng

Những ứng dụng cố gắng thay đổi hoặc xóa các tập tin được bảo vệ có thể được gắn thẻ là có khả năng gây mất an toàn và sẽ bị bổ sung vào danh sách các ứng dụng bị chặn. Nếu ứng dụng đó bị chặn và bạn chắc chắn rằng hành vi của nó là bình thường, bạn có thể cho phép nó bằng cách làm theo các bước sau:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **TỆP AN TOÀN** , nhấp vào **Truy cập ứng dụng** .

3. Các ứng dụng đã yêu cầu thay đổi tệp trong thư mục được bảo vệ của bạn đã được liệt kê. Bật nút gạt bên cạnh ứng dụng mà bạn chắc chắn là an toàn.

Trong cùng một cửa sổ, bạn có thể vô hiệu hoá mã độc tống tiền bảo vệ cho các ứng dụng cụ thể bằng cách tắt gạt tương ứng.

Nếu bạn muốn thêm các ứng dụng mới vào danh sách, hãy nhấp vào liên kết **Thêm ứng dụng mới vào danh sách** .

17.4. Bảo vệ lúc khởi động

Nhiều ứng dụng độc hại được thiết lập để chạy khi khởi động hệ thống, một thực tế có thể làm hỏng máy tính một cách nghiêm trọng. Bitdefender Thời gian khởi động quét tất cả các vùng bảo vệ hệ thống quan trọng trước khi tất cả các tập tin đang được nạp, mà không ảnh hưởng nhiều tới hệ thống.

Để vô hiệu hóa bảo vệ lúc khởi động:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **TỆP TIN AN TOÀN**, nhấp vào **Cài đặt** .
3. Tắt **Bảo vệ khi khởi động** .

Ghi chú

Các ứng dụng được thêm vào mục loại trừ cũng sẽ được quét và được xử lý phù hợp.

18. KHẮC PHỤC RANSOMWARE

Bitdefender Tính năng Khắc phục Ransomware sao lưu các tệp của bạn như tài liệu, hình ảnh, video hoặc nhạc để đảm bảo rằng chúng được bảo vệ khỏi bị hư hỏng hoặc bị mất trong trường hợp mã hóa phần mềm ransomware. Mỗi lần phát hiện tấn công ransomware, Bitdefender sẽ chặn tất cả các quy trình liên quan đến cuộc tấn công và bắt đầu quá trình khắc phục. Bằng cách này, bạn sẽ có thể khôi phục nội dung của toàn bộ tệp mà không phải trả bất kỳ khoản tiền chuộc nào bị yêu cầu.

18.1. Bật hoặc tắt chức năng Khắc phục Ransomware

Bật hoặc tắt chức năng Khắc phục Ransomware

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong ngăn **KHẮC PHỤC RANSOMWARE**, hãy bật hoặc tắt công tắc.

> **Ghi chú**
> Để đảm bảo rằng các tệp của bạn được bảo vệ chống lại phần mềm ransomware, chúng tôi khuyên bạn nên bật tính năng Khắc phục Ransomware.

18.2. Bật hoặc tắt tính năng khôi phục tự động

Khôi phục tự động đảm bảo rằng các tệp của bạn được tự động khôi phục trong trường hợp mã hóa phần mềm ransomware.

Bật hoặc tắt tính năng khôi phục tự động

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **KHẮC PHỤC RANSOMWARE**, nhấp vào **Cài đặt**.
3. Bật hoặc tắt khóa chuyển đổi **Tự động khôi phục**.

18.3. Xem các tệp đã được khôi phục tự động

Khi tùy chọn **Tự động khôi phục** được bật, Bitdefender sẽ tự động khôi phục các tệp đã bị mã hóa bằng phần mềm ransomware. Bằng cách này, bạn có thể tận hưởng trải nghiệm máy tính mà không phải lo lắng khi biết rằng các tệp của mình an toàn.

Để xem các tệp được khôi phục tự động:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.

2. Trong tab **Tất cả**, chọn thông báo liên quan đến hành vi ransomware mới nhất được khắc phục và sau đó nhấp vào **Tệp được khôi phục**.

   Danh sách với các tập tin được khôi phục được hiển thị. Tại đây bạn cũng có thể xem vị trí nơi các tệp của bạn đã được khôi phục.

18.4. Khôi phục các tệp được mã hóa theo cách thủ công

Trong trường hợp bạn phải khôi phục thủ công các tệp đã được mã hóa bằng phần mềm ransomware, hãy làm theo các bước sau:

1. Nhấp vào **Thông báo** trên menu điều hướng trên giao diện Bitdefender.
2. Trong tab **Tất cả**, chọn thông báo liên quan đến hành vi ransomware mới nhất được phát hiện và sau đó nhấp vào **Tệp được mã hóa**.
3. Danh sách với các tập tin được mã hóa được hiển thị.

   Nhấp vào **FILOVER FILES** để tiếp tục.
4. Trong trường hợp toàn bộ hoặc một phần của quá trình khôi phục không thành công, bạn phải chọn vị trí lưu các tệp đã giải mã. Nhấp vào **RESTORE LOCATION** , sau đó chọn vị trí trên PC của bạn.
5. Một cửa sổ xác nhận xuất hiện.

   Nhấp vào **HOÀN THÀNH** để kết thúc quá trình khôi phục.

Các tệp có các phần mở rộng sau có thể được khôi phục trong trường hợp chúng được mã hóa:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

18.5. Thêm ứng dụng vào ngoại lệ

Bạn có thể cấu hình các quy tắc ngoại lệ cho các ứng dụng đáng tin cậy để các tính năng Khắc phục Ransowmare không chặn chúng nếu chúng thực hiện các hành động giống như ransomware.

Để thêm ứng dụng vào danh sách ngoại lệ Khắc phục Ransomware:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **KHẮC PHỤC RANSOMWARE**, nhấp vào **Ngoại lệ**.
3. Để bắt đầu thêm ứng dụng vào danh sách, hãy nhấp vào **Thêm ứng dụng mới vào danh sách** .

19. QUẢN LÝ MẬT KHẨU BẢO VỆ TÀI KHOẢN CỦA BẠN

Chúng ta sử dụng máy tính của mình để mua sắm trực tuyến hoặc thanh toán hóa đơn, để kết nối với mạng xã hội hoặc đăng nhập ứng dụng chat.

Nhưng như mọi người đều biết, không phải luôn dễ dàng để nhớ được mật khẩu!

Và nếu chúng ta không cẩn thận trong khi duyệt web trực tuyến, thông tin cá nhân của chúng ta, chẳng hạn như địa chỉ e-mail, tài khoản tin nhắn tức thời chat hoặc dữ liệu thẻ tín dụng có thể bị lấy cắp.

Để giữ mật khẩu hoặc dữ liệu cá nhân của bạn trên một tờ giấy hoặc trong máy tính có thể nguy hiểm vì chúng có thể bị truy cập và sử dụng bởi những người ăn cắp và sử dụng thông tin đó. Và việc nhớ từng mật khẩu mà bạn đã thiết lập cho các tài khoản trực tuyến hoặc trang web ưa thích của bạn không phải là một nhiệm vụ dễ dàng.

Vậy, có cách nào để đảm bảo rằng chúng ta tìm thấy mật khẩu của mình khi cần? Và chúng ta có thể yên tâm rằng mật khẩu bí mật của mình là luôn luôn an toàn?

Quản lý mật khẩu giúp bạn theo dõi các mật khẩu của mình, bảo vệ sự riêng tư của bạn và cung cấp một trải nghiệm duyệt web an toàn.

Sử dụng một mật khẩu chủ để truy cập thông tin của bạn, Quản lý mật khẩu cho bạn công cụ đơn giản để giữ mật khẩu của bạn an toàn trong Ví.

Để cung cấp bảo vệ tốt nhất cho các hoạt động trực tuyến của bạn, Quản lý mật khẩu tích hợp với Bitdefender Safepay™ để cung cấp một giải pháp thống nhất đối phó với việc dữ liệu cá nhân của bạn có thể bị tổn hại theo nhiều cách.

Quản lý mật khẩu bảo vệ thông tin cá nhân sau đây:

- Thông tin cá nhân, chẳng hạn như địa chỉ e-mail hoặc số điện thoại
- Thông tin đăng nhập cho các trang web
- Thông tin tài khoản ngân hàng hoặc số thẻ tín dụng
- Các tài khoản e-mail
- Mật khẩu cho ứng dụng
- Mật khẩu cho các mạng Wi-Fi

19.1. Tạo một cơ sở dữ liệu Ví mới

Ví Bitdefenderlà nơi mà bạn có thể lưu trữ dữ liệu cá nhân của bạn. Để có trải nghiệm trình duyệt dễ dàng hơn, bạn cần phải tạo một cơ sở dữ liệu Ví như sau:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Tạo Ví mới**.
3. Nhấp vào **Tạo mới**.
4. Nhập các thông tin cần thiết vào các trường tương ứng.
   - Nhãn Ví - Đặt một tên duy nhất cho cơ sở dữ liệu Ví của bạn
   - Mật khẩu chính - nhập mật khẩu cho Ví của bạn
   - Nhập lại mật khẩu - nhập lại mật khẩu mà bạn thiết lập.
   - Gợi ý - gõ một gợi ý để nhớ mật khẩu.
5. Nhấp **Tiếp tục**.
6. Tại bước này, bạn có thể chọn để lưu trữ thông tin của bạn trong đám mây. Nếu bạn chọn Đống ý, thông tin ngân hàng sẽ vẫn được lưu trữ cục bộ trên thiết bị của bạn. Chọn tùy chọn mong muốn, sau đó nhấp vào **Tiếp tục**.
7. Chọn trình duyệt web bạn muốn nhập thông tin từ.
8. Nhấp vào **Kết thúc**.

19.2. Nhập một cơ sở dữ liệu có sẵn

Để nhập dữ liệu ví để lưu trữ:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Tạo Ví mới**.
3. Nhấp vào **TỪ MỤC TIÊU**.
4. Duyệt tới vị trí trên thiết bị của bạn nơi bạn muốn lưu dữ liệu ví tiền, và sau đó chọn một tên cho nó.
5. Nhấn **Mở**.
6. Đặt tên cho Ví của bạn và nhập mật khẩu được chỉ định khi nó được tạo ở nơi đầu tiên.

7. Nhấp vào **NHẬP**.
8. Chọn các chương trình mà bạn muốn Ví sẽ nhập thông tin xác thực, sau đó là nút **Hoàn tất** .

19.3. Xuất khẩu cơ sở dữ liệu Ví bảo mật

Để xuất khẩu cơ sở dữ liệu Ví bảo mật

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Ví của tôi**.
3. Nhấp vào biểu tượng ⋮ trên ví dụ bạn muốn, sau đó chọn **Xuất**
4. Tìm kiếm vị trí dữ liệu ví của bạn và chọn nó (tập tin .db).
5. Nhấp chuột vào **Lưu**.

> **Ghi chú**
> Bạn cần phải mở Ví để có tùy chọn **Xuất**
> Nếu ví bạn cần xuất đã bị khóa, hãy nhấp vào **TỰ ĐỘNG TẠO VÍ** và nhập mật khẩu được chỉ định khi nó được tạo ở nơi đầu tiên.

19.4. Đồng bộ hóa các ví mình trong đám mây

Để bật hoặc tắt đồng bộ ví trong đám mây:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Ví của tôi**.
3. Nhấp vào biểu tượng ⋮ trên ví bạn muốn, sau đó chọn **Cài đặt** .
4. Chọn tùy chọn mong muốn trong cửa sổ hiện ra, sau đó nhấp vào **Lưu** .

> **Ghi chú**
> Bạn cần phải mở Ví để có tùy chọn **Xuất**
> Nếu ví bạn cần đồng bộ hóa bị khóa, hãy nhấp vào**TỰ ĐỘNG TẠO VÍ** và nhập mật khẩu được chỉ định khi nó được tạo ở nơi đầu tiên.

19.5. Quản lý tài khoản với Ví bảo mật

Để quản lý mật khẩu của bạn:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .

2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Ví của tôi**.
3. Chọn cơ sở dữ liệu Ví mong muốn, và sau đó nhấp vào **HOẠT ĐỘNG VÍ**.
4. Nhập mật khẩu chủ, và sau đó bấm **OK**.

Một cửa sổ mới xuất hiện. Chọn danh mục bạn muốn từ phần trên của cửa sổ:

- Định danh
- Các trang web
- Ngân hàng
- Email
- Các ứng dụng
- Wi-Fi

Thêm/ chỉnh sửa định danh

- Để thêm một mật khẩu mới, lựa chọn danh mục bạn muốn từ phía trên, nhấp **+Thêm mục**, đưa thông tin vào các trường tương ứng và nhấp nút Lưu lại.
- Để sửa một mục trong bảng, hãy chọn và bấm vào nút **Sửa**.
- Để xóa một qui tắc hãy chọn và bấm vào nút **Xóa**.

19.6. Bật hoặc tắt chức năng bảo vệ Quản lý mật khẩu

Để bật hoặc tắt bảo vệ Quản Lý Mật Khẩu:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun**QUẢN LÝ MẬT KHẨU**, hãy bật hoặc tắt công tắc.

19.7. Quản lý các thiết lập Quản lý mật khẩu

Để cấu hình mật khẩu chủ trong chi tiết:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Thiết lập**.
3. Chọn tab **Thiết lập an ninh**.

Có những lựa chọn sau:

- **Yêu cầu mật khẩu chủ của tôi khi tôi đăng nhập vào thiết bị của mình** - bạn sẽ được nhắc chèn mật khẩu chính khi bạn truy cập thiết bị.
- **Yêu cầu hỏi mật khẩu chính của tôi khi mở trình duyệt và ứng dụng** - bạn sẽ được yêu cầu nhập vào mật khẩu chính khi bạn truy cập vào một trình duyệt hoặc một ứng dụng.
- **Đừng hỏi mật khẩu của tôi** - bạn sẽ không được nhắc nhập mật khẩu khi bạn truy cập máy tính, trình duyệt hoặc ứng dụng.
- **Tự động khóa Ví bảo mật khi tôi rời thiết bị** - bạn sẽ được yêu cầu nhập vào mật khẩu chính của bạn khi bạn quay trở lại thiết bị sau 15 phút.

! **Quan trọng**
Hãy ghi nhớ mật khẩu chủ của bạn hoặc lưu giữ nó tại một nơi an toàn. Nếu bạn quên mật khẩu, bạn sẽ phải cài đặt lại chương trình hoặc liên hệ với hỗ trợ Bitdefender.

Cải thiện kinh nghiệm của bạn

Lựa chọn các trình duyệt hoặc các ứng dụng mà bạn muốn tích hợp với Quản lý mật khẩu:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Thiết lập**.
3. Chọn tab **Plugins**.

   Kiểm tra ứng dụng để sử dụng Trình quản lý mật khẩu và nâng cao trải nghiệm của bạn:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Cấu hình Tự động điền thông tin

Tính năng Tự động điền thông tin làm bạn dễ dàng kết nối với các trang web yêu thích hoặc đăng nhập vào tài khoản trực tuyến của bạn. Lần đầu tiên bạn nhập thông tin đăng nhập và thông tin cá nhân vào trình duyệt web của bạn, nó sẽ tự động được đưa vào Ví.

Để cấu hình thiết lập **Autofill**

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong mô đun **QUẢN LÝ MẬT KHẨU**, nhấp**Thiết lập**.
3. Chọn tab **Thiết lập Autofill**.
4. Cấu hình các tùy chọn sau đây:
   - **Cấu hình Quản lý mật khẩu bảo vệ thông tin định danh của bạn**:
     - **Lưu định danh tự động vào Ví** - thông tin đăng nhập và thông tin định danh khác như chi tiết thẻ tín dụng cá nhân sẽ tự động lưu và cập nhật vào Ví.
     - **Luôn hỏi tôi** - bạn sẽ được hỏi mỗi khi muốn thêm thông tin của bạn vào Ví.
     - **Không lưu, tôi sẽ cập nhật thông tin thủ công** - các thông tin có thể được thêm vào Ví một cách thủ công.
   - **Tự động điền tài khoản đăng nhập**:
     - **Tự động điền tài khoản đăng nhập mọi lúc** - tài khoản đăng nhập được tự động chèn vào trình duyệt.
   - **Tự động điền mẫu**:
     - **Nhắc lựa chọn điền khi tôi truy cập một trang web có mẫu** - một cửa sổ bật ra với các tùy chọn điền vào sẽ xuất hiện mỗi khi Bitdefender phát hiện ra bạn muốn thực hiện một thanh toán trực tuyến hoặc đăng ký.

Quản lý thông tin Quản lý mật khẩu từ trình duyệt của bạn

Bạn có thể dễ dàng quản lý chi tiết Quản Lý Mật Khẩu trực tiếp từ trình duyệt để có tất cả các dữ liệu quan trọng trong tay. Mở rộng Ví Bitdefender được hỗ trợ bởi các trình duyệt sau: Google Chrome, Internet Explorer và Mozilla Firefox, và cũng tích hợp với Safepay.

