WithSecure Client Security for Windows

Nội dung

Ch□□ng 1

B□t □□u

Chủ đề:

- Tuyên bố từ chối trách nhiệm
- Các yêu cầu về hệ thống
- Thay đổi cài đặt sản phẩm
- Cách xem các tác vụ sản phẩm đã thực hiện

Phần này mô tả cách bạn có thể truy cập vào các tính năng và công cụ của sản phẩm cũng như cách bạn có thể thay đổi cài đặt sản phẩm.

Lưu ý: Quản trị viên của bạn có thể đã thực thi một số cài đặt bảo mật. Điều đó có nghĩa là bạn không thể thay đổi một số tính năng một cách cục bộ.

1.1 Tuyên b t ch i trách nhi m

F-Secure Business hiện là WithSecure ™ được phản ánh dưới dạng logo và tên mới.

Chúng tôi đang trong quá trình đổi thương hiệu sản phẩm của mình và trong thời gian này, bạn có thể thấy sự kết hợp giữa F-Secure và WithSecure ™ trong các sản phẩm và cổng thông tin, cho đến khi tất cả các thay đổi đã được thực hiện.

1.2 Các yêu c u v h th ng

Phần này chứa thông tin về WithSecure Client Security.

Chúng tôi thực sự khuyên bạn nên đọc toàn bộ tài liệu.

H i u hành c h tr

Lưu ý: WithSecure chỉ hỗ trợ những hệ điều hành được hỗ trợ bởi nhà cung cấp của họ. Nếu bạn quan tâm đến hỗ trợ dài hạn cho một nền tảng mà các nhà cung cấp không còn hỗ trợ, hãy liên hệ với đại diện bán hàng của bạn.

WithSecure Client Security hỗ trợ các hệ điều hành sau:

- Microsoft Windows 10 (tất cả các phiên bản 32-bit và 64-bit, bao gồm cả Windows 10 IoT Enterprise)
- Microsoft Windows 11 (tất cả các phiên bản)

Lưu ý: ARM không được hỗ trợ.

Lưu ý: Bạn phải cài đặt Windows Universal C Runtime và Gói Dịch vụ mới nhất cho hệ điều hành của mình trước khi cài đặt sản phẩm.

Lưu ý: Các hệ điều hành phải hỗ trợ chứng chỉ Microsoft Azure Code Signing. Bạn có thể tìm thêm thông tin đây.

Các yêu c u v h th ng

- Dung lượng đĩa: 2 GB dung lượng đĩa trống để cài đặt, cập nhật tự động và hoạt động bình thường. Báo cáo kiểm dịch và quét có thể yêu cầu dung lượng ổ đĩa bổ sung tùy thuộc vào vi-rút được tìm thấy.
- Kết nối Internet: cần có kết nối internet để nhận các bản cập nhật và sử dụng các tính năng công nghệ dựa trên đám mây.

ngôn ng c h tr

Các ngôn ngữ được hỗ trợ là: tiếng Anh, tiếng Trung (PRC, Đài Loan, Hồng Kông), tiếng Séc, tiếng Đan Mạch, tiếng Hà Lan, tiếng Estonia, tiếng Phần Lan, tiếng Pháp, tiếng Pháp Canada, tiếng Đức, tiếng Hy Lạp, tiếng Hungary, tiếng Ý, tiếng Nhật, tiếng Hàn, tiếng Na Uy, tiếng Ba Lan, tiếng Bồ Đào Nha, Tiếng Bồ Đào Nha Brazil, tiếng Rumani, tiếng Nga, tiếng Slovenia, tiếng Tây Ban Nha, tiếng Tây Ban Nha Mỹ Latinh, tiếng Thụy Điển và tiếng Thổ Nhĩ Kỳ.

1.3 Thay i cài t s n ph m

Bạn có thể kiểm soát hành vi của sản phẩm bằng cách thay đổi cài đặt của sản phẩm đó.

Lưu ý rằng bạn cần quyền quản trị để thay đổi cài đặt sản phẩm. Bạn có thể truy cập vào một số cài đặt sản phẩm từ menu ngữ cảnh biểu tượng khay.

Lưu ý: Quản trị viên của bạn có thể đã thực thi một số cài đặt bảo mật. Điều đó có nghĩa là bạn không thể thay đổi một số tính năng một cách cục bộ.

Tác vụ có Liên quan

Chạy quét phần mềm độc hại trên trang14

Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19
DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

Thay đổi thiết đặt Tường lửa của Windows trên trang42
Khi tường lửa được bật, tường lửa giới hạn quyền truy cập vào và ra khỏi máy tính của bạn. Một số ứng dụng có thể yêu cầu bạn cho phép chúng vượt qua tường lửa để hoạt động đúng cách.

Xem các sự kiện gần đây cho sản phẩm trên trang8
Bạn có thể xem các tác vụ sản phẩm đã thực hiện và cách sản phẩm đó đã bảo vệ máy tính của bạn trên trang **Lịch sử sự kiện**.

Tắt tất cả các tính năng bảo mật trên trang6
Bạn có thể tắt tất cả các tính năng bảo mật nếu bạn cần giải phóng thêm các tài nguyên hệ thống.

1.3.1 Quy□n truy c□p nhanh vào thi□t l□p s□n ph□m

Bạn có thể truy cập vào một số cài đặt sản phẩm từ trình đơn ngữ cảnh biểu tượng khay.

Để mở trình đơn ngữ cảnh biểu tượng khay, hãy làm theo các hướng dẫn sau:

Lưu ý: Nếu biểu tượng sản phẩm bị ẩn, hãy nhấp vào mũi tên **Hiển thị biểu tượng bị ẩn** trong thanh tác vụ trước tiên.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trình đơn ngữ cảnh bao gồm các tùy chọn sau:

Tuỳ chọn	Mô tả
Xem trạng thái hiện tại	Hiển thị trạng thái bảo vệ hiện tại của máy tính của bạn.
Kiểm tra cập nhật	Kiểm tra và tải xuống bản cập nhật mới nhất.
Xem các sự kiện gần đây	Xem những hành động mà sản phẩm đã thực hiện để bảo vệ máy tính của bạn.
Mở cài đặt	Mở cài đặt sản phẩm.
Giới thiệu	Hiển thị thông tin phiên bản của sản phẩm.

1.3.2 T□t t□t c□ các tính n□ng b□o m□t

Bạn có thể tắt tất cả các tính năng bảo mật nếu bạn cần giải phóng thêm các tài nguyên hệ thống.