Để truy cập vào phần mở rộng Ví Bitdefender, mở trình duyệt web của bạn, cho phép mở rộng trên được cài đặt và nhấp biểu tượng trên thanh công cụ.

Phần mở rộng Ví Bitdefender chứa các tùy chọn sau:

- Mở Ví - mở Ví của bạn.
- Đóng Ví - đóng lại.

- Các trang web - sẽ mở ra một trình đơn với tất cả thông tin đăng nhập các trang web được lưu trữ trong Ví. Nhấp **Trang web** để thêm các trang web mới vào danh sách.
- Điền vào mẫu - sẽ mở ra trình đơn có chứa các thông tin mà bạn cần thêm vào. Từ đây bạn có thể thêm dữ liệu mới vào Ví.
- Lấy Mật Khẩu Ngẫu Nhiên - cho phép bạn tạo mật khẩu ngẫu nhiên mà bạn có thể sử dụng cho các tài khoản mới hoặc hiện tại. Nhấn vào **Hiện các thiết lập nâng cao** để tùy độ phức tạp của mật khẩu.
- Cài đặt - mở cửa sổ thiết lập Quản Lý Mật Khẩu.
- Báo cáo vấn đề - báo cáo bất kỳ vấn đề bạn gặp phải với Quản Lý Mật Khẩu Bitdefender.

20. CHỐNG THEO DÕI

Nhiều trang web bạn truy cập sử dụng trình theo dõi để thu thập thông tin về hành vi của bạn, để chia sẻ với các công ty bên thứ ba hoặc để hiển thị quảng cáo phù hợp hơn với bạn. Bằng cách này, chủ sở hữu trang web có thể lấy tiền để cung cấp cho bạn nội dung miễn phí hoặc duy trì hoạt động. Bên cạnh việc thu thập thông tin, trình theo dõi có thể làm chậm trải nghiệm duyệt web của bạn hoặc chiếm nhiều băng thông của bạn.

Với tiện ích Bitdefender Chống theo dõi được kích hoạt trong trình duyệt web của bạn, bạn sẽ tránh bị theo dõi để dữ liệu của bạn được an toàn khi duyệt trực tuyến và tăng tốc thời gian các trang web cần tải.

Tiện ích mở rộng Bitdefender tương thích với các trình duyệt web sau:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Các trình theo dõi chúng tôi phát hiện được nhóm vào các loại sau:

- **Quảng cáo** - được sử dụng để phân tích lưu lượng truy cập trang web, hành vi người dùng hoặc khách truy cập Các mẫu lưu lượng truy cập.
- **Tương tác khách hàng** - được sử dụng để đo lường sự tương tác của người dùng với các hình thức nhập khác nhau như trò chuyện hoặc hỗ trợ.
- **Essential** - được sử dụng để giám sát các chức năng quan trọng của trang web.
- **Phân tích trang web** - được sử dụng để thu thập dữ liệu về việc sử dụng trang web.
- **Phương tiện truyền thông** - được sử dụng để giám sát đối tượng xã hội, hoạt động và sự tham gia của người dùng với các nền tảng truyền thông khác nhau.

20.1. Giao diện Chống theo dõi

Khi tiện ích mở rộng Bitdefender Chống theo dõi được kích hoạt, biểu tượng xuất hiện bên cạnh thanh tìm kiếm trong trình duyệt web của bạn. Mỗi khi bạn truy cập một trang web, một bộ đếm có thể được hiển thị trên biểu tượng, đề cập đến các trình theo dõi được phát hiện và bị chặn. Để xem thêm

chi tiết về các trình theo dõi bị chặn, hãy nhấp vào biểu tượng để mở giao diện. Bên cạnh số lượng trình theo dõi bị chặn, bạn có thể xem thời gian cần thiết để tải trang và các mục mà trình theo dõi phát hiện được. Để xem danh sách các trang web đang theo dõi, nhấp vào danh mục mong muốn.

Để tắt Bitdefender khỏi trình chặn theo dõi trên trang web bạn hiện đang truy cập, hãy nhấp vào **Bảo vệ tạm dừng trên trang web này** . Cài đặt này chỉ áp dụng khi bạn mở trang web và sẽ được trả lại về trạng thái ban đầu khi bạn đóng trang web.

Để cho phép trình theo dõi từ một danh mục cụ thể để theo dõi hoạt động của bạn, hãy nhấp vào hành động mong muốn và sau đó nhấp vào nút tương ứng. Nếu bạn đổi ý, hãy nhấp vào nút tương tự một lần nữa.

20.2. Tắt Bitdefender Chống theo dõi

Để tắt Trình theo dõi Bitdefender:

- Từ trình duyệt web của bạn:
  1. Mở trình duyệt web của bạn.
  2. Nhấp vào biểu tượng bên cạnh thanh địa chỉ trong trình duyệt web của bạn.
  3. Nhấp vào biểu tượng ở góc trên bên phải.
  4. Bật hoặc tắt công tắc tương ứng.

     Biểu tượng Bitdefender chuyển sang màu xám.
- Từ giao diện Bitdefender:
  1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
  2. Trong ngăn **ANTI- TRACKER**, nhấp vào **Cài đặt**.
  3. Bên cạnh trình duyệt web mà bạn muốn tắt tiện ích mở rộng, hãy tắt công tắc tương ứng.

20.3. Cho phép một trang web được theo dõi

Nếu bạn muốn được theo dõi trong khi bạn truy cập một trang web cụ thể, bạn có thể thêm địa chỉ của nó vào các ngoại lệ như sau:

1. Mở trình duyệt web của bạn.

2. Nhấp vào bên cạnh thanh tìm kiếm.
3. Nhấp vào biểu tượng ở góc trên bên phải.
4. Nếu đang ở trang web mà bạn muốn cho vào ngoại lệ, hãy nhấp vào **Thêm trang web hiện tại vào danh sách** .

   Nếu bạn muốn thêm một trang web khác, hãy nhập địa chỉ của nó vào trường tương ứng, sau đó nhấp vào .

21. VPN

Ứng dụng VPN có thể được cài đặt từ sản phẩm Bitdefender của bạn và được sử dụng bất cứ khi nào bạn muốn thêm một lớp bảo vệ bổ sung cho kết nối của bạn. VPN hoạt động như một đường hầm giữa thiết bị của bạn và mạng bạn kết nối, đảm bảo kết nối, mã hóa dữ liệu bằng mã hóa cấp ngân hàng và ẩn địa chỉ IP của bạn ở mọi nơi. Lưu lượng truy cập của bạn được chuyển hướng thông qua một máy chủ chuyên dụng, do đó thiết bị của bạn hầu như không thể xác định thông qua vô số thiết bị khác đang sử dụng dịch vụ của chúng tôi. Hơn nữa, trong khi kết nối với Internet thông qua mạng VPN Bitdefender, bạn có thể truy cập nội dung mà thường bị giới hạn trong các khu vực cụ thể.

Ghi chú
Một số quốc gia thực hiện kiểm duyệt internet và do đó việc sử dụng VPN trên lãnh thổ của họ đã bị cấm theo luật pháp. Để tránh các hậu quả pháp lý, thông tin cảnh báo có thể xuất hiện khi bạn thử sử dụng ứng dụng Bitdefender VPN lần đầu tiên. Bằng cách tiếp tục sử dụng ứng dụng, bạn xác nhận rằng bạn biết về các quy định của quốc gia áp dụng và những rủi ro mà bạn có thể bị phơi bày.

21.1. Cài đặt VPN

Ứng dụng VPN có thể được cài đặt từ giao diện Bitdefender của bạn, như sau:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong hộp **VPN**, nhấp vào **Cài đặt VPN**.
3. Trong cửa sổ với mô tả về ứng dụng VPN, hãy đọc **Thỏa thuận đăng ký**, sau đó nhấp vào **CÀI ĐẶT BITDEFENDER VPN**.

   Chờ vài giây cho đến khi các tệp tin được tải xuống và cài đặt.

   Nếu một ứng dụng VPN khác được phát hiện, chúng tôi khuyên bạn nên gỡ cài đặt nó. Khi cài đặt nhiều giải pháp VPN, bạn có thể gặp phải sự cố hệ thống hoặc các vấn đề chức năng khác.
4. Nhấp vào **MỞ BITDEFENDER VPN** để hoàn tất quá trình cài đặt.

Ghi chú
Bitdefender VPN yêu cầu .Net Framework 4. 5. 2 hoặc cao hơn để được cài đặt. Trong trường hợp bạn không có gói cài đặt này, một cửa sổ thông báo sẽ

xuất hiện. Nhấp vào **cài đặt .Net Framework** để được chuyển đến một trang từ nơi bạn có thể tải xuống phiên bản mới nhất của phần mềm này.

21.2. Mở VPN

Để truy cập vào giao diện chính của Bitdefender VPN, sử dụng một trong các phương pháp sau:

- Từ khay hệ thống
  1. Nhấp chuột phải vào biểu tượng trong khay hệ thống, sau đó nhấp vào **Hiển thị**.
- Từ giao diện Bitdefender:
  1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
  2. Trong mô đun **VPN**, nhấp vào **Mở VPN**.

21.3. Giao diện VPN

Giao diện VPN hiển thị trạng thái của ứng dụng, kết nối hoặc ngắt kết nối. Vị trí máy chủ cho người dùng có phiên bản miễn phí được Bitdefender tự động thiết lập cho máy chủ thích hợp nhất, trong khi người dùng cao cấp có thể thay đổi vị trí máy chủ mà họ muốn kết nối. Để biết thêm thông tin về đăng ký VPN, hãy tham khảo "*Các dịch vụ*" (p. 121)

Để kết nối hoặc ngắt kết nối, chỉ cần nhấp vào trạng thái được hiển thị ở đầu màn hình, hoặc nhấp chuột phải vào biểu tượng khay hệ thống. Biểu tượng khay hệ thống hiển thị dấu check màu xanh lá cây khi kết nối VPN và dấu check màu đỏ khi VPN bị ngắt kết nối.

Khi đã kết nối, thời gian và việc sử dụng băng thông được hiển thị ở phần dưới của giao diện.

Để có quyền truy cập vào nhiều tuỳ chọn hơn, hãy truy cập khu vực **Menu** bằng cách nhấp vào ở phía trên bên trái. Bạn có các tùy chọn sau đây:

- **Tài khoản của tôi** - chi tiết về tài khoản Bitdefender và đăng ký VPN của bạn được hiển thị. Nhấp vào **Chuyển tài khoản** nếu bạn muốn đăng nhập bằng một tài khoản khác.
- **Cài đặt** - tùy thuộc vào nhu cầu của bạn, bạn có thể tùy chỉnh hành vi của sản phẩm
  - nhận thông báo khi VPN tự động kết nối hoặc ngắt kết nối

- tự động chạy ứng dụng VPN khi khởi động Windows
- tự động khởi chạy ứng dụng VPN khi thiết bị của bạn kết nối với mạng không dây không an toàn

- **Nâng cấp lên Premium** - nếu bạn đang sử dụng phiên bản miễn phí, bạn có thể nâng cấp lên từ đây.
- **Hỗ trợ** - bạn được chuyển hướng đến Trung tâm hỗ trợ của chúng tôi, từ đó bạn có thể đọc bài viết hữu ích về cách sử dụng Bitdefender VPN.
- **Giới thiệu về** - thông tin về phiên bản được cài đặt sẽ được hiển thị.

21.4. Các dịch vụ

Bitdefender VPN cung cấp miễn phí hạn ngạch lưu lượng 200 MB mỗi ngày cho mỗi thiết bị để đảm bảo kết nối của bạn mỗi khi bạn cần và kết nối bạn tự động đến vị trí máy chủ tối ưu.

Để có được lưu lượng truy cập không giới hạn và quyền truy cập không hạn chế đến nội dung trên toàn thế giới bằng cách chọn vị trí máy chủ theo ý thích của bạn, hãy nâng cấp lên phiên bản cao cấp.

Bạn có thể nâng cấp lên phiên bản Bitdefender Premium VPN bất cứ lúc nào bằng cách nhấp vào nút **NHẬN LƯU LƯỢNG KHÔNG GIỚI HẠN** trong giao diện sản phẩm.

Đăng ký Bitdefender Premium VPN khác với đăng ký Bitdefender Antivirus Plus, có nghĩa là bạn sẽ có thể sử dụng cho toàn bộ tính năng của nó, bất kể trạng thái của thuê bao bảo vệ của bạn. Trong trường hợp thuê bao Bitdefender Premium VPN hết hạn, nhưng đăng ký cho Bitdefender Antivirus Plus vẫn hoạt động, bạn sẽ được hoàn nguyên về gói miễn phí.

Bitdefender VPN là một sản phẩm nền tảng, có sẵn trong sản phẩm Bitdefender tương thích với Windows, macOS, Android và iOS. Khi bạn nâng cấp lên gói cao cấp, bạn sẽ có thể sử dụng đăng ký của mình trên tất cả các sản phẩm, miễn là bạn đăng nhập bằng cùng một tài khoản Bitdefender.

22. SAFEPAY BẢO MẬT CÁC GIAO DỊCH TRỰC TUYẾN

Các máy tính nối mạng nhanh chóng trở thành công cụ chính cho việc mua sắm và giao dịch ngân hàng. Thanh toán hóa đơn, chuyển tiền, mua bất cứ thứ gì bạn tưởng tượng ra chưa bao giờ nhanh và dễ dàng như bây giờ.

Điều này bao gồm việc gửi thông tin cá nhân, tài khoản, dữ liệu thẻ tín dụng, mật khẩu và các loại thông tin cá nhân khác trên internet, nói cách khác đây chính là luồng thông tin tội phạm mạng rất quan tâm khai thác. Tin tặc không ngừng nỗ lực ăn cắp thông tin này, vì vậy bạn không bao giờ là quá thận trọng về việc đảm bảo an ninh giao dịch trực tuyến.

Bitdefender Safepay™ là hàng đầu của các trình duyệt bảo mật, một môi trường đóng kín được thiết kế để thực hiện giao dịch ngân hàng trực tuyến, mua sắm điện tử được an toàn.

Để bảo vệ quyền riêng tư tốt nhất, Bitdefender Quản lý mật khẩu đã được tích hợp vào Bitdefender Safepay™ để bảo vệ thông tin tài khoản của bạn bất cứ khi nào bạn truy cập trực tuyến. Để biết thêm thông tin, hãy chuyển đến "*Quản lý mật khẩu bảo vệ tài khoản của bạn*" (p. 109).

Bitdefender Safepay™ cung cấp các tính năng sau:

- Nó chặn mọi truy cập vào màn hình máy tính của bạn và các nỗ lực chụp ảnh màn hình của bạn.
- Nó bảo vệ mật khẩu bí mật của bạn trong khi duyệt web trực tuyến với Quản lý Mật khẩu.
- Nó đi kèm với một bàn phím ảo mà khi được sử dụng sẽ chặn tin tặc đọc việc gõ bàn phím của bạn.
- Hoàn toàn độc lập với các trình duyệt khác của bạn.
- Nó đi kèm với tính năng bảo vệ điểm phát tín hiệu wi-fi được sử dụng khi máy tính của bạn kết nối với một mạng Wi-fi không an toàn.
- Nó hỗ trợ đánh dấu trang và cho phép bạn di chuyển giữa các ngân hàng / trang web mua sắm yêu thích của bạn.
- Nó không bị giới hạn vào sử dụng cho ngân hàng và mua sắm điện tử. Bất kỳ trang web nào cũng có thể được mở trong Bitdefender Safepay™.

22.1. Sử dụng Bitdefender Safepay™

Theo mặc định, Bitdefender phát hiện khi bạn mở một trang web ngân hàng trực tuyến hoặc cửa hàng trực tuyến từ bất kỳ trình duyệt nào trên máy tính của bạn và sẽ nhắc bạn sử dụng Bitdefender Safepay™.

Để truy cập vào giao diện chính của Bitdefender Safepay™, sử dụng một trong các phương pháp sau:

- Từ giao diện Bitdefender.
  1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
  2. Trong ngăn **SAFEPAY**, nhấp vào **Mở Safepay**.
- Từ Windows:
  - Trong **Windows 7**:
    1. Nhấp **Bắt đầu** và tới **Tất cả các chương trình**.
    2. Nhấp **Bitdefender**.
    3. Sử dụng **Bitdefender Safepay™**.
  - Trong **Windows 8 and Windows 8.1**:

    Xác định vị trí Bitdefender Safepay™ từ màn hình Start của Windows (ví dụ, bạn có thể gõ "Bitdefender Safepay™" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng.
  - Trong **Windows 10**:

    Loại "Bitdefender Safepay™" trong hộp tìm kiếm trên thanh tác vụ và nhấp vào biểu tượng của nó.

Nếu bạn quen sử dụng các trình duyệt web, bạn sẽ không gặp vấn đề gì khi sử dụng Bitdefender Safepay™ - nó có giao diện và hoạt động như một trình duyệt bình thường:

- nhập địa chỉ trang web mà bạn muốn đến vào thanh địa chỉ.
- thêm tab để xem nhiều trang web trong cửa sổ Bitdefender Safepay™ bằng cách nhấp .
- quay lại và đi tiếp, làm mới các trang sử dụng tương ứng.