Lưu ý: Quản trị viên của bạn có thể đã đặt chính sách ngăn không cho bạn tắt các tính năng bảo mật.

Lưu ý: Máy tính của bạn không được bảo vệ đầy đủ khi bạn tắt các tính năng bảo mật.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⋯.
3. Chọn **Tắt tất cả các tính năng bảo mật**.

Tính năng sẽ tự động được bật lại vào lần tiếp theo khi bạn khởi động lại máy tính của mình. Bạn cũng có thể bật các tính năng đó một cách thủ công trong chế độ xem chính của sản phẩm.

1.4 Cách xem các tác v s n ph m ã th c hi n

Biểu tượng trạng thái bảo vệ cho biết sản phẩm đang chạy và số liệu thống kê bảo vệ hiển thị thông tin cách sản phẩm đã bảo vệ máy tính của bạn.

1.4.1 Bi u t ng tr ng thái báo v

Biểu tượng trạng thái bảo vệ sẽ cho bạn biết trạng thái tổng thể của sản phẩm và các tính năng của sản phẩm đó.

Biểu tượng trạng thái bảo vệ:

Biểu tượng trạng thái	Tên trạng thái	Mô tả
	OK	Máy tính của bạn đã được bảo vệ. Các tính năng đã được bật và đang hoạt động đúng cách.
	Đã hết hạn	Máy tính của bạn không được bảo vệ. Gói đăng ký của bạn đã hết hạn.
	Đã hết hạn và bị vô hiệu hóa	Máy tính của bạn không được bảo vệ. Gói đăng ký đã hết hạn và sản phẩm đã bị vô hiệu hóa.
	Đã bị vô hiệu hóa; gặp trục trặc	Máy tính của bạn không được bảo vệ đầy đủ hoặc hoàn toàn. Sản phẩm này yêu cầu hành động ngay lập tức, ví dụ: một tính năng quan trọng đã bị tắt hoặc gặp trục trặc hoặc bản cập nhật đã quá cũ.
	Đã bị vô hiệu hóa	Máy tính của bạn không được bảo vệ đầy đủ. Sản phẩm yêu cầu sự chú ý của bạn, ví dụ: một tính năng bảo mật như Duyệt web dựa trên danh tiếng đã bị tắt.
	Đang cập nhật	Đang thiết lập tính năng bảo vệ. Sản phẩm đang cập nhật.

Bi□u t□□ng khay tr□ng thái b□o v□

Các biểu tượng trạng thái bảo vệ sau đây được hiển thị trên khay hệ thống khi sản phẩm yêu cầu bạn chú ý hoặc hành động.

Biểu tượng khay trạng thái	Tên trạng thái	Mô tả
	Chú ý	Máy tính của bạn không được bảo vệ đầy đủ. Sản phẩm cần sự chú ý của bạn, ví dụ: một hoặc nhiều tính năng bảo mật bị tắt hoặc các bản cập nhật quá cũ.
	Cảnh báo	Máy tính của bạn không được bảo vệ. Sản phẩm yêu cầu hành động ngay lập tức, ví dụ: đăng ký đã hết hạn hoặc một tính năng quan trọng bị trục trặc.

1.4.2 Xem các s□ ki□n g□n □ây cho s□n ph□m

Bạn có thể xem các tác vụ sản phẩm đã thực hiện và cách sản phẩm đó đã bảo vệ máy tính của bạn trên trang **Lịch sử sự kiện**.

Lịch sử sự kiện sẽ hiển thị cho bạn các sự kiện khác nhau cho các sản phẩm được cài đặt cũng như chi tiết về các biện pháp bảo vệ mà sản phẩm đã thực hiện. Ví dụ: lịch sử sự kiện sẽ hiển thị cho bạn tất cả các mục độc hại đã được phát hiện và được làm sạch hoặc bị cách ly.

Để xem toàn bộ lịch sử sự kiện của sản phẩm:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ···.
3. Chọn **Sự kiện gần đây**.
   Trang **Lịch sử sự kiện** mở ra.

Lịch sử sự kiện sẽ hiển thị cho bạn thời gian và mô tả của từng sự kiện. Tùy thuộc vào loại sự kiện, bạn có thể bấm vào sự kiện để xem thêm thông tin chi tiết về sự kiện đó. Ví dụ: đối với các tệp độc hại thì bạn có thể xem thông tin sau:

- Ngày và giờ tìm thấy tệp độc hại
- Tên của phần mềm độc hại và vị trí của phần mềm độc hại đó trên máy tính của bạn
- Tác vụ đã thực hiện

Ch□□ng 2

B□o v□ máy tính kh□i n□i dung □□c h□i

Chủ đề:

- Nội dung độc hại là gì
- Cách quét máy tính của tôi
- DeepGuard là gì
- Sử dụng Kiểm soát truy cập DataGuard
- Ngăn ứng dụng tải xuống tệp độc hại
- Sử dụng tích hợp AMSI để xác định các cuộc tấn công dựa trên tập lệnh

Sản phẩm sẽ bảo vệ máy tính của bạn khỏi các chương trình có thể đánh cắp thông tin cá nhân của bạn, làm hỏng máy tính hoặc sử dụng cho mục đích bất hợp pháp.

Theo mặc định, tính năng chống phần mềm độc hại sẽ xử lý tất cả các tệp có hại ngay khi tìm thấy để chúng không thể gây hại.

Sản phẩm sẽ tự động quét ổ đĩa cứng cục bộ, mọi phương tiện di động (như đĩa di động hoặc DVD) và bất kỳ nội dung nào bạn tải xuống.

Sản phẩm cũng giám sát máy tính của bạn để biết mọi thay đổi có thể cho biết bạn có các tệp độc hại trên máy tính. Khi sản phẩm phát hiện thấy bất kỳ thay đổi nào gây nguy hiểm cho hệ thống, chẳng hạn như thay đổi về thiết lập hệ thống hoặc nỗ lực thay đổi các quá trình quan trọng của hệ thống, cấu phần DeepGuard của nó sẽ không cho ứng dụng chạy vì đó có thể là phần mềm độc hại.

Lưu ý: Quản trị viên của bạn có thể thực thi một số cài đặt bảo mật. Điều đó có nghĩa là bạn không thể thay đổi một số tính năng một cách cục bộ.

2.1 N□i dung □□c h□i là gì

Các tệp và ứng dụng độc hại có thể cố gắng phá hủy dữ liệu hoặc giành quyền truy cập trái phép vào hệ thống máy tính để ăn cắp thông tin cá nhân của bạn.

2.1.1 □ng d□ng không mong mu□n ti□m □n (PUA) và □ng d□ng không mong mu□n (UA)

'Ứng dụng không mong muốn tiềm ẩn' có các hành vi hoặc đặc điểm mà bạn có thể coi là không mong đợi hoặc không mong muốn. 'Ứng dụng không mong muốn' có thể ảnh hưởng nghiêm trọng hơn đối với thiết bị hoặc dữ liệu của bạn.

Một ứng dụng có thể bị xác định là 'không mong muốn tiềm ẩn' (PUA) nếu ứng dụng đó có thể:

- **Ảnh hưởng đến quyền riêng tư hoặc năng suất của bạn** - ví dụ: tiết lộ thông tin cá nhân hoặc thực hiện hành động trái phép
- **Đặt áp lực quá mức lên các tài nguyên của thiết bị của bạn** - ví dụ: sử dụng quá nhiều dung lượng hoặc bộ nhớ
- **Xâm phạm bảo mật của thiết bị của bạn hoặc thông tin được lưu trữ trên thiết bị đó** - ví dụ: hiển thị cho bạn nội dung hoặc ứng dụng không mong muốn

Những hành vi và đặc điểm này có thể ảnh hưởng đến thiết bị hoặc dữ liệu của bạn ở mức độ khác nhau. Tuy nhiên, chúng không đủ mức độ độc hại để đảm bảo phân loại ứng dụng là phần mềm độc hại.

Ứng dụng có hành vi hoặc đặc điểm có tác động nghiêm trọng hơn được coi là 'ứng dụng không mong muốn' (UA). Sản phẩm sẽ cẩn trọng hơn khi xử lý những ứng dụng đó.

Sản phẩm sẽ xử lý ứng dụng theo cách khác nhau tùy thuộc vào việc ứng dụng đó là PUA hay UA:

- **Ứng dụng không mong muốn tiềm ẩn** - Sản phẩm sẽ tự động chặn không cho ứng dụng chạy. Nếu bạn chắc chắn rằng bạn tin cậy ứng dụng đó thì bạn có thể chỉ dẫn sản phẩm WithSecure loại trừ ứng dụng đó khỏi quá trình quét. Bạn phải có quyền quản trị để loại trừ tệp bị chặn khỏi quá trình quét.
- **Ứng dụng không mong muốn** - Sản phẩm sẽ tự động chặn không cho ứng dụng chạy.

Tác vụ có Liên quan

Bật tính năng quét trong thời gian thực trên trang14
Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Chạy quét phần mềm độc hại trên trang14
Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19
DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

2.1.2 Sâu

Sâu là chương trình gửi bản sao của chính nó từ thiết bị này sang thiết bị khác qua mạng. Một số sâu cũng thực hiện các hành động độc hại đối với thiết bị bị ảnh hưởng.

Nhiều sâu được thiết kế nhằm thu hút người dùng. Chúng có thể giống như các hình ảnh, video, ứng dụng hoặc bất kỳ loại tệp hoặc chương trình hữu ích nào khác. Mục tiêu của hành động lừa gạt này chính là nhử người dùng cài đặt sâu. Các sâu khác được thiết kế nhằm hoàn toàn ăn cắp do chúng sử dụng các lỗi trên thiết bị (hoặc các chương trình được cài đặt trên thiết bị đó) để tự cài đặt mà người dùng không hề hay biết gì.

Sau khi được cài đặt, sâu sẽ sử dụng các tài nguyên thực để tự tạo các bản sao rồi gửi những bản sao đó đến mọi máy tính khác có thể tiếp cận được qua mạng. Nếu nhiều bản sao đang được gửi đi thì hiệu suất của thiết bị có thể bị ảnh hưởng. Nếu nhiều thiết bị trong mạng bị ảnh hưởng và đang gửi nhiều bản sao của sâu thì chính mạng đó có thể bị gián đoạn. Một số sâu cũng có thể gây ra thiệt hại trực tiếp hơn đối với thiết bị bị ảnh hưởng, chẳng hạn như sửa đổi các tệp được lưu trữ trên thiết bị đó, cài đặt các ứng dụng độc hại khác hoặc ăn cắp dữ liệu.

Hầu hết các sâu chỉ lây lan qua một loại mạng cụ thể. Một số sâu có thể lây lan qua hai hoặc nhiều mạng mặc dù tương đối hiếm gặp. Thường thì sâu sẽ cố gắng và lây lan qua một trong các mạng sau đây (mặc dù đây là những kênh đích ít phổ biến hơn):

- Mạng cục bộ
- Mạng email
- Trang web truyền thông xã hội
- Kết nối ngang hàng (P2P)
- Tin nhắn SMS hoặc MMS

Tác vụ có Liên quan

Bật tính năng quét trong thời gian thực trên trang14
Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Chạy quét phần mềm độc hại trên trang14
Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19
DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

2.1.3 Trojan

Trojan là chương trình cung cấp, hoặc có vẻ cung cấp, một chức năng hoặc tính năng hấp dẫn nhưng sau đó âm thầm thực hiện các tác vụ độc hại trong nền.

Được đặt tên là huyền thoại Ngựa Trojan tại Hy Lạp, các trojan được thiết kế để hấp dẫn người dùng. Chúng có thể giống như các trò chơi, trình bảo vệ màn hình, bản cập nhật ứng dụng hay bất kỳ tệp hoặc chương trình hữu ích nào khác. Một số trojan sẽ bắt chước hoặc thậm chí là sao chép toàn bộ các chương trình phổ biến hoặc nổi tiếng để trông đáng tin cậy hơn. Mục đích của hành vi lừa gạt này chính là đánh lừa người dùng cài đặt trojan.

Sau khi được cài đặt, các trojan cũng có thể sử dụng 'bẫy' để duy trì hoạt động đánh lừa rằng các trojan đó là hợp lệ. Ví dụ: một trojan đã ngụy trang dưới dạng ứng dụng trình bảo vệ màn hình hoặc tệp tài liệu sẽ hiển thị hình ảnh hoặc tài liệu. Trong khi người dùng bị sao lãng bởi những cạm bẫy đó thì trojan có thể âm thầm thực hiện các hành động khác trong nền.