- truy cập cài đặt của Bitdefender Safepay™ bằng cách nhấn ••• và chọn **Cài đặt** .
- bảo vệ mật khẩu của bạn với Quản lý Tài khoản bằng cách nhấn vào .
- quản lý các đánh dấu trang bằng cách nhấn vào ☆ bên cạnh thanh địa chỉ.
- mở bàn phím ảo bằng cách nhấn vào .
- tăng hoặc giảm kích thước trình duyệt bằng cách nhấn đồng thời **Ctrl** và phím **+/-** trong vùng phím số.
- xem thông tin về sản phẩm Bitdefender của bạn bằng cách nhấn ••• và chọn **About** .
- In thông tin quan trọng bằng cách nhấp vào ••• và chọn **In**.

Ghi chú
Để chuyển đổi giữa Bitdefender Safepay™ và màn hình nền Windows, nhấn các phím **Alt + Tab** hoặc nhấp vào **Chuyển sang màn hình nền** ở phía trên bên trái của cửa sổ.

22.2. Thiết lập cấu hình

Nhấn vào ••• và chọn **Cài đặt** để cấu hình Bitdefender Safepay™:

Áp dụng quy tắc Bitdefender Safepay cho các miền được truy cập
Các trang web bạn đã thêm vào Đánh dấu trang với **Tự động mở trong tùy chọn Safepay** được bật sẽ xuất hiện tại đây. Nếu bạn muốn dừng tự động mở Bitdefender Safepay ™ cho một trang web có sẵn từ danh sách, hãy nhấp × bên cạnh mục nhập mong muốn từ cột **Xóa** .

Chặn các bật lên
Bạn có thể chặn cửa sổ bật lên bằng cách nhấn vào nút tương ứng.

Bạn cũng có thể tạo một danh sách các trang web cho phép cửa sổ bật lên. Danh sách này sẽ chỉ bao gồm các trang web mà bạn tin tưởng.

Để thêm một trang web vào danh sách, đưa địa chỉ của nó vào trường tương ứng và nhấp **Thêm miền**.

Để loại bỏ một trang web từ danh sách, bấm "X" tương ứng với các mục mong muốn.

Quản lý các trình cắm
Bạn có thể chọn nếu bạn muốn kích hoạt hoặc vô hiệu hóa các plugin cụ thể trong Bitdefender Safepay™.

Quản lý giấy chứng nhận
Bạn có thể nhập khẩu giấy chứng nhận từ hệ thống của bạn đến một kho chứng nhận.

Nhấp vào **NHẬP CHỨNG CHỈ** và làm theo trình hướng dẫn để sử dụng chứng chỉ trong Bitdefender Safepay™.

Sử dụng bàn phím ảo
Bàn phím ảo sẽ tự động xuất hiện khi trường mật khẩu được chọn.

Sử dụng chuyển đổi tương ứng để kích hoạt hoặc vô hiệu hóa tính năng này.

Xác nhận in
Bật tùy chọn này nếu bạn muốn cung cấp xác nhận của bạn trước khi quá trình in bắt đầu.

22.3. Quản lý đánh dấu trang

Nếu bạn vô hiệu hóa tự động phát hiện một số hoặc tất cả các trang web, hoặc Bitdefender đơn giản không phát hiện một số trang web, bạn có thể thêm đánh dấu trang vào Bitdefender Safepay™ để dễ dàng mở trang web ưa thích trong trình duyệt này.

Thực hiện theo các bước sau để thêm một địa chỉ web vào đánh dấu trang của Bitdefender Safepay™:

1. Nhấp ☆ bên cạnh thanh địa chỉ để mở mục đánh dấu trang.

   Ghi chú
   Trang đánh dấu được mở ra theo mặc định khi bạn mở Bitdefender Safepay™.

2. Nhấp vào nút **+** để thêm một mục mới.

3. Nhập URL và tiêu đề của thẻ đánh dấu trang, và nhấp vào **TẠO**. Kiểm tra tùy chọn **Tự động mở trong Safepay** nếu bạn muốn các trang đánh dấu để mở với Bitdefender Safepay™ mỗi khi bạn truy cập vào nó. Địa chỉ web cũng có thể được bổ sung vào danh sách tên miền tại cài đặt.

22.4. Tắt thông báo Safepay

Khi phát hiện trang web ngân hàng, sản phẩm Bitdefender được thiết lập để thông báo cho bạn qua cửa sổ bật lên.

Để tắt thông báo Safepay:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong ngăn **SAFEPAY**, nhấp vào **Cài đặt**.
3. Tắt **thông báo Safepay** .

22.5. Sử dụng VPN với Safepay

Để thực hiện thanh toán trực tuyến trong môi trường an toàn khi được kết nối với mạng không an toàn, sản phẩm Bitdefender có thể được thiết lập để tự động khởi chạy ứng dụng VPN cùng với Safepay.

Để bắt đầu sử dụng ứng dụng VPN cùng với Safepay:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong ngăn **SAFEPAY**, nhấp vào **Cài đặt**.
3. Bật **Sử dụng VPN với Safepay**.

23. BẢO VỆ DỮ LIỆU

23.1. Xóa Tệp tin vĩnh viễn

Khi bạn xóa một file, nó có thể không còn truy nhập được thông qua cách bình thường nữa. Tuy nhiên, tập tin tiếp tục được lưu trữ trên ổ cứng cho tới khi bị ghi đè bởi tập tin mới.

Bitdefender Hủy tập tin giúp bạn xóa dữ liệu vĩnh viễn, loại bỏ nó khỏi đĩa cứng của bạn ở mức độ vật lý.

Bạn có thể nhanh chóng xóa sạch tập tin hoặc thư mục từ máy tính của bạn bằng cách sử dụng trình đơn ngữ cảnh Windows bằng cách làm theo các bước sau:

1. Bấm chuột phải vào tập tin hoặc thư mục mà bạn muốn xóa vĩnh viễn.
2. Chọn **Bitdefender** > **Hủy tập tin** từ trình đơn theo ngữ cảnh xuất hiện.
3. Nhấp vào **XÓA VĨNH VIỄN** và sau đó xác nhận rằng bạn muốn tiếp tục quá trình.

   Đợi đến khi Bitdefender hoàn tất hủy các tập tin.
4. Các kết quả được hiển thị. Nhấp **HOÀN THÀNH** để thoát khỏi tiện ích.

Ngoài ra, bạn có thể chia nhỏ các tập tin từ giao diện Bitdefender, như sau:

1. Nhấp vào **Bảo mật** trên menu điều hướng trên giao diện Bitdefender .
2. Trong ngăn **DỮ LIỆU ĐƯỢC BẢO VỆ** , nhấp vào **Chia nhỏ dữ liệu** .
3. Theo các hướng dẫn Hủy Tập tin sau:
   a. Nhấp vào nút **THÊM THƯ MỤC** để thêm các tệp hoặc thư mục bạn muốn xóa vĩnh viễn.

      Ngoài ra, hãy kéo các tệp hoặc thư mục đó vào cửa sổ này.
   b. Nhấp vào **XÓA VĨNH VIỄN** và sau đó xác nhận rằng bạn muốn tiếp tục quá trình.

      Đợi đến khi Bitdefender hoàn tất hủy các tập tin.
   c. **Tóm tắt kết quả**

      Các kết quả được hiển thị. Nhấp **HOÀN THÀNH** để thoát khỏi tiện ích.

24. MIỄN DỊCH USB

Tính năng Tự động chạy là một công cụ rất hữu ích của hệ điều hành Windows, cho phép máy tính tự động thực thi một tập tin từ thiết bị tháo lắp gắn với máy tính. Ví dụ, cài đặt phần mềm có thể tự khởi động khi một đĩa CD được đưa vào ổ đĩa quang.

Thật không may, tính năng này cũng có thể được sử dụng bởi phần mềm độc hại để tự động khởi động và xâm nhập máy tính của bạn từ các thiết bị như ổ đĩa USB và thẻ nhớ được kết nối thông qua đầu đọc thẻ. Các cuộc tấn công dựa trên Tự động chạy đã được thực hiện trong những năm gần đây.

Với tính năng Miễn dịch USB, bạn có thể ngăn chặn bất kỳ ổ đĩa flash có định dạng NTFS, FAT, FAT32 không tự động chạy phần mềm độc hại. Khi một thiết bị USB được miễn dịch, phần mềm độc hại không thể cấu hình để chạy một ứng dụng tự động khi thiết bị được kết nối với máy tính Windows.

Để immunize một thiết bị USB:

1. Gắn ổ đĩa flash vào máy tính của bạn.
2. Tìm đến các thiết bị lưu trữ tháo lắp và nhấp chuột phải vào biểu tượng của nó.
3. Trong trình đơn ngữ cảnh, vào **Bitdefender** và chọn **Miễn dịch cho ổ đĩa này**.

> **Ghi chú**
> Nếu ổ đĩa đã được miễn dịch, sẽ xuất hiện thông báo **Thiết bị USB đã được bảo vệ chống lại phần mềm độc hại tự động chạy** thay vì các tùy chọn miễn dịch.

Để ngăn chặn máy tính của bạn không khởi động cùng các phần mềm độc hại từ các thiết bị USB không được miễn dịch, hãy vô hiệu hóa tính năng tự động chạy của các thiết bị này. Để biết thêm thông tin, hãy chuyển đến *"Sử dụng Tự động giám sát lỗ hổng bảo mật "* (p. 96).

TỐI ƯU HÓA HỆ THỐNG

25. HỒ SƠ

Các hoạt động hàng ngày, xem phim hoặc chơi trò chơi có thể làm hệ thống chậm lại, đặc biệt nếu chúng chạy đồng thời cùng quá trình cập nhật Windows và các nhiệm vụ bảo trì. Với Bitdefender, bạn có thể lựa chọn và áp dụng hồ sơ ưa thích của bạn, giúp điều chỉnh hệ thống phù hợp để tăng hiệu suất của các ứng dụng cụ thể được cài đặt.

Bitdefender cung cấp các hồ sơ sau:

- Hồ sơ Công việc
- Hồ sơ Xem phim
- Hồ sơ Chơi
- Hồ sơ Wi-Fi công cộng
- Chế độ Pin Hồ sơ

Nếu bạn quyết định không sử dụng **Hồ sơ**, một hồ sơ mặc định được gọi là **Chuẩn** sẽ được kích hoạt và nó không thực hiện tối ưu hóa hệ thống cho bạn.

Theo hoạt động của bạn, cài đặt sau đây được áp dụng khi hồ sơ làm việc, Xem phim, trò chơi được kích hoạt:

- Tất cả các cảnh báo và cửa sổ thông tin Bitdefender đều bị ngừng.
- Cập nhật Tự động bị hoãn
- Quét theo lịch được hoãn lại.
- Cố Vấn Tìm Kiếm bị tắt.
- Thông báo phiếu mua hàng đặc biệt bị vô hiệu.

Theo hoạt động của bạn, cài đặt hệ thống sau đây được áp dụng khi hồ sơ làm việc, Xem phim, trò chơi được kích hoạt:

- Tự động cập nhật Windows bị hoãn.
- Cảnh báo Windows và cửa sổ bật ra bị vô hiệu hóa.
- Các chương trình nền không cần thiết bị đình chỉ.
- Hiệu ứng hình ảnh được điều chỉnh cho hiệu suất tốt nhất.
- Tác vụ bảo dưỡng được hoãn lại.
- Thiết lập sử dụng nguồn điện được điều chỉnh.

Trong khi đang chạy trong hồ sơ Wifi công cộng, Bitdefender Antivirus Plus được thiết lập để tự động thực hiện các cài đặt chương trình sau đây:

- Phòng chống tấn công nâng cao được bật
- Các cài đặt sau từ tính năng Ngăn chặn mối đe dọa trực tuyến được bật:
  - Quét trang web mã hóa
  - Bảo vệ khỏi gian lận
  - Bảo vệ khỏi lừa đảo

25.1. Hồ sơ Công việc

Chạy nhiều tác vụ như gửi e-mail, liên lạc video với các đồng nghiệp ở xa hoặc làm việc với các ứng dụng thiết kế có thể ảnh hưởng đến hiệu năng hệ thống. Hồ sơ công việc được thiết kế để giúp bạn nâng cao hiệu quả làm việc bằng cách tắt một số dịch vụ nền và công việc bảo trì.

Cấu hình hồ sơ làm việc

Để cấu hình các hành động được thực hiện khi ở Hồ Sơ Làm Việc:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **Cấu hình** từ khu vực Hồ sơ làm việc.
4. Chọn điều chỉnh hệ thống được áp dụng bằng cách chọn các tùy chọn sau:
   - Tăng cường hiệu suất làm việc trên các ứng dụng
   - Tối ưu hóa cài đặt sản phẩm cho cấu hình hồ sơ
   - Hoãn các chương trình thường trú và tác vụ bảo trì
   - Hoãn Tự động cập nhật Windows
5. Nhấp **Lưu lại** để lưu các thay đổi và đóng cửa sổ.

Tự thêm các ứng dụng cho danh sách Hồ sơ làm việc

Nếu Bitdefender không tự động thêm vào Hồ sơ khi bạn khởi động một ứng dụng nhất định, bạn có thể tự thêm ứng dụng này vào **Danh sách ứng dụng làm việc**.

Để tự thêm các ứng dụng vào Danh sách ứng dụng làm việc trong Hồ sơ làm việc:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **Cấu hình** từ khu vực Hồ sơ làm việc.
4. Trong cửa sổ **Thiết lập hồ Sơ Làm Việc**, nhấp vào **Danh sách ứng dụng**.
5. Nhấn vào **Thêm**.

   Một cửa sổ mới xuất hiện. Duyệt đến tập tin thực thi của ứng dụng, chọn nó và nhấn **OK** để thêm nó vào danh sách.

25.2. Hồ sơ Xem phim

Hiển thị nội dung video chất lượng cao, chẳng hạn như phim ảnh độ nét cao, đòi hỏi đáng kể tài nguyên hệ thống. Hồ sơ xem Phim điều chỉnh hệ thống và cài đặt sản phẩm, giúp bạn thưởng thức một bộ phim liên tục, không bị gián đoạn.

Cấu hình Hồ sơ xem Phim

Để cấu hình các hành động được thực hiện khi ở Hồ Sơ xem Phim:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **Cấu hình** từ khu vực Hồ Sơ Xem Phim.
4. Chọn điều chỉnh hệ thống được áp dụng bằng cách chọn các tùy chọn sau:
   - Tăng hiệu suất trên trình đọc video
   - Tối ưu hóa cài đặt sản phẩm cho Hồ sơ xem Phim
   - Hoãn các chương trình thường trú và tác vụ bảo trì
   - Hoãn Tự động cập nhật Windows
   - Điều chỉnh các thiết lập kế hoạch năng lượng cho việc xem phim
5. Nhấp **Lưu lại** để lưu các thay đổi và đóng cửa sổ.

Tự thêm các ứng dụng xem Video cho danh sách Hồ sơ xem Phim

Nếu Bitdefender không tự động thêm vào Hồ sơ xem Phim khi bạn khởi động một ứng dụng đọc video, bạn có thể tự thêm ứng dụng này vào **Danh sách ứng dụng Movie**.

Để tự thêm ứng dụng đọc video vào danh sách ứng dụng của Hồ Sơ xem Phim:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **Cấu hình** từ khu vực Hồ Sơ Xem Phim.
4. Trong cửa sổ **Thiết lập hồ Sơ Làm Việc**, nhấp vào **Danh sách ứng dụng**.
5. Nhấn vào **Thêm**.

   Một cửa sổ mới xuất hiện. Duyệt đến tập tin thực thi của ứng dụng, chọn nó và nhấn **OK** để thêm nó vào danh sách.

25.3. Hồ sơ Chơi

Thưởng thức trò chơi không bị gián đoạn là đòi hỏi giảm việc tải hệ thống và chậm hệ thống. Bằng cách sử dụng công nghệ tự động hành vi cùng với một danh sách các trò chơi nổi tiếng, Bitdefender có thể tự động phát hiện các hoạt động trò chơi và tối ưu hóa tài nguyên hệ thống để bạn có thể thưởng thức việc chơi game.

Cấu hình Hồ sơ Trò chơi

Để cấu hình các hành động được thực hiện khi ở Hồ Sơ Trò Chơi:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **Cấu hình** từ khu vực Hồ Sơ Trò Chơi.
4. Chọn điều chỉnh hệ thống được áp dụng bằng cách chọn các tùy chọn sau:
   - Tăng cường hiệu suất làm việc trên các trò chơi
   - Tối ưu hóa cài đặt sản phẩm cho Hồ sơ Trò chơi

- Hoãn các chương trình thường trú và tác vụ bảo trì
- Hoãn Tự động cập nhật Windows
- Điều chỉnh các thiết lập kế hoạch năng lượng cho các trò chơi

5. Nhấp **Lưu lại** để lưu các thay đổi và đóng cửa sổ.

Tự bạn thêm trò chơi vào danh sách trò chơi

Nếu Bitdefender không tự động thêm vào Hồ sơ Trò chơi khi bạn khởi động một ứng dụng trò chơi, bạn có thể tự thêm ứng dụng này vào **Danh sách Trò Chơi**.