Trojan thường sẽ thực hiện các thay đổi có hại đối với thiết bị (chẳng hạn như xóa hoặc mã hóa các tệp hoặc thay đổi cài đặt chương trình) hoặc ăn cắp thông tin bí mật được lưu trữ trên thiết bị đó. Các trojan có thể được nhóm theo những hành động chúng thực hiện:

- **Trình tải xuống trojan**: kết nối với trang web từ xa để tải xuống và cài đặt các chương trình khác
- **Trình thả trojan**: chứa một hoặc nhiều chương trình khác mà trình thả sẽ cài đặt
- **Trojan-pws**: Ăn cắp mật khẩu được lưu trữ trên thiết bị hoặc được nhập vào trình duyệt web
    - **Trojan ngân hàng**: Trojan-pws chuyên dụng đặc biệt tìm tên người dùng và mật khẩu của các cổng ngân hàng trực tuyến
- **Trojan-gián điệp**: Giám sát hoạt động trên thiết bị và chuyển tiếp thông tin chi tiết đến một trang web từ xa

Tác vụ có Liên quan

Bật tính năng quét trong thời gian thực trên trang14
Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Chạy quét phần mềm độc hại trên trang14
Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19
DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

2.1.4 C□a sau

Cửa sau là tính năng hoặc chương trình được sử dụng để tránh các tính năng bảo mật của chương trình, thiết bị, cổng thông tin hoặc dịch vụ.

Một tính năng trong chương trình, thiết bị, cổng thông tin hoặc dịch vụ có thể là cửa sau nếu thiết kế hoặc quá trình triển khai của tính năng đó mang đến rủi ro về bảo mật. Ví dụ: điểm truy cập của quản trị viên được mã hóa cứng cho cổng thông tin trực tuyến có thể được dùng làm một cửa sau.

Cửa sau thường lợi dụng lỗi trong mã của chương trình, thiết bị, cổng thông tin hoặc dịch vụ. Lỗi có thể là lỗi, lỗ hổng bảo mật hoặc tính năng không được cung cấp.

Cửa sau có thể bị những kẻ tấn công sử dụng để giành quyền truy cập trái phép hoặc để thực hiện các tác vụ độc hại cho phép chúng tránh các tính năng bảo mật như giới hạn quyền truy cập, xác thực hoặc mã hóa.

Tác vụ có Liên quan

Bật tính năng quét trong thời gian thực trên trang14
Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Chạy quét phần mềm độc hại trên trang14
Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19
DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

2.1.5 Ho□t □□ng khai thác

Hoạt động khai thác là đối tượng hoặc phương pháp sử dụng lỗi trong chương trình để làm cho lỗi đó hoạt động không mong muốn. Việc này sẽ tạo điều kiện cho kẻ tấn công có thể sử dụng để thực hiện các tác vụ độc hại.

Khai thác có thể là đối tượng hoặc phương pháp. Ví dụ: chương trình được thiết kế đặc biệt, một đoạn mã hoặc một chuỗi ký tự là các đối tượng; trình tự cụ thể của các lệnh là một phương pháp.

Hoạt động khai thác được sử dụng để lợi dụng lỗi hoặc kẻ hở (còn được gọi là lỗ hổng) trong chương trình. Do mỗi chương trình là khác nhau nên mỗi hoạt động khai thác được gắn kỹ với một chương trình cụ thể.

Có một vài cách để kẻ tấn công sử dụng để gửi công cụ khai thác có thể ảnh hưởng đến máy tính hoặc thiết bị:

- **Nhúng vào chương trình được thiết kế đặc biệt hoặc bị tấn công** - khi bạn cài đặt và khởi chạy chương trình thì hoạt động khai thác sẽ được khởi chạy
- **Nhúng vào tài liệu được đính kèm với email** - khi bạn mở tệp đính kèm thì hoạt động khai thác sẽ được khởi chạy
- **Lưu trữ trên trang web bị tấn công hoặc độc hại** - khi bạn truy cập trang web thì hoạt động khai thác đó sẽ được khởi chạy

Việc tiến hành khai thác có thể khiến các chương trình hoạt động ngoài mong đợi, chẳng hạn như buộc chương trình gặp sự cố hoặc gây xáo trộn bộ nhớ hoặc dung lượng của hệ thống. Việc này có thể tạo điều kiện cho kẻ tấn công thực hiện các tác vụ độc hại khác, chẳng hạn như ăn cắp dữ liệu hoặc giành quyền truy cập vào các phần bị giới hạn của hệ điều hành.

Tác vụ có Liên quan

Bật tính năng quét trong thời gian thực trên trang14
Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Chạy quét phần mềm độc hại trên trang14
Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19

DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

2.1.6 B công c khai thác

Bộ công cụ khai thác là bộ công cụ được những kẻ tấn công sử dụng để quản lý các hoạt động khai thác và phát tán các chương trình độc hại vào máy tính hoặc thiết bị dễ bị tấn công.

Bộ công cụ khai thác chứa một nhiều hoạt động khai thác, từng hoạt động khai thác đó có thể lợi dụng lỗi (lỗ hổng) trong chương trình, máy tính hoặc thiết bị. Thường thì chính bộ công được lưu trữ trên trang web độc hại hoặc bị tấn công, do đó, mọi máy tính hoặc thiết bị truy cập vào trang web đó sẽ bị ảnh hưởng.

Khi máy tính hoặc thiết bị mới kết nối với trang web đặt bẫy, bộ công cụ khai thác sẽ thăm dò mọi lỗi có thể bị ảnh hưởng bởi hành vi khai thác trong kho lưu trữ của bộ công cụ. Nếu tìm thấy một lỗi, bộ công cụ sẽ khởi chạy hành vi khai thác để lợi dụng lỗ hổng đó.

Sau khi máy tính hoặc thiết bị bị xâm phạm, bộ công cụ khai thác có thể đưa phần tải vào máy tính hoặc thiết bị đó. Đây thường là một ứng dụng độc hại khác được cài đặt và khởi chạy trên máy tính hoặc thiết bị. Đến lượt mình, ứng dụng này sẽ thực hiện các hành động trái phép khác.

Bộ công cụ khai thác được thiết kế theo thành phần và dễ sử dụng, do đó, những bộ điều khiển có thể dễ dàng thêm hoặc xoá hoạt động khai thác và phần tải vào bộ công cụ.

Tác vụ có Liên quan

Bật tính năng quét trong thời gian thực trên trang14
Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Chạy quét phần mềm độc hại trên trang14
Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Sử dụng Kiểm soát truy cập DataGuard trên trang19
DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

2.2 Cách quét máy tính c a tôi

Khi ***Bảo vệ chống phần mềm độc hại*** được bật, tính năng này sẽ tự động quét các tệp độc hại cho máy tính của bạn.

Chúng tôi khuyên bạn luôn luôn nên bật tính năng ***Bảo vệ chống phần mềm độc hại***. Bạn cũng có thể quét tệp theo cách thủ công và thiết lập quá trình quét theo lịch nếu bạn muốn đảm bảo rằng không có tệp độc hại nào trên máy tính của mình hoặc để quét tệp mà bạn đã loại bỏ khỏi quá trình quét trong thời gian thực. Thiết lập quá trình quét theo lịch nếu bạn muốn định kỳ quét máy tính của mình hàng tuần hoặc hàng tháng.

2.2.1 Cách th c ho t ng c a tính n ng quét theo th i gian th c

Quét trong thời gian thực bảo vệ máy tính của bạn bằng cách quét tất cả các tệp khi chúng được truy cập và bằng cách chặn truy cập vào những tệp chứa ***phần mềm độc hại***.

Khi máy tính của bạn cố truy cập vào một tệp, Quét trong thời gian thực quét phần mềm độc hại cho tệp trước khi cho phép máy tính của bạn truy cập vào tệp đó.

Nếu Quét trong thời gian thực tìm thấy bất kỳ nội dung độc hại nào, Quét trong thời gian thực sẽ cách ly tệp trước khi tệp có thể gây ra gây hại.

Quét trong th i gian th c có nh h ng n hi u su t c a máy tính c a tôi không?

Thông thường, bạn không biết quá trình quét vì nó chỉ mất một ít thời gian và tài nguyên hệ thống. Ví dụ: lượng thời gian và tài nguyên hệ thống mà quá trình quét trong thời gian thực cần tuỳ thuộc vào nội dung, vị trí và loại tệp.

Các tệp trên các ổ đĩa di động như CD, DVD và ổ đĩa USB di động mất nhiều thời gian hơn để quét.

Lưu ý: Các tệp được nén, chẳng hạn như tệp ***.zip***, không được quét bởi tính năng quét trong thời gian thực.

Quét trong thời gian thực có thể làm chậm máy tính của bạn nếu:

- bạn có máy tính không đáp ứng các yêu cầu hệ thống hoặc
- bạn truy cập vào nhiều tệp cùng một lúc. Ví dụ: khi bạn mở thư mục chứa nhiều tệp cần được quét.

B□t tính n□ng quét trong th□i gian th□c

Bật tính năng quét trong thời gian thực để xóa các tệp độc hại khỏi máy tính trước khi các tệp đó có thể gây hại cho máy tính.

Để đảm bảo rằng tính năng quét trong thời gian thực đã được bật:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Bảo vệ Chống phần mềm độc hại** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

4. Bật **Quét trong Thời gian thực**.

2.2.2 Quét t□p m□t cách th□ công

Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Quá trình quét toàn bộ máy tính sẽ quét vi-rút, phần mềm gián điệp và ứng dụng không mong muốn tiềm ẩn cho tất cả các ổ cứng trong và ngoài. Quá trình quét này cũng sẽ kiểm tra các mục có thể bị rootkit làm ẩn. Quá trình quét toàn bộ máy tính có thể mất nhiều thời gian để hoàn tất. Bạn cũng có thể chỉ quét các phần của hệ thống nơi thường tìm thấy các ứng dụng độc hại để xóa các ứng dụng không mong muốn cũng như mục độc hại trên máy tính của mình hiệu quả hơn.

Quét t□p và th□ m□c c□a b□n

Nếu bạn nghi ngờ các tệp nhất định trên máy tính của mình, bạn có thể chỉ quét những tệp hoặc thư mục đó. Quá trình quét này sẽ hoàn thành nhanh hơn nhiều so với quá trình quét toàn bộ máy tính của bạn. Ví dụ: khi bạn kết nối ổ cứng ngoài hoặc ổ USB flash với máy tính của mình, bạn có thể quét các ổ đó để đảm bảo rằng chúng không chứa bất kỳ tệp độc hại nào.

Ch□y quét ph□n m□m □□c h□i

Bạn có thể quét toàn bộ máy tính của mình để hoàn toàn đảm bảo rằng máy tính đó không có tệp độc hại hoặc ứng dụng không mong muốn nào.

Để quét máy tính của bạn, hãy làm theo các hướng dẫn sau:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Nếu bạn muốn tối ưu hoá cách tính năng quét thủ công sẽ quét máy tính của bạn, hãy chọn ⚙ rồi chọn **Cài đặt Quét**.
   a) Chọn **Chỉ quét các loại tệp thường chứa mã độc hại (nhanh hơn)** nếu bạn không muốn quét tất cả các tệp.

      Các tệp có đuôi mở rộng sau là các ví dụ về các loại tệp được quét khi bạn chọn tùy chọn này: `com`, `doc`, `dot`, `exe`, `htm`, `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.

   b) Chọn **Quét trong các tệp nén** để quét các tệp bên trong các tệp lưu trữ được nén, ví dụ: tệp zip. Việc quét bên trong các tệp được nén sẽ làm cho quá trình quét chậm hơn. Bỏ chọn tùy chọn này để quét tệp lưu trữ chứ không quét các tệp bên trong tệp lưu trữ đó.
3. Trên trang chính, chọn 🔍.
4. Chọn **Quét phần mềm độc hại** hoặc **Quét toàn bộ máy tính**.

- **Quét phần mềm độc hại** bắt đầu bằng cách quét bộ nhớ đang hoạt động của máy tính rồi đến các vị trí thường phát hiện thấy phần mềm độc hại, bao gồm các thư mục tài liệu. Quá trình quét này có thể tìm và xóa những ứng dụng không mong muốn cũng như các mục độc hại trên máy tính trong thời gian ngắn hơn.
- **Quét toàn bộ máy tính** sẽ quét vi-rút, phần mềm gián điệp và các ứng dụng không mong muốn tiềm ẩn cho tất cả các ổ đĩa cứng trong và ngoài. Quá trình ngày cũng kiểm tra các mục có thể bị rootkit làm ẩn. Quét toàn bộ máy tính có thể mất nhiều thời gian để hoàn thành.

Quá trình quét vi-rút sẽ bắt đầu.

5. Nếu quá trình quét vi-rút tìm thấy bất kỳ mục độc hại nào, quá trình quét đó sẽ hiển thị cho bạn danh sách các mục độc hại được phát hiện.
6. Nhấp vào mục được phát hiện để chọn cách bạn muốn xử lý nội dung độc hại.