Để tự thêm trò chơi vào danh sách ứng dụng Game trong Hồ sơ Trò chơi:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **Cấu hình** từ khu vực Hồ Sơ Trò Chơi.
4. Trong cửa sổ **Thiết lập hồ Sơ Làm Việc**, nhấp vào **Danh sách ứng dụng**.
5. Nhấn vào **Thêm**.

   Một cửa sổ mới xuất hiện. Duyệt đến tập tin thực thi của trò chơi, chọn nó và nhấp **OK** để thêm nó vào danh sách.

25.4. Hồ sơ Wi-Fi công cộng

Gửi email, gõ thông tin nhạy cảm hoặc mua sắm trực tuyến trong khi kết nối với mạng không dây không an toàn có nguy cơ lộ dữ liệu cá nhân của bạn. Hồ sơ Wifi công cộng điều chỉnh cài đặt sản phẩm để cung cấp cho bạn khả năng để thực hiện thanh toán trực tuyến và sử dụng thông tin nhạy cảm trong một môi trường được bảo vệ.

Cấu hình hồ sơ Wifi công cộng

Để cấu hình Bitdefender để áp dụng cài đặt sản phẩm khi kết nối với một mạng không dây không an toàn:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **CẤU HÌNH** từ khu vực Hồ Sơ Wifi công cộng.

4. Để **Điều chỉnh cài đặt sản phẩm để tăng bảo vệ khi kết nối mạng cộng cộng không an toàn**hộp kiểm được kích hoạt.
5. Nhấp chuột vào **Lưu**.

25.5. Chế độ Pin Hồ sơ

Hồ sơ Chế độ chạy Pin được thiết kế đặc biệt cho máy tính xách tay và máy tính bảng. Mục đích của nó là để giảm thiểu cả hệ thống và ảnh hưởng Bitdefender đến tiêu thụ điện năng khi mức độ sạc pin là thấp hơn so với mặc định hoặc bạn đã chọn.

Cấu hình Hồ Sơ Chế độ chạy pin

Để cấu hình các hồ sơ Chế độ Pin:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. nhấp vào nút **CẤU HÌNH** từ khu vực Hồ Sơ Chế độ Pin.
4. Chọn điều chỉnh hệ thống được áp dụng bằng cách kiểm tra các tùy chọn sau:
   - Tối ưu các thiết lập sản phẩm cho chế độ pin.
   - Hoãn các chương trình thường trú và tác vụ bảo trì.
   - Hoãn Tự động cập nhật Windows.
   - Điều chỉnh các thiết lập kế hoạch năng lượng cho chế độ pin.
   - Vô hiệu hóa các thiết bị ngoại vi và cổng mạng.
5. Nhấp **Lưu lại** để lưu các thay đổi và đóng cửa sổ.

Nhập một giá trị hợp lệ trong hộp tròn hoặc cách sử dụng các phím mũi tên lên và xuống để xác định khi hệ thống nên bắt đầu hoạt động Chế độ Pin. Theo mặc định, chế độ được kích hoạt khi mức pin giảm xuống dưới 30%.

Các cài đặt sau đây được áp dụng khi Bitdefender hoạt động trong hồ sơ chế độ chạy pin:

- Bitdefender Tự động cập nhật được hoãn lại.
- Quét theo lịch được hoãn lại.
- Thuật sỹ An ninh bị tắt.

Bitdefender phát hiện khi máy tính xách tay của bạn đã chuyển sang sử dụng pin và dựa trên mức độ sạc pin nó sẽ tự động chuyển sang chế độ chạy pin. Tương tự như vậy, Bitdefender tự động thoát ra khỏi chế độ chạy pin khi nó phát hiện các máy tính xách tay không còn chạy pin.

25.6. Tối ưu theo thời gian thực

Bitdefender Tối ưu hóa theo thời gian thực là một bổ trợ để cải thiện hiệu năng hệ thống một cách âm thầm, ở chế độ nền, đảm bảo rằng bạn không bị gián đoạn trong khi đang ở trong một chế độ Hồ sơ cụ thể. Tùy thuộc vào tải CPU, các bổ trợ giám sát tất cả các quá trình, tập trung vào những tiến trình có tải cao hơn, để điều chỉnh theo nhu cầu của bạn.

Để bật hoặc tắt Tối ưu thời gian thực:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Hồ Sơ**.
3. Cuộn xuống cho đến khi bạn thấy tùy chọn Tối ưu hoá thời gian thực, và sau đó sử dụng nút chuyển đổi tương ứng để bật hoặc tắt.

SỬA LỖI

26. GIẢI QUYẾT CÁC VẤN ĐỀ PHỔ BIẾN

Chương này trình bày một số vấn đề bạn có thể gặp phải khi sử dụng Bitdefender và cung cấp cho bạn giải pháp cho những vấn đề này. Hầu hết các vấn đề có thể được giải quyết thông qua các cấu hình thích hợp của các cài đặt cho sản phẩm.

- "*Hệ thống của tôi chạy chậm*" (p. 138)
- "*Quét chưa khởi động*" (p. 139)
- "*Tôi không thể sử dụng ứng dụng nữa*" (p. 142)
- "*Phải làm gì khi Bitdefender chặn trang web, tên miền, địa chỉ IP hoặc ứng dụng trực tuyến an toàn*" (p. 143)
- "*Phải làm gì nếu Bitdefender phát hiện một ứng dụng an toàn lại là mã độc tống tiền.*" (p. 143)
- "*Làm thế nào để cập nhật Bitdefender trên một đường truyền Internet chậm*" (p. 144)
- "*Các dịch vụ của Bitdefender không phản hồi*" (p. 144)
- "*Tính năng Tự động điền thông tin trong Ví bảo mật của tôi không làm việc*" (p. 145)
- "*Gỡ bỏ Bitdefender không thực hiện được*" (p. 146)
- "*Hệ thống của tôi không khởi động sau khi cài đặt Bitdefender*" (p. 147)

Nếu bạn không thể tìm thấy vấn đề của bạn ở đây, hoặc nếu các giải pháp trình bày không giải quyết được vấn đề, bạn có thể liên lạc với hỗ trợ kỹ thuật Bitdefender như đã trình bày trong chương "*Muốn được giúp*" (p. 162).

26.1. Hệ thống của tôi chạy chậm

Thông thường, sau khi cài đặt một phần mềm bảo mật, có thể xuất hiện sự sụt giảm nhẹ của hệ thống, mà ở một mức độ nào đó là bình thường.

Nếu bạn nhận thấy một sự suy giảm đáng kể, vấn đề này có thể xuất hiện vì những lý do sau đây:

- **Bitdefender không phải là chương trình bảo mật duy nhất được cài đặt trên hệ thống.**

  Mặc dù Bitdefender có tìm kiếm và loại bỏ các chương trình bảo mật được tìm thấy trong quá trình cài đặt, chúng tôi vẫn khuyến khích bạn nên loại

bỏ các chương trình này trước khi cài đặt Bitdefender. Để biết thêm thông tin, hãy chuyển đến "*Làm thế nào để gỡ bỏ các giải pháp bảo mật khác?*" (p. 66).

- **Các yêu cầu hệ thống để chạy Bitdefender không được đáp ứng.**

  Nếu máy của bạn không đáp ứng các yêu cầu hệ thống, máy tính sẽ trở nên chậm chạp, đặc biệt là khi nhiều ứng dụng đang chạy cùng một lúc. Để biết thêm thông tin, hãy chuyển đến "*Yêu cầu hệ thống*" (p. 3).

- **Bạn đã cài đặt ứng dụng mà bạn không sử dụng** .

  Bất kỳ máy tính nào có chương trình hoặc ứng dụng mà bạn không sử dụng. Và nhiều chương trình không mong muốn chạy dưới nền chiếm không gian đĩa và bộ nhớ. Nếu bạn không sử dụng tới chương trình nào, gỡ bỏ nó đi. Điều này cũng áp dụng với bất kỳ phần mềm cài đặt sẵn hoặc ứng dụng dùng thử khác mà bạn quên chưa gỡ ra.

  > **Quan trọng**
  > Nếu bạn nghi ngờ một chương trình hoặc một ứng dụng là một phần thiết yếu của hệ điều hành, đừng gỡ bỏ nó và liên hệ với chăm sóc khách hàng của Bitdefender để được hỗ trợ.

- **Hệ thống của bạn có thể bị nhiễm virus**.

  Tốc độ hệ thống của bạn và hành vi chung của nó cũng có thể bị ảnh hưởng bởi các mối đe dọa. Phần mềm gián điệp, mã độc, trojan và phần mềm quảng cáo, tất cả chúng đều ảnh hưởng lên hiệu suất máy tính của bạn. Đảm bảo quét hệ thống của bạn theo định kỳ, ít nhất một lần một tuần. Bạn nên sử dụng Quét hệ thống của Bitdefender vì nó sẽ quét tất cả các loại phần mềm độc hại đe dọa sự an toàn của hệ thống.

  Để bắt đầu quét hệ thống:

  1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
  2. Trong phần **CHỐNG VIRUS** , nhấp **Quét hệ thống** .
  3. Thực hiện theo các bước hướng dẫn.

26.2. Quét chưa khởi động

Loại vấn đề này có thể do hai nguyên nhân chính:

- **Một cài đặt Bitdefender trước đây chưa được gỡ bỏ hoàn toàn hoặc bị lỗi cài đặt Bitdefender**.

Trong trường hợp này cài đặt lại Bitdefender:

- Trong **Windows 7**:
  1. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
  2. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  3. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
  4. Chờ quá trình cài đặt lại hoàn tất, và sau đó khởi động lại hệ thống của bạn.
- Trong **Windows 8 and Windows 8.1**:
  1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
  2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
  3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  4. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
  5. Chờ quá trình cài đặt lại hoàn tất, và sau đó khởi động lại hệ thống của bạn.
- Trong **Windows 10**:
  1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
  2. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **cài đặt các ứng dụng** .
  3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
  5. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
  6. Chờ quá trình cài đặt lại hoàn tất, và sau đó khởi động lại hệ thống của bạn.

Ghi chú

Bằng cách làm theo thủ tục cài đặt lại này, các cài đặt tùy chỉnh được lưu và có sẵn trong sản phẩm được cài đặt mới. Các cài đặt khác có thể được chuyển trở lại cấu hình mặc định của chúng.

- **Bitdefender không phải là giải pháp bảo mật duy nhất được cài đặt trên hệ thống của bạn**.

  Trong trường hợp này:

  1. Gỡ bỏ các giải pháp bảo mật khác. Để biết thêm thông tin, hãy chuyển đến "*Làm thế nào để gỡ bỏ các giải pháp bảo mật khác?*" (p. 66).
  2. Cài đặt lại Bitdefender
     - Trong **Windows 7**:
       a. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
       b. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
       c. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
       d. Chờ quá trình cài đặt lại hoàn tất, và sau đó khởi động lại hệ thống của bạn.
     - Trong **Windows 8 and Windows 8.1**:
       a. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
       b. Nhấp **Uninstall a program** hoặc **Programs and Features**.
       c. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
       d. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
       e. Chờ quá trình cài đặt lại hoàn tất, và sau đó khởi động lại hệ thống của bạn.
     - Trong **Windows 10**:
       a. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
       b. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **cài đặt các ứng dụng** .
       c. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
       d. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
       e. Nhấp vào **CÀI ĐẶT LẠI** tại cửa sổ hiện ra.
       f. Chờ quá trình cài đặt lại hoàn tất, và sau đó khởi động lại hệ thống của bạn.

Ghi chú
Bằng cách làm theo thủ tục cài đặt lại này, các cài đặt tùy chỉnh được lưu và có sẵn trong sản phẩm được cài đặt mới. Các cài đặt khác có thể được chuyển trở lại cấu hình mặc định của chúng.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

26.3. Tôi không thể sử dụng ứng dụng nữa

Vấn đề này xảy ra khi bạn đang cố gắng sử dụng một chương trình đã hoạt động bình thường trước khi cài đặt Bitdefender.

Sau khi cài đặt Bitdefender bạn có thể gặp phải một trong những tình huống:

- Bạn có thể nhận được một tin nhắn từ Bitdefender rằng chương trình đang cố gắng can thiệp thay đổi hệ thống.
- Bạn có thể nhận được một thông báo lỗi từ chương trình mà bạn đang cố gắng để sử dụng.

Kiểu tình huống này xảy ra khi mô-đun PHÒNG CHỐNG TẤN CÔNG NÂNG CAO nhầm lẫn trong việc coi một số ứng dụng hợp lệ là độc hại.

Kiểm soát chủ động là một tính năng của Bitdefender liên tục theo dõi các ứng dụng đang chạy trên hệ thống của bạn và báo cáo những hành vi nguy hiểm tiềm ẩn. Tính năng này dựa trên một hệ thống phỏng đoán, nên có thể có trường hợp các ứng dụng hợp pháp được báo cáo là độc hại bởi mô-đun Kiểm soát chủ động.

Khi tình huống này xảy ra, bạn có thể loại trừ ứng dụng tương ứng khỏi danh sách được theo dõi bởi Kiểm soát chủ động.

Thêm chương trình vào danh sách loại trừ.

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **PHÒNG THỦ MỐI ĐE DỌA NÂNG CAO**, nhấp **Thiết lập**.
3. Trong khu vực **Loại trừ**, nhấp vào **Thêm ứng dụng vào loại trừ**.
4. Tìm và chọn ứng dụng bạn muốn loại trừ, sau đó nhấp **OK**.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

26.4. Phải làm gì khi Bitdefender chặn trang web, tên miền, địa chỉ IP hoặc ứng dụng trực tuyến an toàn

Bitdefender cung cấp việc duyệt web an toàn bằng cách lọc tất cả lưu lượng truy cập web và ngăn chặn các nội dung độc hại. Tuy nhiên, có thể Bitdefender nhìn nhận một trang web, tên miền, địa chỉ IP hoặc ứng dụng trực tuyến an toàn là không an toàn, điều này sẽ khiến việc quét lưu lượng HTTP của Bitdefender chặn chúng không chính xác

Nếu cùng một trang, tên miền, địa chỉ IP hoặc ứng dụng trực tuyến bị chặn liên tục, chúng có thể được thêm vào các ngoại lệ để chúng không bị quét bởi các công cụ Bitdefender, điều này đảm bảo trải nghiệm duyệt web mượt mà hơn.

Để thêm trang web vào **Ngoại lệ**:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **NGĂN CHẶN MỐI ĐE DỌA TRỰC TUYẾN**, nhấp **Thiết lập**.
3. Cung cấp địa chỉ của trang web bị chặn, tên miền, địa chỉ IP hoặc ứng dụng trực tuyến trong trường tương ứng và nhấp vào **THÊM** .
4. Nhấp **Lưu lại** để lưu các thay đổi và đóng cửa sổ.

Chỉ những trang web, tên miền, địa chỉ IP và ứng dụng mà bạn hoàn toàn tin tưởng mới được thêm vào danh sách này. Chúng sẽ được bỏ qua khi quét bởi các công cụ sau đây: chống phần mềm độc hại, lừa đảo và gian lận.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

26.5. Phải làm gì nếu Bitdefender phát hiện một ứng dụng an toàn lại là mã độc tống tiền.

Ransomware là một chương trình độc hại mà cố gắng kiếm tiền từ người dùng bằng cách khóa các hệ thống dễ bị tổn thương của họ. Để giữ cho hệ thống của bạn an toàn từ những tình huống không may, Bitdefender cung cấp cho bạn khả năng để đảm bảo cho các tập tin cá nhân.

Khi một ứng dụng cố gắng để thay đổi hoặc xóa một trong các tập tin được bảo vệ, chúng sẽ được coi là không an toàn và Bitdefender sẽ chặn chức năng của nó.

Trong trường hợp một ứng dụng đã được thêm vào danh sách ứng dụng không đáng tin cậy và bạn chắc chắn rằng nó là an toàn để sử dụng nó, hãy làm theo các bước sau:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Trong cửa sổ **TỆP AN TOÀN** , nhấp vào **Truy cập ứng dụng** .
3. Các ứng dụng đã yêu cầu thay đổi tệp trong thư mục được bảo vệ của bạn đã được liệt kê. Nhấp vào nút **Cho phép** bên cạnh ứng dụng bạn chắc chắn là an toàn.

26.6. Làm thế nào để cập nhật Bitdefender trên một đường truyền Internet chậm

Nếu bạn có một kết nối Internet chậm (kết nối qua dial-up), các lỗi có thể xảy ra trong quá trình cập nhật.