Tuỳ chọn	Mô tả
Làm sạch	Tự động làm sạch các tệp. Không thể làm sạch các tệp bị cách ly.
Cách ly	Lưu trữ các tệp ở nơi an toàn nơi chúng không thể phát tán hoặc gây hại cho máy tính của bạn.
Xoá	Xoá vĩnh viễn các tệp khỏi máy tính của bạn.
Bỏ qua	Không cần làm gì vào lúc này và để nguyên các tệp trên máy tính của bạn.
Loại trừ	Cho phép ứng dụng chạy và loại trừ tệp đó khỏi quá trình quét trong tương lai.

Lưu ý: Một số tuỳ chọn không khả dụng với tất cả các loại mục độc hại.

7. Chọn **Xử lý tất cả** để bắt đầu quá trình làm sạch.
8. Quá trình quét phần mềm độc hại sẽ hiển thị kết quả cuối cùng cùng số lượng các tệp độc hại đã được làm sạch.

Lưu ý: Quá trình quét phần mềm độc hại có thể yêu cầu bạn khởi động lại máy tính của bạn để hoàn tất quá trình làm sạch. Nếu quá trình làm sạch yêu cầu khởi động lại máy tính, hãy nhấp vào **Khởi động lại** để hoàn tất quá trình làm sạch các mục độc hại và khởi động lại máy tính của bạn.

Bạn có thể xem kết quả cuối cùng của lần quét vi-rút mới nhất bằng cách chọn **Mở báo cáo quét cuối cùng**.

Quét trong Windows Explorer

Bạn có thể quét các tệp độc hại và ứng dụng không mong muốn cho các ổ đĩa, thư mục và tệp trong Windows Explorer.

Nếu bạn nghi ngờ về một số tệp nhất định trên máy tính của mình, bạn chỉ có thể quét các tệp hoặc thư mục đó. Những lần quét này sẽ kết thúc nhanh hơn rất nhiều so với lần quét toàn bộ máy tính của bạn. Ví dụ: khi bạn kết nối ổ cứng ngoài hoặc ổ flash USB với máy tính, bạn có thể quét những ổ đó để đảm bảo rằng chúng không chứa bất kỳ tệp độc hại nào.

Để quét ổ đĩa, thư mục hoặc tệp:

1. Nhấp chuột phải vào ổ đĩa, thư mục hoặc tệp bạn muốn quét.
2. Từ menu chuột phải, chọn **Duyệt vi rút**.

Lưu ý: Trên Windows 11, chọn **Hiển thị thêm các tùy chọn** và sau đó chọn **Quét phần mềm độc hại**.

Quá trình quét vi-rút sẽ bắt đầu và quét ổ đĩa, thư mục hoặc tệp bạn đã chọn.

Quá trình quét vi-rút sẽ hướng dẫn bạn qua các giai đoạn làm sạch nếu quá trình quét đó tìm thấy các tệp độc hại hoặc ứng dụng không mong muốn trong quá trình quét.

2.2.3 Lên l□ch quét

Đặt máy tính của bạn tự động quét và xoá phần mềm độc hại và các ứng dụng độc hại khác khi bạn sử dụng máy tính hoặc đặt quá trình quét chạy định kỳ để đảm bảo máy tính của bạn sạch.

Để đặt lịch quét:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Cài đặt Quét**.
4. Bật **Quét theo lịch**.
5. Trong **Tiến hành quét**, hãy chọn tần suất bạn muốn quét máy tính của mình một cách tự động.

Tuỳ chọn	Mô tả
Hàng ngày	Quét máy tính của bạn hàng ngày.
Hàng tuần	Quét máy tính của bạn vào những ngày được chọn trong tuần. Chọn ngày trong tuần từ danh sách.
Bốn tuần một lần	Quét máy tính của bạn vào ngày trong tuần được chọn trong khoảng thời gian bốn tuần. Chọn ngày trong tuần từ danh sách. Quá trình quét sẽ bắt đầu vào lần tiếp theo của ngày trong tuần được chọn.

6. Trong **Thời gian bắt đầu**, hãy chọn thời điểm bắt đầu lần quét theo lịch.
7. Chọn **Chạy quá trình quét ở mức ưu tiên thấp** để đảm bảo làm cho quét theo lịch ít can thiệp vào các hoạt động khác trên máy tính. Việc chạy quá trình quét ở mức ưu tiên thấp sẽ mất nhiều thời gian hơn để hoàn thành.
8. Chọn **Chỉ quét các loại tệp thường chứa mã độc hại (nhanh hơn)** nếu bạn không muốn quét tất cả các tệp.

   Các tệp có đuôi mở rộng sau là các ví dụ về các loại tệp được quét khi bạn chọn tùy chọn này: `com`, `doc`, `dot`, `exe`, `htm`, `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.
9. Chọn **Quét trong các tệp nén** để quét các tệp bên trong các tệp lưu trữ được nén, ví dụ: tệp zip. Việc quét bên trong các tệp được nén sẽ làm cho quá trình quét chậm hơn. Bỏ chọn tùy chọn này để quét tệp lưu trữ chứ không quét các tệp bên trong tệp lưu trữ đó.

👉 **Lưu ý:** Quét theo lịch bị hủy khi chế độ chơi trò chơi được bật. Khi bạn tắt ***chế độ thuyết trình***, quá trình quét sẽ chạy lại theo lịch.

2.3 DeepGuard là gì

DeepGuard cung cấp khả năng bảo vệ chủ động, tức thời trước các mối đe dọa không xác định.

DeepGuard giám sát các ứng dụng để phát hiện và dừng các thay đổi độc hại tiềm ẩn đối với hệ thống trong thời gian thực. DeepGuard đảm bảo rằng bạn chỉ sử dụng ứng dụng an toàn. Mức độ an toàn của ứng dụng được xác minh từ dịch vụ đám mây được tin cậy.Nếu mức độ an toàn không được xác minh, DeepGuard bắt đầu giám sát hành vi của ứng dụng.

👉 **Mẹo:** Nếu bạn muốn WithSecure thêm ứng dụng của mình vào danh sách ứng dụng được phép, hãy gửi đơn đăng ký của bạn để phân tích tại đây. Sau khi chúng tôi đã phân tích chương trình, chúng tôi sẽ thông báo cho bạn về kết quả phân tích nếu bạn đã cung cấp cho chúng tôi chi tiết liên hệ của bạn.