Để cập nhật hệ thống của bạn với cơ sở dữ liệu Bitdefender mới nhất:

1. Nhấp vào **Cài đặt** trên menu điều hướng trên giao diện Bitdefender.
2. Chọn tab **Cập nhật**.
3. Tắt khóa chuyển **Cập nhật thầm lặng** .
4. Lần tới khi có bản cập nhật, bạn sẽ được nhắc chọn bản cập nhật bạn muốn tải xuống. Chỉ chọn **Cập nhật chữ ký** .
5. Bitdefender sẽ chỉ tải xuống và cài đặt cơ sở dữ liệu về mối đe dọa mới nhất.

26.7. Các dịch vụ của Bitdefender không phản hồi

Mục này sẽ giúp bạn khắc phục sự cố **Dịch vụ Bitdefender không hoạt động**. Bạn có thể gặp lỗi này như sau:

- Biểu tượng Bitdefender trong khay hệ thống chuyển sang màu xám và bạn được thông báo rằng dịch vụ Bitdefender không hoạt động.
- Cửa sổ Bitdefender chỉ ra rằng dịch vụ Bitdefender không làm việc.

Các lỗi có thể được gây ra bởi một trong các khả năng sau:

- lỗi liên lạc tạm thời giữa các dịch vụ Bitdefender.
- một số các dịch vụ Bitdefender bị dừng lại.

- giải pháp bảo mật khác đang chạy trên máy tính của bạn cùng lúc với Bitdefender.

Để khắc phục lỗi này, hãy thử các giải pháp:

1. Chờ một vài phút để xem có gì thay đổi không. Lỗi có thể là tạm thời.
2. Khởi động lại máy tính và đợi một vài phút cho đến khi Bitdefender được nạp. Mở Bitdefender để xem nếu lỗi vẫn còn. Khởi động lại máy tính thường giải quyết được vấn đề.
3. Kiểm tra xem bạn có bất kỳ giải pháp bảo mật nào khác được cài đặt vì chúng có thể làm gián đoạn hoạt động bình thường của Bitdefender. Nếu đây là lý do, chúng tôi khuyên bạn nên gỡ bỏ tất cả các giải pháp bảo mật khác và sau đó cài đặt lại Bitdefender.

   Để biết thêm thông tin, hãy chuyển đến *"Làm thế nào để gỡ bỏ các giải pháp bảo mật khác?"* (p. 66).

Nếu lỗi vẫn còn, xin vui lòng liên hệ với đại diện hỗ trợ của chúng tôi để được giúp đỡ như được mô tả trong phần *"Muốn được giúp"* (p. 162).

26.8. Tính năng Tự động điền thông tin trong Ví bảo mật của tôi không làm việc

Bạn đã lưu thông tin trực tuyến của bạn trong Quản lý Mật khẩu Bitdefender và bạn nhận thấy rằng tính năng Tự động điền thông tin không làm việc. Thông thường, vấn đề này xuất hiện khi mở rộng Ví bảo mật của Bitdefender không được cài đặt trong trình duyệt của bạn.

Để giải quyết tình huống này, hãy làm theo các bước sau:

- Tại **Internet Explorer:**
  1. Mở Internet Explorer.
  2. Nhấp mục "Tools".
  3. Nhấp "Manage Add-ons".
  4. Nhấp "Toolbars and Extensions".
  5. Chọn **Ví bảo mật Bitdefender** và nhấp **Kích hoạt**.
- Tại **Mozilla Firefox:**
  1. Mở Mozilla Firefox.
  2. Nhấp mục "Tools".

3. Nhấp "Add-ons".
4. Nhấp "Extensions".
5. Chọn **Ví bảo mật Bitdefender** và nhấp **Kích hoạt**.

- Tại **Google Chrome:**
  1. Mở Google Chrome.
  2. Vào biểu tượng trình đơn.
  3. Nhấp vào Thêm Công cụ.
  4. Nhấp "Extensions".
  5. Chọn **Ví bảo mật Bitdefender** và nhấp **Kích hoạt**.

> **Ghi chú**
> Tiện ích sẽ được kích hoạt sau khi bạn khởi động lại trình duyệt web của bạn.

Bây giờ kiểm tra xem tính năng Tự động điền thông tin của Ví bảo mật hoạt động chưa.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

26.9. Gỡ bỏ Bitdefender không thực hiện được

Nếu bạn muốn gỡ bỏ sản phẩm Bitdefender và bạn nhận thấy rằng quá trình này bị treo hoặc hệ thống bị đóng băng, nhấn **Hủy** để hủy bỏ hành động. Nếu không có tác dụng, khởi động lại hệ thống.

Khi loại bỏ không thành công, một số khóa thanh ghi hệ thống Bitdefender và các tập tin có thể vẫn tồn tại trong hệ thống của bạn. Tàn dư này có thể ngăn chặn việc cài đặt mới của Bitdefender. Chúng cũng có thể ảnh hưởng đến hiệu năng và ổn định hệ thống.

Để loại bỏ hoàn toàn Bitdefender từ hệ thống của bạn:

- Trong **Windows 7**:
  1. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
  2. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  3. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
  4. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

- Trong **Windows 8 and Windows 8.1**:
  1. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
  2. Nhấp **Uninstall a program** hoặc **Programs and Features**.
  3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  4. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
  5. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
- Trong **Windows 10**:
  1. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
  2. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **cài đặt các ứng dụng** .
  3. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
  4. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
  5. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
  6. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

26.10. Hệ thống của tôi không khởi động sau khi cài đặt Bitdefender

Nếu sau khi cài đặt Bitdefender và không thể khởi động lại hệ thống ở chế độ bình thường nữa, có thể có nhiều lý do cho vấn đề này.

Nhiều khả năng là do cài đặt trước đó của Bitdefender không được gỡ bỏ hoàn toàn hoặc do một giải pháp bảo mật khác vẫn còn tồn tại trên hệ thống.

Đây là cách bạn có thể giải quyết từng tình huống:

- **Bạn có Bitdefender đã được cài đặt trước đây và bạn đã không gỡ bỏ nó đúng cách.**

  Để giải quyết điều này:

1. Khởi động lại hệ thống của bạn và đăng nhập vào trong chế độ Safe Mode. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để khởi động vào chế độ An toàn?*" (p. 67).
2. Loại bỏ Bitdefender khỏi hệ thống của bạn:
   - Trong **Windows 7**:
     a. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
     b. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
     c. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
     d. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
     e. Khởi động lại máy về chế độ bình thường.
   - Trong **Windows 8 and Windows 8.1**:
     a. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
     b. Nhấp **Uninstall a program** hoặc **Programs and Features**.
     c. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
     d. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
     e. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
     f. Khởi động lại máy về chế độ bình thường.
   - Trong **Windows 10**:
     a. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
     b. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **cài đặt các ứng dụng** .
     c. Tìm đến **Bitdefender Antivirus Plus** và chọn **Uninstall**.
     d. Nhấn vào **Uninstall** một lần nữa để xác nhận lựa chọn của bạn.
     e. Nhấp vào **LOẠI BỎ** tại cửa sổ hiện ra.
     f. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

g. Khởi động lại máy về chế độ bình thường.

3. Cài đặt lại sản phẩm Bitdefender.

- **Bạn đã cài đặt một giải pháp bảo mật khác trước đây và bạn đã không gỡ bỏ nó đúng cách.**

  Để giải quyết điều này:

  1. Khởi động lại hệ thống của bạn và đăng nhập vào trong chế độ Safe Mode. Để hiểu cách thực hiện việc này, hãy tham khảo *"Làm thế nào để khởi động vào chế độ An toàn?"* (p. 67).
  2. Gỡ bỏ các giải pháp bảo mật khác khỏi hệ thống của bạn:
     - Trong **Windows 7**:
       a. Nhấp **Start**, vào **Control Panel** và nhấn đúp **Programs and Features**.
       b. Tìm tên của chương trình mà bạn muốn loại bỏ và chọn **Gỡ bỏ**.
       c. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
     - Trong **Windows 8 and Windows 8.1**:
       a. Từ màn hình Start của Windows, vào **Control Panel** (ví dụ, bạn có thể gõ "Control Panel" trực tiếp vào màn hình Start) và sau đó nhấp vào biểu tượng của nó.
       b. Nhấp **Uninstall a program** hoặc **Programs and Features**.
       c. Tìm tên của chương trình mà bạn muốn loại bỏ và chọn **Gỡ bỏ**.
       d. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.
     - Trong **Windows 10**:
       a. Nhấn vào **Bắt đầu**, sau đó nhấp vào thiết lập.
       b. Nhấn vào biểu tượng**Hệ thống** trong khu vực thiết lập, sau đó chọn **cài đặt các ứng dụng** .
       c. Tìm tên của chương trình mà bạn muốn loại bỏ và chọn **Gỡ cài đặt**.
       d. Đợi cho quá trình gỡ bỏ hoàn tất, và sau đó khởi động lại hệ thống của bạn.

Để gỡ bỏ một cách chính xác các phần mềm, hãy vào trang web của hãng và chạy công cụ gỡ bỏ cài đặt của hãng hoặc liên hệ trực tiếp để được hỗ trợ.

3. Khởi động lại hệ thống của bạn trong chế độ bình thường và cài đặt lại Bitdefender.

Bạn đã thực hiện các bước nêu trên và tình hình không được giải quyết.

Để giải quyết điều này:

1. Khởi động lại hệ thống của bạn và đăng nhập vào trong chế độ Safe Mode. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để khởi động vào chế độ An toàn?*" (p. 67).
2. Sử dụng tính năng Khôi phục hệ thống của Windows để khôi phục lại máy tính về thời điểm trước khi cài đặt Bitdefender.
3. Khởi động lại hệ thống trong chế độ bình thường và liên hệ với đại diện hỗ trợ của chúng tôi để được giúp đỡ như được mô tả trong phần "*Muốn được giúp*" (p. 162).

27. LOẠI BỎ PHẦN MỀM ĐỘC HẠI KHỎI HỆ THỐNG CỦA BẠN

Phần mềm độc hại có thể ảnh hưởng đến hệ thống của bạn bằng nhiều cách khác nhau và phương pháp tiếp cận của Bitdefender phụ thuộc vào kiểu tấn công của phần mềm độc hại. Vì mã độc thay đổi hành vi của chúng thường xuyên, rất khó để thiết lập một khuôn mẫu cho hành vi và hành động của chúng.

Có những tình huống mà Bitdefender có thể sẽ không tự động loại bỏ được các phần mềm độc hại lây nhiễm ra khỏi hệ thống của bạn. Trường hợp này đòi hỏi sự can thiệp của bạn.

- "*Bitdefender Chế độ cứu hộ (Cứu hộ trong môi trường Windows 10)*" (p. 151)
- "*Phải làm gì khi Bitdefender tìm thấy các mối đe dọa trên máy tính của bạn?*" (p. 155)
- "*Làm thế nào để làm sạch virus trong một tập tin nén?*" (p. 156)
- "*Làm thế nào để làm sạch mã độc trong một e-mail nén?*" (p. 157)
- "*Phải làm gì nếu tôi nghi ngờ một tập tin là nguy hiểm?*" (p. 158)
- "*Các tập tin có mật khẩu bảo vệ trong các bản ghi lịch sử quét là gì?*" (p. 159)
- "*Các đối tượng bị bỏ qua được lưu trong các bản ghi lịch sử quét là gì?*" (p. 159)
- "*Các tập tin nén quá nhiều lớp trong các bản ghi lịch sử quét là gì?*" (p. 159)
- "*Tại sao Bitdefender tự động xóa một tập tin bị nhiễm?*" (p. 160)

Nếu bạn không thể tìm thấy vấn đề của bạn ở đây, hoặc nếu các giải pháp trình bày không giải quyết được vấn đề, bạn có thể liên lạc với hỗ trợ kỹ thuật Bitdefender như đã trình bày trong chương "*Muốn được giúp*" (p. 162).

27.1. Bitdefender Chế độ cứu hộ (Cứu hộ trong môi trường Windows 10)

Chế độ cứu hộ là một tính năng Bitdefender cho phép bạn quét và khử nhiễm tất cả các phân vùng ổ cứng bên ngoài hệ điều hành của bạn.

Một khi Bitdefender Antivirus Plus được cài đặt trên **Windows 7, Windows 8 và Windows 8. 1** và tập tin cứu hộ Bitdefender đã được tải về, Chế độ Cứu

hộ có thể là Được sử dụng ngay cả khi bạn không còn có thể khởi động vào Windows được nữa.

Trong Windows 10, Bitdefender Môi trường cứu hộ được tích hợp với Windows RE, có nghĩa là không cần phải tải xuống bất kỳ Hình ảnh chế độ cứu hộ nào trên hệ điều hành này.

Đang tải Bitdefender Rescue Mode Image

Để sử dụng Chế độ Cứu Hộ trong **Windows 7, Windows 8 và Windows 8. 1** , trước hết bạn phải tải tập tin image như sau:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Tại mô đun **Chống virus**, chọn **Chế độ cứu hộ**.
3. Nhấp vào **YES** trong cửa sổ xác nhận xuất hiện để khởi động lại máy tính của bạn.

   Đợi cho Tải xuống tập tin Bitdefender Rescue Mode Image từ các máy chủ Bitdefender. Ngay khi quá trình tải xuống kết thúc, máy tính sẽ khởi động lại.

   Một trình đơn xuất hiện nhắc bạn chọn một hệ điều hành. Ở bước này, bạn có thể chọn để khởi động hệ thống ở Chế độ Cứu Hộ hoặc ở chế độ bình thường.

Ghi chú

Do được tích hợp với Windows Recovery Environment trong **Windows 10** , bạn không cần phải tải bất kỳ Rescue Mode Image nào trên hệ điều hành này.

Khởi động hệ thống ở Chế độ Cứu hộ trong Windows 7, Windows 8 và Windows 8.1

Bạn có thể vào Chế độ cứu hộ theo một trong hai cách:

Từ giao diện Bitdefender.

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Tại mô đun **Chống virus**, chọn **Chế độ cứu hộ**.
3. Nhấp vào **YES** trong cửa sổ xác nhận xuất hiện để khởi động lại máy tính của bạn.

4. Sau khi khởi động lại máy tính, một trình đơn xuất hiện yêu cầu bạn chọn một hệ điều hành. Chọn **Chế độ cứu hộ Bitdefender** để khởi động vào môi trường Bitdefender mà bạn có thể làm sạch ổ đĩa Windows.
5. Nếu được nhắc nhở, nhấn **Enter** và chọn độ phân giải màn hình bạn thường sử dụng. Nhấn **Enter** lần nữa.

   Chế độ cứu hộ của Bitdefender nạp trong vài phút.

Khởi động máy tính của bạn trực tiếp vào Chế độ cứu hộ

Nếu Windows không khởi động, bạn có thể khởi động máy tính của bạn trực tiếp vào Chế độ cứu hộ Bitdefender bằng cách làm theo các bước dưới đây:

- Trong **Windows 7**:
  1. Nhấn phím **F8** cho đến khi màn hình **Advanced Boot Options** xuất hiện.
  2. Sử dụng các phím mũi tên để chọn Bitdefender Rescue Mode, sau đó nhấn **Enter** .

     Chế độ cứu hộ của Bitdefender sẽ được nạp trong vài phút.
- Trong **Windows 8 and Windows 8.1**:
  1. Nhấn phím **Shift** cho đến khi màn hình **Advanced Startup Options** xuất hiện.
  2. Chọn tùy chọn **Sử dụng hệ điều hành khác** và sau đó chọn Bitdefender Rescue Mode.

     Chế độ cứu hộ của Bitdefender sẽ được nạp trong vài phút.

Ghi chú

Chỉ có thể chạy máy tính của bạn ở chế độ Cứu Hộ nếu tập tin escue Mode Image đã được tải xuống trước đây như được mô tả trong “Đang tải Bitdefender Rescue Mode Image” (p. 152).

Khởi động hệ thống ở môi trường cứu hộ trong Windows 10

Bạn chỉ có thể vào Môi Trường Cứu Hộ từ sản phẩm Bitdefender, như sau:

1. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
2. Tại mô đun **Chống virus**, chọn **Chế độ cứu hộ**.

3. Nhấp vào **Khởi động lại** tại cửa sổ hiện ra.

   Môi Trường Cứu Hộ của Bitdefender sẽ được nạp trong vài phút.

Quét hệ thống của bạn ở chế độ Cứu hộ (Môi trường Cứu trợ trong Windows 10)

Để quét hệ thống của bạn ở Chế độ Cứu Hộ (Môi trường Cứu Hộ):

- Trong **Windows 7, Windows 8 và Windows 8.1**:

  1. Vào Chế độ cứu hộ, như được mô tả trong "Khởi động hệ thống ở Chế độ Cứu hộ trong Windows 7, Windows 8 và Windows 8.1" (p. 152).
  2. Logo Bitdefender sẽ xuất hiện và các công cụ bảo mật sẽ bắt đầu được sao chép.
  3. Một cửa sổ chào mừng sẽ xuất hiện. Nhấp **Tiếp tục**.
  4. Cập nhật cơ sở dữ liệu về mối đe dọa được bắt đầu.
  5. Sau khi cập nhật hoàn tất, cửa sổ Quét virus theo yêu cầu của Bitdefender sẽ xuất hiện.
  6. Nhấp **Quét ngay**, chọn mục tiêu quét trong cửa sổ xuất hiện và sau đó nhấn **Mở** để bắt đầu quét.