DeepGuard chặn ***Trojan***, ***sâu***, ***hoạt động lợi dụng*** và chưa được phát hiện cũng như những ứng dụng độc hại khác cố thực hiện thay đổi đối với máy tính của bạn và ngăn các ứng dụng đáng ngờ truy cập vào internet.

Các thay đổi hệ thống có thể có hại mà DeepGuard phát hiện bao gồm:

- thay đổi cài đặt hệ thống (registry của Windows),
- cố gắng tắt các chương trình hệ thống quan trọng, ví dụ: các chương trình bảo mật như sản phẩm này và
- tìm cách chỉnh sửa các tệp hệ thống quan trọng.

Để đảm bảo rằng DeepGuard đang hoạt động:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Bảo vệ Chống phần mềm độc hại** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

   
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

   
5. Bật **DeepGuard**.

Khi DeepGuard được bật, DeepGuard sẽ tự động chặn các ứng dụng cố thực hiện thay đổi độc hại tiềm ẩn đối với hệ thống.

Lưu ý: Tất cả các quy tắc của DeepGuard đều hiển thị cho tất cả người dùng. Các quy tắc có thể bao gồm tên tệp và tên thư mục với thông tin cá nhân. Do đó, hãy lưu ý rằng những người dùng khác trên cùng một máy tính có thể thấy các đường dẫn và tên tệp được bao gồm trong các quy tắc của DeepGuard.

Tác vụ có Liên quan

Dữ liệu Bảo mật trên trang48
Dịch vụ gửi các truy vấn về các hoạt động độc hại tiềm ẩn hoặc trên các thiết bị được bảo vệ tới WithSecure ***Đám mây bảo mật*** .

2.3.1 Cho phép các □ng d□ng mà DeepGuard □ã ch□n

Bạn có thể kiểm soát những ứng dụng mà DeepGuard cho phép và chặn.

Đôi khi DeepGuard có thể chặn không cho ứng dụng an toàn chạy, ngay cả khi bạn muốn sử dụng ứng dụng và biết rằng ứng dụng đó an toàn. Việc này xảy ra do ứng dụng cố thực hiện thay đổi hệ thống có thể có hại. Bạn cũng có thể vô tình chặn một ứng dụng khi cửa sổ bật lên của DeepGuard được hiển thị.

Để cho phép ứng dụng mà DeepGuard đã chặn:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⋯.
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Đã chặn**.
   Tác vụ này sẽ hiển thị cho bạn danh sách các ứng dụng mà DeepGuard đã chặn.
5. Tìm ứng dụng bạn muốn cho phép và chọn **Cho phép**.
6. Chọn **Đúng** để xác nhận rằng bạn muốn cho phép ứng dụng.

Ứng dụng được chọn đã được thêm vào danh sách **Đã loại trừ** và DeepGuard cho phép ứng dụng thực hiện lại các thay đổi đối với hệ thống.

2.3.2 S□ d□ng DataGuard

DataGuard sẽ giám sát một nhóm các thư mục mà phần mềm tống tiền hoặc phần mềm độc hại tương tự khác đã thực hiện các thay đổi có thể gây hại.

Phần mềm tống tiền là phần mềm độc hại sẽ mã hóa các tệp quan trọng trên máy tính của bạn, ngăn bạn truy cập vào các tệp đó. Những tên tội phạm sẽ yêu cầu một khoản tiền chuộc để khôi phục các tệp của bạn. Tuy nhiên, không có gì đảm bảo bạn sẽ nhận lại được dữ liệu cá nhân của mình ngay cả khi bạn chọn trả tiền.

DataGuard chỉ cho phép các ứng dụng an toàn truy cập vào các thư mục được bảo vệ. Sản phẩm sẽ thông báo cho bạn nếu có bất kỳ ứng dụng không an toàn nào cố truy cập vào thư mục được bảo vệ. Nếu bạn biết và tin cậy ứng dụng thì bạn có thể cho phép ứng dụng đó truy cập vào thư mục. DataGuard cũng cho phép DeepGuard sử dụng danh sách các thư mục được bảo vệ cho lớp bảo vệ bổ sung.

Bạn có thể chọn các thư mục yêu cầu lớp bảo vệ bổ sung chống lại phần mềm phá hoại, chẳng hạn như phần mềm tống tiền.

Lưu ý: Bạn phải bật DeepGuard để sử dụng DataGuard. DataGuard chỉ có sẵn trong phiên bản Cao cấp.

Để quản lý các thư mục được bảo vệ của bạn:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn .
3. Chọn **Bảo vệ Chống phần mềm độc hại** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.
4. Bật **DataGuard**.
5. Chọn **Xem thư mục được bảo vệ**.
6. Chọn tab **Được bảo vệ**.
   Tác vụ này sẽ hiển thị cho bạn danh sách tất cả các thư mục hiện được bảo vệ.
7. Thêm hoặc xóa các thư mục khi cần.
   Để thêm thư mục được bảo vệ mới:
   a) Nhấp vào **Thêm mới**.
   b) Chọn thư mục bạn muốn bảo vệ.
   c) Nhấp vào **Chọn thư mục**.
   Để xóa thư mục:
   a) Chọn thư mục trong danh sách.
   b) Nhấp vào **Xoá**.

Mẹo: Nhấp vào **Khôi phục mặc định** nếu bạn muốn hoàn tác mọi thay đổi mình đã thực hiện đối với danh sách các thư mục được bảo vệ kể từ khi cài đặt sản phẩm.

Tác vụ có Liên quan

Thêm và xóa các thư mục được bảo vệ trên trang18
Bạn có thể chọn các thư mục yêu cầu lớp bảo vệ bổ sung chống lại phần mềm phá hoại, chẳng hạn như phần mềm tống tiền.

2.3.3 Thêm và xóa các th□ m□c □□□c b□o v□

Bạn có thể chọn các thư mục yêu cầu lớp bảo vệ bổ sung chống lại phần mềm phá hoại, chẳng hạn như phần mềm tống tiền.

DataGuard sẽ chặn bất kỳ quyền truy cập không an toàn nào vào các thư mục được bảo vệ của bạn.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn .
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Được bảo vệ**.
   Tác vụ này sẽ hiển thị cho bạn danh sách tất cả các thư mục hiện được bảo vệ.
5. Thêm hoặc xóa các thư mục khi cần.
   Để thêm thư mục được bảo vệ mới:
   a) Nhấp vào **Thêm mới**.

b) Chọn thư mục bạn muốn bảo vệ.
c) Nhấp vào **Chọn thư mục**.