     Bạn nên quét toàn bộ phân vùng Windows.

     > **Ghi chú**
     > Khi làm việc trong Chế độ cứu hộ, bạn đang làm việc với tên phân vùng theo quy ước của Linux. Phân vùng đĩa sẽ xuất hiện như sda1 có thể tương ứng với kiểu phân vùng (C:) trong Windows , sda2 tương ứng với (D:) và tiếp theo.

  7. Chờ cho quá trình quét hoàn tất. Nếu phát hiện bất kỳ mối đe dọa nào, hãy làm theo hướng dẫn để xóa nó.
  8. Để thoát khỏi Chế độ cứu hộ, nhấp chuột phải vào vùng trống trên màn hình, chọn **Thoát** từ trình đơn hiện ra và sau đó chọn khởi động lại hoặc tắt máy tính.

- Trong **Windows 10**:

  1. Vào Chế độ cứu hộ, như được mô tả trong "Khởi động hệ thống ở môi trường cứu hộ trong Windows 10" (p. 153).

2. Quá trình quét Bitdefender bắt đầu tự động ngay sau khi hệ thống được nạp vào Môi trường Cứu Hộ.
3. Chờ cho quá trình quét hoàn tất. Nếu phát hiện bất kỳ mối đe dọa nào, hãy làm theo hướng dẫn để xóa nó.
4. Để thoát khỏi Môi trường Cứu Hộ, nhấp vào nút **Đóng** trong cửa sổ với kết quả quét.

27.2. Phải làm gì khi Bitdefender tìm thấy các mối đe dọa trên máy tính của bạn?

Bạn có thể thấy có một mối đe dọa trên máy tính của bạn theo một trong những cách sau:

- Bạn quét máy tính của bạn và Bitdefender tìm thấy những tập tin bị nhiễm virus.
- Một cảnh báo về mã độc cho bạn biết rằng Bitdefender đã chặn một hoặc nhiều mã độc trên máy tính của bạn.

Trong tình huống như vậy, cập nhật Bitdefender để chắc chắn rằng bạn có mẫu chữ ký phần mềm độc hại mới nhất và chạy lệnh Quét hệ thống để phân tích.

Ngay sau khi việc quét hệ thống kết thúc, chọn hành động mong muốn cho các tập tin bị nhiễm virus (Khử nhiễm, xóa, cách ly).

Cảnh báo

Nếu bạn nghi ngờ tập tin là một phần của hệ điều hành Windows hoặc nó không phải là một tập tin bị nhiễm, không làm gì và liên hệ Chăm sóc khách hàng Bitdefender càng sớm càng tốt.

Nếu hành động được lựa chọn không thể được thực hiện và các bản ghi cho thấy tập tin bị lây nhiễm không thể bị xóa, bạn phải loại bỏ các tập tin theo cách thủ công:

Phương pháp đầu tiên có thể được sử dụng ở chế độ bình thường:

1. Tắt chế độ bảo vệ theo thời gian thực của Bitdefender:
   a. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
   b. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
   c. Trong cửa sổ **Shield** , tắt **Bitdefender Shield** .

2. Hiển thị các đối tượng ẩn trong Windows. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để hiển thị các đối tượng ẩn trong Windows?*" (p. 65).
3. Tìm đến vị trí của tập tin bị nhiễm virus (kiểm tra các bản nghi nhật ký) và xóa nó.
4. Bật chế độ bảo vệ theo thời gian thực của Bitdefender.

Trong trường hợp các phương pháp đầu tiên thất bại trong việc loại bỏ nhiễm :

1. Khởi động lại hệ thống của bạn và đăng nhập vào trong chế độ Safe Mode. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để khởi động vào chế độ An toàn?*" (p. 67).
2. Hiển thị các đối tượng ẩn trong Windows. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để hiển thị các đối tượng ẩn trong Windows?*" (p. 65).
3. Tìm đến vị trí của tập tin bị nhiễm virus (kiểm tra các bản nghi nhật ký) và xóa nó.
4. Khởi động lại hệ thống của bạn ở chế độ bình thường.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

27.3. Làm thế nào để làm sạch virus trong một tập tin nén?

Một kho lưu trữ là một tập tin hoặc một tập hợp các tập tin nén theo một định dạng đặc biệt để giảm không gian trên đĩa cần thiết để lưu trữ các tập tin.

Một số các định dạng là định dạng mở, do đó cho phép Bitdefender quét bên trong chúng và có những hành động thích hợp tiếp theo để loại bỏ virus.

Một số định dạng lưu trữ khác sẽ bị đóng một phần hoặc đóng hoàn toàn, vì vậy Bitdefender chỉ có thể phát hiện sự hiện diện của virus có trong đó, nhưng không thể thực hiện bất kỳ hành động nào khác.

Nếu Bitdefender thông báo cho bạn rằng một loại virus đã được phát hiện trong một nơi lưu trữ và không có hành động nào được thực hiện, có nghĩa là việc loại bỏ virus này là không thể.

Đây là cách bạn có thể làm sạch virus trong một tập tin nén:

1. Xác định lưu trữ có chứa vi rút bằng cách thực hiện Quét hệ thống.
2. Tắt chế độ bảo vệ theo thời gian thực của Bitdefender:
   a. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.
   b. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .
   c. Trong cửa sổ **Shield** , tắt **Bitdefender Shield** .
3. Tìm đến nơi chứa tập tin nén và giải nén nó bằng cách sử dụng một ứng dụng giải nén, như WinZip.
4. Xác định các tập tin bị nhiễm và xóa nó.
5. Xóa tập tin nén gốc để đảm bảo sự lây nhiễm được loại bỏ hoàn toàn.
6. Nén lại các tập tin trong một tập tin nén mới sử dụng một ứng dụng nén, như WinZip.
7. Bật Bảo vệ chống virus thời gian thực của Bitdefender và chạy Quét hệ thống để đảm bảo không có virus khác tồn tại trên hệ thống.

Ghi chú
Điều quan trọng cần lưu ý rằng mã độc được nén trong một tập tin nén chưa phải là mối đe dọa trực tiếp đến hệ thống của bạn, vì mã độc cần được giải nén và kích hoạt mới có thể lây nhiễm lên hệ thống của bạn.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

27.4. Làm thế nào để làm sạch mã độc trong một e-mail nén?

Bitdefender cũng có thể xác định mã độc trong dữ liệu e-mail và các lưu trữ e-mail được lưu trữ trên đĩa.

Đôi khi cần thiết phải xác định các email bị nhiễm virus bằng cách sử dụng thông tin có trong các báo cáo sau khi quét, và xóa nó một cách thủ công.

Đây là cách bạn có thể làm sạch mã độc được trong một kho lưu trữ email:

1. Dung Bitdefender quét cơ sở dữ liệu e-mail.
2. Tắt chế độ bảo vệ theo thời gian thực của Bitdefender:
   a. Nhấp vào **Bảo vệ** trên menu điều hướng trên giao diện Bitdefender.

b. Trong ngăn **ANTIVIRUS** , nhấp vào **Cài đặt** .

c. Trong cửa sổ **Shield** , tắt **Bitdefender Shield** .

3. Mở báo cáo quét và sử dụng các thông tin nhận dạng (Chủ đề, Gửi từ, Đến) của các email bị nhiễm virus để xác định đúng e-mail cần xử lý.
4. Xóa các email bị nhiễm virus. Hầu hết các ứng dụng e-mail cũng dời các tin nhắn đã bị xóa vào một thư mục phục hồi, từ đó có thể khôi phục lại email đã bị xóa. Bạn nên chắc chắn rằng các email cũng bị xóa khỏi thư mục phục hồi này.
5. Nén lại các thư mục lưu trữ các tin nhắn bị nhiễm virus.
   - Trong Microsoft Outlook 2007: Từ trình đơn File, nhấp mục Quản lý file dữ liệu. Chọn tập tin lưu trữ cá nhân (.pst) cần nén, nhấp Cài đặt. Nhấp Nén ngay.
   - Trong Microsoft Outlook 2010 / 2013 / 2016: Trên trình đơn File, nhấp vào Thông tin và sau đó Cài đặt tài khoản (Thêm và loại bỏ các tài khoản hoặc thay đổi cài đặt kết nối hiện tại). Sau đó nhấp vào Tập tin dữ liệu, chọn thư mục cá nhân (.pst). Tập tin mà bạn có ý định nén lại, và bấm Cài đặt. Nhấp Nén ngay.
6. Bật chế độ bảo vệ theo thời gian thực của Bitdefender.

Nếu thông tin này không hữu ích, bạn có thể liên hệ với hỗ trợ Bitdefender như mô tả trong phần "*Muốn được giúp*" (p. 162).

27.5. Phải làm gì nếu tôi nghi ngờ một tập tin là nguy hiểm?

Bạn có thể nghi ngờ một tập tin trên hệ thống của bạn là nguy hiểm, ngay cả khi sản phẩm Bitdefender đã không phát hiện ra nó.

Để đảm bảo hệ thống của bạn được bảo vệ:

1. Chạy **Quét hệ thống** với Bitdefender. Để hiểu cách thực hiện việc này, hãy tham khảo "*Làm thế nào để quét hệ thống?*" (p. 51).
2. Nếu kết quả quét cho biết hệ thống là sạch, nhưng bạn vẫn nghi ngờ và muốn chắc chắn về các tập tin, hãy liên hệ với đại diện hỗ trợ của chúng tôi để được giúp đỡ.

   Để hiểu cách thực hiện việc này, hãy tham khảo "*Muốn được giúp*" (p. 162).

27.6. Các tập tin có mật khẩu bảo vệ trong các bản ghi lịch sử quét là gì?

Đây là thông báo chỉ ra rằng Bitdefender đã phát hiện những tập tin được bảo vệ bằng mật khẩu hoặc một số hình thức mã hóa.

Các tập tin có mật khẩu bảo vệ phổ biến là:

- Các tập tin thuộc về một giải pháp an ninh khác.
- Các tập tin thuộc hệ điều hành.

Để quét được nội dung, những tập tin này sẽ cần được mở hoặc được giải mã.

Nếu tập tin cần được mở, trình Quét thời gian thực của Bitdefender sẽ tự động quét chúng để bảo vệ máy tính của bạn. Nếu bạn muốn Bitdefender quét các tập tin này, bạn phải liên hệ với nhà sản xuất sản phẩm để cung cấp cho bạn thêm chi tiết về chúng.

Bạn có thể bỏ qua các tập tin này bởi vì chúng không phải là một mối đe dọa cho hệ thống của bạn.

27.7. Các đối tượng bị bỏ qua được lưu trong các bản ghi lịch sử quét là gì?

Tất cả các tập tin được bỏ qua có trong báo cáo quét là sạch sẽ.

Để tăng hiệu suất, Bitdefender không quét các tập tin không thay đổi kể từ lần quét cuối.

27.8. Các tập tin nén quá nhiều lớp trong các bản ghi lịch sử quét là gì?

Các tập tin nén quá nhiều lớp là những đối tượng không thể được mở bởi động cơ quét hoặc các đối tượng đòi hỏi thời gian giải mã sẽ rất lâu khiến hệ thống không ổn định.

Nén quá nhiều lớp có nghĩa là Bitdefender bỏ qua việc quét chúng vì tốn quá nhiều tài nguyên hệ thống. Nội dung của chúng sẽ được quét lúc truy cập thời gian thực, nếu cần thiết.

27.9. Tại sao Bitdefender tự động xóa một tập tin bị nhiễm?

Nếu một tập tin bị nhiễm được phát hiện, Bitdefender sẽ tự động cố gắng để khử nhiễm nó. Nếu khử nhiễm thất bại, các tập tin sẽ được chuyển đến khu vực cách ly.

Đối với phần mềm độc hại cụ thể, khử nhiễm là không thể vì các tập tin được phát hiện hoàn toàn độc hại. Trong trường hợp này, các tập tin bị nhiễm sẽ bị xóa khỏi đĩa.

Thường là trường hợp xảy ra với các tập tin cài đặt được tải về từ các trang web không đáng tin cậy. Nếu bạn gặp tình huống như vậy, hãy tải về tập tin cài đặt từ trang web của nhà sản xuất hoặc trang web đáng tin cậy khác.

LIÊN HỆ CHÚNG TÔI

28. MUỐN ĐƯỢC GIÚP

Bitdefender cung cấp cho khách hàng của mình sự hỗ trợ nhanh chóng và chính xác. Nếu bạn gặp bất kỳ vấn đề hoặc nếu bạn có bất kỳ câu hỏi về sản phẩm Bitdefender, bạn có thể sử dụng một số nguồn trực tuyến để tìm một giải pháp hay một câu trả lời. Đồng thời, bạn có thể liên lạc với đội chăm sóc khách hàng của Bitdefender. Đại diện hỗ trợ của chúng tôi sẽ trả lời câu hỏi của bạn một cách kịp thời và sự hỗ trợ cần thiết.

Phần "*Giải quyết các vấn đề phổ biến*" (p. 138) cung cấp các thông tin cần thiết liên quan đến các vấn đề thường gặp nhất bạn có thể gặp phải khi sử dụng sản phẩm này.

Nếu bạn không tìm thấy câu trả lời cho câu hỏi của bạn từ các nguồn cung cấp, bạn có thể liên hệ trực tiếp:

- "Liên hệ trực tiếp với chúng tôi từ Bitdefender Antivirus Plus" (p. 162)
- "Liên hệ với chúng tôi qua Trung tâm Hỗ trợ trực tuyến" (p. 163)

Liên hệ trực tiếp với chúng tôi từ Bitdefender Antivirus Plus

Nếu bạn có một kết nối Internet, bạn có thể liên hệ Bitdefender để được hỗ trợ trực tiếp từ giao diện sản phẩm.

Theo những bước sau:

1. Nhấp vào **Hỗ trợ** trên menu điều hướng trên giao diện Bitdefender .
2. Bạn có các tùy chọn sau đây:
   - **Hướng dẫn sử dụng**

     Truy cập vào cơ sở dữ liệu của chúng tôi và tìm kiếm các thông tin cần thiết.
   - **Trung tâm hỗ trợ**

     Truy cập các bài viết trực tuyến và hướng dẫn bằng video của chúng tôi.
   - **Liên hệ Hỗ trợ**

     Sử dụng nút **Liên hệ Hỗ trợ** để khởi động công cụ hỗ trợ Bitdefender và liên lạc với Bộ phận Chăm sóc Khách hàng.

a. Hoàn thành việc điền thông tin vào mẫu với các dữ liệu cần thiết:

i. Chọn loại sự cố bạn đã gặp phải.

ii. Nhập vào mô tả vấn đề bạn gặp phải.

iii. Nhấp vào **THỬ TẠO LẠI VẤN ĐỀ** trong trường hợp bạn đang gặp vấn đề về sản phẩm. Tái tạo vấn đề, và sau đó nhấp vào **KẾT THÚC** trong khung TÁI BẢN.

iv. Nhấp vào **Xác nhận phiếu** .

b. Tiếp tục hoàn thành mẫu đăng ký với các dữ liệu cần thiết:

i. Nhập tên đầy đủ của bạn.

ii. Nhập vào địa chỉ e-mail của bạn.

iii. Chọn hộp kiểm thỏa thuận.

iv. Nhấp vào **TẠO GÓI GỠ LỖI**.

Xin vui lòng chờ một vài phút trong khi Bitdefender tập hợp thông tin liên quan. Thông tin này sẽ giúp các kỹ sư của chúng tôi tìm ra giải pháp cho vấn đề của bạn.

c. Nhấp **Đóng** để thoát khỏi tiện ích. Bạn sẽ được một trong những đại diện của chúng tôi liên lạc ngay khi có thể.

Liên hệ với chúng tôi qua Trung tâm Hỗ trợ trực tuyến

Nếu bạn không thể truy cập các thông tin cần thiết bằng cách sử dụng sản phẩm Bitdefender, tham khảo Trung tâm Hỗ trợ trực tuyến của chúng tôi:

1. Đi tới http://www.bitdefender.com/support/consumer.html.

   Trung tâm hỗ trợ Bitdefender lưu giữ rất nhiều bài báo có chứa các giải pháp cho các vấn đề liên quan tới Bitdefender.

2. Sử dụng thanh tìm kiếm ở trên cùng của cửa sổ để tìm các bài viết có thể cung cấp một giải pháp cho vấn đề của bạn. Để tìm kiếm, chỉ cần gõ một từ trong thanh tìm kiếm và nhấn **Tìm kiếm**.

3. Đọc những bài báo hoặc tài liệu liên quan và thử các giải pháp đề xuất.

4. Nếu giải pháp này không giải quyết vấn đề của bạn, hãy tới

   http://www.bitdefender.com/support/contact-us.htmlvà liên hệ với đại diện hỗ trợ của chúng tôi.

29. NGUỒN THÔNG TIN TRỰC TUYẾN

Một số thông tin trực tuyến có sẵn có thể giúp bạn giải quyết các vấn đề và các câu hỏi liên quan Bitdefender.

- Trung tâm hỗ trợ Bitdefender:

  http://www.bitdefender.com/support/consumer.html

- Diễn đàn Hỗ trợ Bitdefender:

  http://forum.bitdefender.com

- Cổng thông tin an ninh máy tính HOTforSecurity:

  http://www.hotforsecurity.com

Bạn cũng có thể sử dụng công cụ tìm kiếm ưa thích của mình để tìm hiểu thêm thông tin về an ninh máy tính, sản phẩm Bitdefender và công ty.

29.1. Trung tâm hỗ trợ Bitdefender

Trung tâm hỗ trợ Bitdefender là một kho lưu trữ trực tuyến các thông tin về sản phẩm Bitdefender. Nó lưu trữ thông tin theo một định dạng cơ bản dễ dàng truy cập, báo cáo về kết quả hỗ trợ kỹ thuật liên tục và các hoạt động sửa lỗi của bộ phận hỗ trợ và phát triển sản phẩm Bitdefender. cùng với các bài viết chung về phòng chống đe dọa, giải pháp Bitdefender cùng với các giải thích chi tiết và nhiều bài viết khác.

Trung tâm hỗ trợ Bitdefender được mở cho công chúng truy cập miễn phí. Các thông tin mở rộng có tại đó cung cấp thêm phương tiện tới khách hàng Bitdefender những kiến thức kỹ thuật và cái nhìn sâu sắc mà họ cần. Tất cả các yêu cầu hợp lệ về thông tin hoặc sửa lỗi đến từ khách hàng Bitdefender cuối cùng đều tìm đến Trung tâm hỗ trợ Bitdefender, như báo cáo sửa lỗi, mẹo, hoặc các bài viết sẽ bổ sung cho tài liệu trợ giúp của sản phẩm.

Trung tâm hỗ trợ Bitdefender sẵn sàng mọi lúc tại

http://www.bitdefender.com/support/consumer.html.

29.2. Diễn đàn Hỗ trợ Bitdefender

Diễn đàn hỗ trợ Bitdefender cung cấp trợ giúp tới người sử dụng Bitdefender một cách dễ dàng.

Nếu sản phẩm Bitdefender của bạn không hoạt động tốt, hoặc nếu nó không thể loại bỏ mã độc khỏi máy tính của bạn hoặc nếu bạn có câu hỏi về cách làm việc của chương trình, hãy đưa vấn đề hoặc câu hỏi của bạn lên diễn đàn này.

Các kỹ thuật viên hỗ trợ của Bitdefender luôn theo dõi các bài viết mới trên diễn đàn để hỗ trợ bạn. Bạn cũng có thể nhận được câu trả lời và giải pháp từ người dùng có kinh nghiệm về Bitdefender.

Trước khi gửi bài về vấn đề hoặc câu hỏi của bạn, hãy tìm kiếm thông tin bạn cần từ chủ đề tương tự hoặc liên quan đang có trên diễn đàn.

Diễn đàn hỗ trợ Bitdefender có sẵn tại http://forum.bitdefender.com, với 5 ngôn ngữ khác nhau: Anh, Đức, Pháp, Tây Ban Nha và Rumani. Nhấp vào liên kết **Home & Home Office Protection** để truy cập vào phần dành riêng cho các sản phẩm tiêu dùng.

29.3. Cổng thông tin HOTforSecurity

HOTforSecurity là một nguồn thông tin bảo mật máy tính phong phú. Tại đây bạn có thể tìm hiểu về rất nhiều nguy cơ an ninh mà máy tính của bạn có thể gặp phải khi kết nối Internet (phần mềm độc hại, lừa đảo, thư rác, tội phạm mạng).

Các bài báo mới được đăng tải thường xuyên cập nhật về những mối đe dọa mới nhất được phát hiện, các xu hướng an ninh hiện tại và các thông tin khác về ngành công nghiệp bảo mật máy tính.

Trang web HOTforSecurity là http://www.hotforsecurity.com.

30. THÔNG TIN LIÊN HỆ

Trao đổi thông tin là chìa khoá cho kinh doanh thành công. Từ năm 2001, BITDEFENDER đã tạo nên một danh tiếng không thể nghi ngờ bằng cách liên tục phấn đấu để truyền thông tốt hơn và vượt ngoài mong đợi của khách hàng và đối tác của chúng tôi. Nếu bạn có bất cứ câu hỏi nào, hãy liên hệ với chúng tôi.

30.1. Các địa chỉ Web

Bộ phận Bán hàng: sales@bitdefender.com
Trung tâm hỗ trợ:http://www.bitdefender.com/support/consumer.html
Tài liệu: documentation@bitdefender.com
Các nhà phân phối địa phương: http://www.bitdefender.com/partners
Đối tác: partners@bitdefender.com
Media Relations: pr@bitdefender.com
Nghề nghiệp: jobs@bitdefender.com
Gửi thông tin mối đe dọa: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Trang Webhttp://www.bitdefender.com

30.2. Các nhà phân phối địa phương

Các nhà phân phối Bitdefender sẵn sàng đáp ứng mọi yêu cầu liên quan đến lĩnh vực hoạt động của họ, cả về vấn đề thương mại lẫn các vấn đề chung.

Để tìm một nhà phân phối Bitdefender tại quốc gia của bạn:

1. Đi tới http://www.bitdefender.com/partners/partner-locator.html.
2. Chọn quốc gia và thành phố của bạn bằng cách sử dụng các tùy chọn tương ứng.
3. Nếu bạn không tìm thấy một nhà phân phối Bitdefender tại quốc gia của bạn, hãy liên hệ với chúng tôi bằng e-mail tại sales@bitdefender.com. Xin vui lòng viết e-mail của bạn bằng tiếng Anh để chúng tôi có thể hỗ trợ bạn kịp thời.

30.3. Văn phòng của Bitdefender

Các văn phòng Bitdefender sẵn sàng đáp ứng bất cứ yêu cầu liên quan đến lĩnh vực hoạt động của mình, cả về thương mại và các vấn đề chung. Các địa chỉ liên lạc tương ứng được liệt kê dưới đây.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Điện thoại (văn phòng&bán hàng): 1-954-776-6262
Sales: sales@bitdefender.com
Hỗ trợ kỹ thuật: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Anh quốc và Ai-xơ-len

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Email: info@bitdefender.co.uk
Điện thoại: (+44) 2036 080 456
Sales: sales@bitdefender.co.uk
Hỗ trợ kỹ thuật: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Đức

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Văn phòng: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Sales: vertrieb@bitdefender.de
Hỗ trợ kỹ thuật: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Denmark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Văn phòng: +45 7020 2282
Hỗ trợ kỹ thuật: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Tây ban nha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Điện thoại: +34 902 19 07 65
Sales: comercial@bitdefender.es
Hỗ trợ kỹ thuật: https://www.bitdefender.es/support/consumer.html
Trang Web https://www.bitdefender.es

Rumani

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax: +40 21 2641799
Điện thoại bán hàng: +40 21 2063470
Email bán hàng: sales@bitdefender.ro
Hỗ trợ kỹ thuật: https://www.bitdefender.ro/support/consumer.html
Trang Web https://www.bitdefender.ro

Các Tiểu vương quốc Ả-rập thống nhất

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Điện thoại bán hàng: 00971-4-4588935 / 00971-4-4589186
Email bán hàng: mena-sales@bitdefender.com
Hỗ trợ kỹ thuật: https://www.bitdefender.com/support/consumer.html
Trang Web https://www.bitdefender.com

Sổ tay thuật ngữ

Bộ nhớ

Vùng lưu trữ trong máy tính. Thuật ngữ bộ nhớ mô tả kho dữ liệu dưới dạng các con chíp, và từ kho dữ liệu được sử dụng cho các bộ nhớ tồn tại trên băng hay đĩa. Mỗi máy tính có một dung lượng bộ nhớ vật lý nào đó, và thường được nói đến như bộ nhớ chính hay bộ nhớ Truy cập ngẫu nhiên.

Các chương trình đóng gói

Một tập tin trong một định dạng nén. Nhiều hệ điều hành và các ứng dụng chứa các câu lệnh cho phép bạn đóng gói một tập tin để nó chiếm ít bộ nhớ hơn. Ví dụ, bạn có một tập tin văn bản có chứa mười ký tự trống liên tiếp. Thông thường, điều đó đòi hỏi phải có mười bytes lưu trữ.

Tuy nhiên, một chương trình sẽ gói gọn các tập tin này sẽ thay thế các ký tự trống bằng một ký tự đại diện đặc biệt. Trong trường hợp này, mười chỗ trống chỉ dùng đến 2 bytes. Đây chỉ là một kỹ thuật gói gọn - ngoài ra còn nhiều thứ khác hơn nữa.

Các mục tự chạy

Bất kỳ tập tin nào trong thư mục này sẽ được mở khi máy tính khởi động. Ví dụ, trên màn hình khởi động, một tập tin âm thanh được chạy khi máy tính khởi động, một lịch nhắc việc, hay các chương trình ứng dụng có thể là các mục tự khởi động. Thông thường, bí danh của một tập tin được đặt trong thư mục này chứ không phải tại chính tập tin đó.

Các virus dưới dạng macros

Một dạng mã độc máy tính được mã hóa dưới dạng macro nhúng trong tài liệu. Nhiều ứng dụng như Microsoft Word và Excel, có ngôn ngữ macro rất mạnh.

Các ứng dụng này cho phép nhúng macro trong tài liệu, và macro sẽ được kích hoạt tại thời điểm tài liệu được mở.

Cập nhật

Một phiên bản mới của sản phẩm phần mềm hoặc phần cứng được thiết kế để thay thế phiên bản cũ của cùng một sản phẩm. Ngoài ra, các bản cập nhật thường xuyên kiểm tra xem phiên bản cũ đã được cài đặt trên máy tính của bạn chưa, nếu không, bạn không thể cài đặt bản cập nhật.

Bitdefender có tính năng cập nhật riêng cho phép bạn kiểm tra cập nhật theo cách thủ công hoặc để nó tự động cập nhật.

Cập nhật thông tin về mối đe dọa:
Mô hình nhị phân của một mã độc, được sử dụng bởi các giải pháp bảo mật để phát hiện và loại bỏ các mối đe dọa.

Cổng
Là một giao diện trên máy tính mà bạn có thể gắn thiết bị vào đó. Máy tính cá nhân có rất nhiều loại cổng. Xét về thiết bị nội bộ, có vài cổng nối ổ cứng, màn hình, và bàn phím. Xét về thiết bị ngoại vi, máy tính cá nhân có cổng để nối modem, máy in, chuột, và các thiết bị ngoại vi khác.

Trong mạng TCP/IP và UDP, một điểm cuối tới một kết nối lô gích. Số hiệu cổng kết nối xác định nó là loại cổng nào. Ví dụ, cổng 80 được sử dụng cho giao thức HTTP.

Công nghệ ActiveX
ActiveX là một khuôn mẫu để viết các chương trình cho phép các chương trình và hệ điều hành khác có thể gọi tới. Công nghệ ActiveX được sử dụng với Microsoft Internet Explorer để làm cho các trang web tương tác được với người dùng, chứ không phải là các trang tĩnh. Với ActiveX, người dùng có thể hỏi và trả lời câu hỏi, sử dụng các nút nhấn và tương tác với trang web theo cách thức mới. Điều khiển ActiveX thường được viết bằng Visual Basic.

Công nghệ Active X là một nguy cơ đáng chú ý việc thiếu hoàn toàn các kiểm soát an ninh, các chuyên gia bảo mật máy tính không khuyến khích sử dụng nó trên internet.

Cookie
Trong ngành công nghiệp Internet, cookies được mô tả là tập tin nhỏ có chứa thông tin về máy tính cá nhân có thể được phân tích và được sử dụng bởi các nhà quảng cáo để tìm hiểu sở thích và thói quen của bạn. Trong lĩnh vực này, công nghệ cookie vẫn đang được phát triển và chủ định của nó là để nhắm vào mục tiêu quảng cáo trực tiếp đến những gì bạn yêu thích. Đó là một con dao hai lưỡi đối với nhiều người bởi vì một mặt, nó hiệu quả và xác đáng khi bạn chỉ xem quảng cáo về những gì bạn đang quan tâm. Mặt khác, nó bao gồm "theo dõi" và "lần theo" nơi bạn đến và bạn nhấn chuột vào cái gì. Tuy dễ hiểu như vậy, vẫn có một cuộc tranh luận về tính riêng tư và nhiều người cảm thấy bị xúc phạm

khi biết được rằng họ được xem như là một "Mã số" (bạn đã biết, mã vạch trên mặt sau của gói hàng để quét tại nơi xếp hàng thanh toán tại các cửa hàng tạp hóa). Trong khi quan điểm này có thể là cực đoan, trong một số trường hợp nó là chính xác.

Cửa sau

Một lỗ hổng an ninh hệ thống được để lại bởi người thiết kế hay người bảo dưỡng một cách có tính toán. Động cơ của những lỗ hổng này thường không vì mục đích xấu; một vài hệ điều hành, ví dụ, được mở ra trước một tài khoản ưu tiên dành riêng cho kỹ thuật viên hay lập trình viên thực hiện bảo dưỡng sản phẩm do họ cung cấp.

Cung khởi động

Cung khởi động nằm ngay vị trí đầu tiên của đĩa cứng sẽ chứa nhận dạng cấu trúc của đĩa (độ lớn cung, độ lớn liên cung, v.v). Đối với đĩa khởi động, cung khởi động cũng chứa chương trình để tải lên hệ điều hành.

Đăng ký

Hợp đồng mua bán cung cấp cho người sử dụng quyền sử dụng một sản phẩm hoặc dịch vụ cụ thể trên một số thiết bị cụ thể và trong một thời gian nhất định. Một thuê bao đã hết hạn có thể được tự động gia hạn sử dụng các thông tin được cung cấp bởi người sử dụng tại đơn hàng đầu tiên.

Dòng lệnh

Trong giao diện dòng lệnh, người dùng có thể đánh lệnh trong khoảng trống được cấp ngay trên màn hình, sử dụng ngôn ngữ lệnh.

Đường dẫn

Các hướng dẫn chính xác dẫn đến một tập tin trên máy tính. Những hướng dẫn này thường được mô tả bằng các phương tiện của hệ thống tập tin phân cấp từ trên xuống.

Đường dẫn giữa hai điểm, giống như các kênh giao tiếp giữa hai máy tính.

Email

Thư điện tử. Một dịch vụ gửi tin nhắn giữa các máy tính thông qua mạng cục bộ hay mạng toàn cầu.

Giả danh

Một hệ thống máy tính mồi được thiết lập nhằm thu hút các hacker để nghiên cứu cách thức chúng hành động và xác định các phương pháp khác thường được sử dụng để thu thập thông tin hệ thống. Các công ty và các tập đoàn quan tâm nhiều hơn trong việc thực hiện và sử dụng giả danh để cải thiện tình trạng tổng thể của họ về an ninh.

Giao thức internet

Giao thức internet là một giao thức có thể định hướng trong tập các giao thức TCP/IP mà có trách nhiệm định địa chỉ IP, định đường, và phân mảnh cũng như tái gộp các gói IP.

Giao thức TCP/IP

Transmission Control Protocol/Internet Protocol - Một tập hợp các giao thức mạng sử dụng rộng rãi trên Internet cho phép cung cấp thông tin liên lạc thông qua mạng kết nối của máy tính với các kiến trúc phần cứng khác nhau và các hệ điều hành khác nhau. TCP / IP bao gồm các tiêu chuẩn về cách các máy tính giao ước cho việc kết nối mạng và định tuyến.

kẻ xấu trên mạng

Khi đồng nghiệp hoặc người lạ có hành vi ngược đãi trẻ em nhằm mục đích gây tổn thương về thể xác. Để gây tổn hại về mặt cảm xúc, những kẻ tấn công gửi tin nhắn có ý nghĩa hoặc những bức ảnh không đẹp, do đó khiến nạn nhân của chúng bị cô lập với người khác hoặc cảm thấy tuyệt vọng.

Khai thác

Một cách để tận dụng các lỗi hoặc lỗ hổng khác nhau có trong máy tính (phần mềm hoặc phần cứng). Do đó, tin tặc có thể giành quyền kiểm soát máy tính hoặc hệ thống mạng.

Khay hệ thống

Được giới thiệu trong Windows 95, khay hệ thống được đặt tại thanh nhiệm vụ trong Windows (thường là nằm phía dưới cạnh đồng hồ), bao gồm các biểu tượng nhỏ cho phép truy cập một cách dễ dàng hơn tới các chức năng hệ thống như fax, máy in, modem, âm lượng và nhiều thứ khác nữa. Nhấp đúp chuột hoặc kích chuột phải vào một biểu tượng để xem và truy cập các chi tiết.

Lừa đảo

Hành động gửi một thư điện tử tới một người sử dụng nào đó, nói rằng mình là một cá nhân hợp pháp nhằm yêu cầu người sử dụng cung cấp các thông tin cá nhân được dùng để ăn trộm thông tin định dạng . Các e-mail hướng người dùng đến thăm một trang web nơi họ được yêu cầu cập nhật thông tin cá nhân, chẳng hạn như mật khẩu và thẻ tín dụng, số an sinh xã hội, và số tài khoản ngân hàng sử dụng bởi các tổ chức hợp pháp. Trang web, tuy nhiên, là trang ma được dựng lên nhằm ăn cắp thông tin người dùng.

Mã kích hoạt

Là một mã duy nhất mà có thể được mua từ bán lẻ và được sử dụng để kích hoạt một sản phẩm hoặc dịch vụ cụ thể. Một mã kích hoạt cho phép kích hoạt của một thuê bao hợp lệ trong một thời gian nhất định và số lượng thiết bị và cũng có thể được sử dụng để mở rộng một thuê bao với các điều kiện để được tạo ra cho các sản phẩm hay dịch vụ tương tự.

Mạng máy tính ma

Thuật ngữ "botnet" bao gồm từ "robot" và "network". Botnet được hiểu là thiết bị kết nối Internet bị nhiễm phần mềm độc hại và có thể được sử dụng để gửi thư rác, ăn cắp dữ liệu, điều khiển các thiết bị dễ bị tấn công hoặc lây lan phần mềm gián điệp, mã độc tống tiền và các loại phần mềm độc hại khác. Mục tiêu của chúng là lây nhiễm càng nhiều thiết bị được kết nối càng tốt, chẳng hạn như máy tính cá nhân, máy chủ, thiết bị di động hoặc các thiết bị IoT thuộc các công ty lớn hoặc ngành công nghiệp.

Mạng riêng ảo (VPN)

Là một công nghệ cho phép kết nối trực tiếp tạm thời và được mã hóa với một mạng nào đó qua mạng kém an toàn. Bằng cách này, việc gửi và nhận dữ liệu được an toàn và được mã hóa, việc đánh cắp thông tin sẽ khó khăn. Một bằng chứng về bảo mật là xác thực, có thể được thực hiện chỉ bằng một tên người dùng và mật khẩu.

Máy trạm có chức năng thư điện tử

Ứng dụng email là ứng dụng cho phép bạn gửi và nhận thư điện tử.

Mối đe dọa

Một chương trình hoặc một đoạn mã được tải về máy tính của bạn mà bạn không biết và hoạt động trái với ý muốn của bạn. Phần lớn các mã

độc đều có thể tự nhân bản. Tất cả các mối đe dọa máy tính đều do con người tạo ra. Một mã độc đơn giản có thể tự nhân bản nhiều lần và tương đối dễ dàng để thực hiện việc này. Ngay cả một mã độc đơn giản cũng rất nguy hiểm bởi vì nó sẽ nhanh chóng sử dụng tất cả bộ nhớ có sẵn và làm treo hệ thống. hậm chí một dạng mã độc nguy hiểm hơn có khả năng tự truyền qua mạng, vượt qua cả hệ thống an ninh.

Mối đe dọa dai dẳng cao

Mối đe dọa dai dẳng cao (APT) khai thác các lỗ hổng của hệ thống để ăn cắp thông tin quan trọng để cung cấp đến nguồn. Các tổ chức lớn như các tập đoàn, công ty, hoặc các tổ chức chính phủ, là mục tiêu của phần mềm độc hại này.

Mục tiêu của một mối đe dọa dai dẳng cao liên tục là để không bị phát hiện trong một thời gian dài có thể theo dõi và thu thập thông tin quan trọng mà không làm tổn hại đến máy tính mục tiêu. Các phương thức được sử dụng để lây nhiễm mã độc vào mạng thường thông qua một tập tin PDF hoặc một tài liệu Office được thấy như vô hại mà ai cũng có thể chạy các tập tin.

Ngựa Trojan (một loại virus)

Một chương trình phá hoại giả mạo như một ứng dụng chính thống. Không giống như các chương trình phần mềm độc hại và sâu, Trojan không sao chép bản thân nhưng chúng có thể tàn phá. Một trong những loại nguy hiểm nhất của Trojan là một chương trình được quảng cáo là để gỡ bỏ virus khỏi máy tính nhưng thực ra nó lại cài virus vào máy tính của bạn.

Thuật ngữ này xuất phát từ một câu chuyện trong quyển Iliad của Homer, trong đó người Hy Lạp cho kẻ thù của họ một con ngựa khổng lồ bằng gỗ, Trojans, với bề ngoài như một vật cầu hòa. Nhưng sau khi Trojans kéo ngựa vào thành, lính Hy lạp thoát ra từ trong chiếc bụng rỗng của con ngựa, mở cổng thành từ bên trong cho đồng đội tiến vào thành và lấy lại thành Troy.

Nhận diện nhầm

Nhận diện nhầm xảy ra khi chương trình quét nhận diện một tập tin nào đó là nhiễm virus trong khi tập tin đó là sạch.

Những kẻ săn mồi trực tuyến

Kẻ xấu tìm cách thu hút trẻ vị thành niên hoặc thanh thiếu niên vào các cuộc trò chuyện nhằm mục đích lôi kéo họ vào các hoạt động tình dục bất hợp pháp. Mạng xã hội là nơi lý tưởng khiến trẻ em dễ bị tổn thương có thể dễ dàng bị tìm kiếm và dụ dỗ tham gia các hoạt động tình dục, trực tuyến hoặc trực tiếp.

Ổ đĩa

Là một máy đọc dữ liệu từ đĩa và ghi dữ liệu lên đĩa.

Một ổ đĩa cứng đọc và ghi lên đĩa cứng.

Một ổ đĩa mềm truy cập đĩa mềm.

Ổ đĩa có thể là ổ đĩa trong (nằm cố định trong một máy tính) hay ổ đĩa ngoài (được gắn với một hộp riêng biệt nối với máy tính).

Phần mềm Applet của Java

Java là một chương trình được thiết kế để chạy trên các trang web. Để sử dụng applet trên một trang web, bạn phải chỉ định tên cũng như kích cỡ (độ dài, độ rộng tính bằng điểm ảnh) mà applet có thể thực hiện. Khi một trang web được truy cập, trình duyệt sẽ tải applet về từ máy chủ và chạy applet trên máy tính của người dùng (máy trạm). Applet khác với các ứng dụng khác là ở chỗ chúng được khống chế bởi một giao thức an ninh nghiêm ngặt.

Ví dụ, mặc dù các applet chạy trên máy khách, chúng không thể đọc hoặc ghi dữ liệu lên máy khách. Hơn nữa, applet thường bị hạn chế sao cho chúng chúng chỉ có thể đọc và ghi dữ liệu từ cùng miền web mà chúng được thực hiện từ đó.

Phần mềm gián điệp

Bất kỳ phần mềm nào thu thập thông tin người dùng thông qua kết nối Internet mà người dùng không được biết, thường sử dụng cho mục đích quảng cáo. Các phần mềm gián điệp được đi kèm dưới dạng các yếu tố ẩn đi của một phần mềm miễn phí hoặc chương trình phần mềm chia sẻ mà có thể tải từ internet xuống; tuy nhiên, cần phải lưu ý rằng mục đích chính của các ứng dụng chia sẻ và ứng dụng miễn phí là không đi kèm với phần mềm gián điệp. Khi đã được cài đặt, phần mềm gián điệp theo dõi hành động trên internet của người dùng và gửi thông tin này tới một người nào đó. Phần mềm gián điệp cũng thu thập thông tin về các địa chỉ thư điện tử và thậm chí mật khẩu cũng như số thẻ tín dụng.

Sự tương đồng của phần mềm gián điệp với Trojan ở chỗ là người dùng vô tình cài đặt chúng trong khi họ đang cài đặt một phần mềm khác. Một cách thông thường để trở thành một nạn nhân của phần mềm gián điệp là tải về một tập tin bị đánh tráo là các sản phẩm có ích.

Ngoài những vấn đề về đạo đức và quyền riêng tư, phần mềm gián điệp lấy cắp từ người dùng bằng cách sử dụng tài nguyên bộ nhớ và băng thông kết nối vì nó gửi thông tin cho tin tặc thông qua kết nối Internet của người dùng. Bởi vì phần mềm gián điệp sử dụng bộ nhớ và tài nguyên hệ thống, các ứng dụng chạy ẩn có thể dẫn đến sự cố hoặc mất ổn định hệ thống.

Phần mở rộng của một tập tin

Phần của một tập tin đi sau dấu chấm, biểu thị dạng dữ liệu được lưu trữ trong tập tin.

Nhiều hệ điều hành quy ước phần mở rộng tập tin riêng cho nó, ví như Unix, VMS, và MS-DOS. Chúng thường có từ một đến ba chữ cái (một số hệ điều hành cũ hỗ trợ không quá ba ký tự). Ví dụ "c" dành cho mã nguồn của C, "ps" là PostScript, "txt" là văn bản.

Photon

Photon là công nghệ đột phá của Bitdefender không làm ảnh hưởng người dùng, được thiết kế để tăng tốc làm việc của phần mềm chống mã độc. Bằng cách theo dõi hoạt động máy tính của bạn ở chế độ nền, nó tạo ra mô hình sử dụng giúp tối ưu hóa quá trình khởi động và quét.

Phương pháp không theo kinh nghiệm

Phương pháp quét này không dựa vào cơ sở dữ liệu về mối đe dọa cụ thể. Ưu điểm của việc quét không so sánh mẫu giúp bạn không bị nhầm lẫn bởi những thứ có vẻ như là một mối đe dọa, và không tạo ra báo động giả.

Phương pháp theo kinh nghiệm

Một phương pháp dựa trên nguyên tắc nhận dạng mã độc mới. Phương pháp quét này không dựa vào cơ sở dữ liệu về mối đe dọa cụ thể. Ưu điểm của phương pháp nhận dạng phỏng đoán là nó không bị qua mặt bởi các biến thể mới của một mã độc đã tồn tại. Tuy nhiên, đôi khi nó phát hiện các dòng mã nghi ngờ trong các chương trình bình thường, tạo ra hiện tượng gọi là "nhận diện nhầm".

Quảng cáo rác

Phần mềm quảng cáo thường đi kèm với một ứng dụng máy chủ được cung cấp miễn phí cho tới khi người dùng vẫn còn chấp nhận phần mềm quảng cáo này. Bởi vì các ứng dụng phần mềm quảng cáo rác thường được cài đặt sau khi người dùng đã đồng ý với một thỏa thuận cấp phép nói rõ mục đích của ứng dụng được cam kết.

Tuy nhiên, các quảng cáo bắn ra có thể gây khó chịu, và trong một số trường hợp làm giảm hiệu suất hệ thống. Ngoài ra, thông tin mà các ứng dụng này thu thập có thể là thông tin riêng tư của người dùng khi họ không nhận thức đầy đủ các điều khoản trong thỏa thuận cấp phép.

Ransomware

Ransomware là một chương trình độc hại mà cố gắng kiếm tiền từ người dùng bằng cách khóa các hệ thống dễ bị tổn thương của họ. Cryptolocker, CryptoWall, và TeslaWall, chỉ có một số biến thể mà săn hệ thống cá nhân của người sử dụng.

Các lây nhiệm có thể lây lan bằng cách truy cập thư rác, tải file đính kèm e-mail, hoặc cài đặt các ứng dụng, mà không để cho người dùng biết về những gì đang xảy ra trên hệ thống của mình. Người sử dụng hàng ngày và các công ty đang là mục tiêu của tin tặc ransomware.

Rootkit

Rootkit là một bộ các công cụ phần mềm cho phép truy cập mức quản trị tới một hệ thống. Thuật ngữ này lần đầu tiên được sử dụng trên hệ điều hành UNIX nói về các công cụ biên dịch lại để cung cấp cho kẻ xâm nhập quyền quản trị, cho phép chúng che dấu sự hiện diện trước các quản trị viên hệ thống.

Vai trò chính của rootkit là làm ẩn các quá trình, các tập tin, các sự truy cập cũng như các bản ghi nhật ký. Chúng cũng có thể can thiệp vào dữ liệu từ máy trạm, kết nối mạng hoặc thiết bị ngoại vi, nếu chúng kết hợp với phần mềm thích hợp.

Về bản chất nguyên thủy, Rootkit không độc hại. Ví dụ, các hệ thống và thậm chí một số ứng dụng ẩn các tệp quan trọng bằng cách sử dụng rootkit. Tuy nhiên, phần lớn chúng được sử dụng để dấu các phần mềm phá hoại hoặc dấu sự có mặt của một sự xâm phạm bất hợp pháp vào hệ thống. Khi được kết hợp với phần mềm phá hoại, rootkits sẽ tạo ra sự đe dọa lớn tới tính toàn vẹn và an ninh hệ thống. Chúng có thể điều khiển

kết nối, tạo các cửa hậu trong hệ thống, thay đổi tập tin, nhật trình và ẩn dấu khỏi bị phát hiện.

Sâu
Một chương trình tự lan truyền bản thân nó qua mạng, tự sao chép chính nó khi hoạt động. Nó không ký gửi bản thân vào các chương trình khác.

Sự kiện
Một hành động hay một sự kiện được phát hiện bởi một chương trình. Sự kiện có thể là hành động của người dùng, ví như nhấp chuột hoặc nhấn một phím, hoặc tình trạng hệ thống, chẳng hạn như thiếu bộ nhớ.

Tải về
Để sao chép dữ liệu (thường là cả một tập tin) từ một nguồn chính tới thiết bị ngoại vi. Thuật ngữ này thường được sử dụng để mô tả quá trình sao chép một tập tin từ một dịch vụ trực tuyến vào máy tính của chính mình. Tải về cũng được hiểu là quá trình sao chép một tập tin từ máy chủ hệ thống tới một máy tính trên mạng.

Tấn công Brute Force
Tấn công đoán mật khẩu được sử dụng để đột nhập vào hệ thống máy tính bằng cách nhập các kết hợp mật khẩu có thể, chủ yếu bắt đầu bằng mật khẩu dễ đoán nhất.

Tập lệnh
Một thuật ngữ nữa của tâp tin đa lệnh, script là một danh sách có thể được hoạt động không cần sự tương tác người dùng.

Tập tin báo cáo
Tập tin liệt kê các hành động đã xảy ra. Bitdefender duy trì một tập tin báo cáo các đường dẫn, các thư mục, các tài liệu lưu trữ và các tập tin đã được quét virus, bao nhiêu file bị nhiễm và nghi ngờ đã được tìm thấy.

Tệp lưu trữ:
Archive là đĩa, băng, hoặc thư mục có chứa các tập tin đã được lưu cho mục đích dự phòng.

Một tập tin có chứa một hay nhiều tập tin khác dưới dạng nén.

Thư rác
Thư điện tử rác hoặc nhóm tin rác. Thông thường được biết đến như là các thư điện tử không mong muốn.

Tìm

Viết tắt của trình duyệt web, một ứng dụng phần mềm được sử dụng để định vị và hiển thị các trang web. Các trình duyệt phổ biến bao gồm Microsoft Internet Explorer, Mozilla Firefox và Google Chrome. Đây là những trình duyệt đồ họa, nghĩa là chúng có thể hiển thị đồ họa cũng như văn bản. Thêm vào đó, phần lớn các trình duyệt hiện đại có thể hiển thị các thông tin đa truyền thông, bao gồm âm thanh, hình ảnh, dù chúng có đòi hỏi cài thêm vài công cụ gắn kèm cho một vài định dạng.

Trình ghi lại phím gõ

Keylogger là một ứng dụng ghi lại mọi thứ bạn nhập.

Về cơ bản, Trình ghi lại phím gõ không có tính phá hoại Chúng có thể được sử dụng cho các mục đích hợp pháp, chẳng hạn như giám sát nhân viên hoặc hoạt động của trẻ em. Tuy nhiên, chúng đang ngày càng được sử dụng bởi tội phạm mạng cho mục đích xấu (ví dụ, để thu thập dữ liệu cá nhân, chẳng hạn như thông tin đăng nhập và số an sinh xã hội).

Từ điển tấn công

Các cuộc tấn công đoán mật khẩu được sử dụng để đột nhập vào hệ thống máy tính bằng cách nhập kết hợp các từ phổ biến để tạo mật khẩu tiềm năng. Phương pháp tương tự được sử dụng để đoán các khóa giải mã của tin nhắn hoặc tài liệu được mã hóa. Các cuộc tấn công từ điển thành công vì nhiều người có xu hướng chọn mật khẩu từ ngắn và đơn dễ đoán.

Virus đa sắc

Một loại virus thay đổi hình thái theo từng tập tin chúng nhiễm. Vì chúng không có mẫu nhị phân nhất định nên rất khó nhận dạng.

Virus khởi động

Một loại mã độc lây nhiễm vào vùng khởi động của đĩa cứng cố định hoặc đĩa mềm. Khởi động từ một đĩa bị nhiễm mã độc cũng sẽ khởi động tải virus vào bộ nhớ. Ổi lần bạn khởi động hệ thống từ vùng khởi động đó, bạn sẽ đưa mã độc vào hoạt động của bộ nhớ.