Mẹo: Do bạn phải cho phép một cách riêng rẽ tất cả các ứng dụng cần truy cập vào thư mục được bảo vệ, chúng tôi khuyên bạn không nên thêm các thư mục chứa các ứng dụng hoặc trò chơi đã cài đặt của bạn (Ví dụ: Thư mục Thư viện Steam). Nếu không, những ứng dụng này có thể không hoạt động đúng cách.

Để xóa thư mục:

a) Chọn thư mục trong danh sách.
b) Nhấp vào **Xoá**.

Mẹo: Nhấp vào **Khôi phục mặc định** nếu bạn muốn hoàn tác mọi thay đổi mình đã thực hiện đối với danh sách các thư mục được bảo vệ kể từ khi cài đặt sản phẩm.

2.4 S□ d□ng Ki□m soát truy c□p DataGuard

DataGuard Access Control bảo vệ các thư mục khỏi ransomware (mã hóa tống tiền) bằng cách ngăn ứng dụng không xác định truy cập chúng.

Lưu ý: DataGuard chỉ có sẵn trong phiên bản Premium.

Bật **Kiểm soát truy cập DataGuard**:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn .
3. Chọn **Bảo vệ Chống phần mềm độc hại** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.
4. Bật **Kiểm soát truy cập DataGuard**.

2.4.1 Xem các m□c □□□c cách ly

Bạn có thể xem thêm thông tin về các mục được đặt trong khu vực cách ly.

Khu vực cách ly là hệ thống lưu trữ an toàn cho các tệp có thể gây hại. Sản phẩm có thể đặt cả mục độc hại và ứng dụng không mong muốn tiềm ẩn trong khu vực cách ly nhằm biến chúng thành vô hại. Bạn có thể khôi phục các ứng dụng hoặc tệp từ khu vực cách ly sau này nếu cần. Nếu bạn không cần mục bị cách ly, bạn có thể xóa mục đó. Việc xoá một mục trong khu vực cách ly sẽ xoá vĩnh viễn mục đó khỏi máy tính của bạn.

Để xem thông tin về các mục được đặt trong khu vực cách ly:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn .
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Đã cách ly**.
   Danh sách này sẽ hiển thị cho bạn tên, ngày phát hiện và loại lây nhiễm cho từng mục bị cách ly.
5. Nhấp hai lần vào mục bị cách ly để xem thêm thông tin.
   Đối với các mục đơn lẻ, tác vụ này sẽ hiển thị cho bạn vị trí ban đầu của mục bị cách ly.

2.4.2 Khôi ph□c m□c □ã cách ly

Bạn có thể khôi phục các mục đã cách ly mà bạn cần.

Bạn có thể khôi phục ứng dụng hoặc tệp từ khu vực cách ly nếu bạn cần chúng. Đừng khôi phục bất kỳ mục nào từ khu vực cách ly trừ khi bạn chắc chắn rằng chúng không mang lại nguy hiểm. Các mục được khôi phục chuyển trở lại vị trí ban đầu trên máy tính của bạn.

Để khôi phục các mục đã cách ly:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⋯.
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Đã cách ly**.
5. Chọn mục đã cách ly mà bạn muốn khôi phục.
6. Nhấp vào **Cho phép**.
7. Nhấp vào **Có** để xác nhận rằng bạn muốn khôi phục mục bị cách ly.

Mục được chọn sẽ tự động được khôi phục về vị trí ban đầu của mục đó. Tùy thuộc vào loại lây nhiễm, mục có thể bị loại trừ khỏi quá trình quét trong tương lai.

Lưu ý: Để xem tất cả các tệp và ứng dụng hiện đã bị loại trừ, hãy chọn tab **Đã loại trừ** trong chế độ xem **Điều khiển ứng dụng và tệp**.

2.4.3 Loại trừ các tệp hoặc thư mục khỏi quá trình quét

Khi bạn loại trừ các tệp hoặc thư mục khỏi quá trình quét, chúng sẽ không được quét nội dung độc hại.

Để loại trừ các tệp hoặc thư mục khỏi quá trình quét:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⋯.
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Đã loại trừ**.
   Chế độ xem này sẽ hiển thị cho bạn danh sách các tệp và thư mục bị loại trừ.
5. Chọn **Thêm mới**.
6. Chọn tệp hoặc thư mục bạn muốn loại trừ khỏi quá trình quét.
7. Chọn **OK**.

Các tệp hoặc thư mục được loại trừ khỏi quá trình quét trong tương lai.

2.4.4 Xem các ứng dụng được loại trừ

Bạn có thể xem các ứng dụng mà bạn đã loại trừ khỏi quá trình quét và xoá chúng khỏi danh sách mục được loại trừ nếu bạn muốn quét chúng trong tương lai.

Nếu sản phẩm phát hiện thấy ứng dụng không mong muốn tiềm ẩn mà bạn biết là an toàn hoặc là phần mềm gián điệp mà bạn cần giữ trên máy tính để sử dụng ứng dụng nào đó khác, bạn có thể loại trừ ứng dụng đó khỏi quá trình quét để sản phẩm không cảnh báo cho bạn về ứng dụng đó nữa.

Lưu ý: Không thể loại trừ ứng dụng nếu ứng dụng đó có hành vi giống như vi-rút hoặc ứng dụng độc hại khác.

Ngoài ra, DeepGuard không chặn các trò chơi Steam nhất định. Do đó, bạn không phải loại trừ các trò chơi Steam quét hoặc tắt DeepGuard để chạy chúng.

Để xem các ứng dụng được loại trừ khỏi quá trình quét:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.

2. Trên trang chính, chọn ⋯.
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Đã loại trừ**.
   Chế độ xem này sẽ hiển thị cho bạn danh sách các tệp và thư mục bị loại trừ.
5. Nếu bạn muốn quét lại ứng dụng được loại trừ:
   a) Chọn ứng dụng bạn muốn đưa vào quá trình quét.
   b) Nhấp vào **Xoá**.

Các ứng dụng mới chỉ xuất hiện trên danh sách loại trừ sau khi bạn loại trừ chúng khỏi quá trình quét và không thể được thêm vào danh sách loại trừ trực tiếp.

2.4.5 Thêm và xóa các th□ m□c □□□c b□o v□

Bạn có thể chọn các thư mục yêu cầu lớp bảo vệ bổ sung chống lại phần mềm phá hoại, chẳng hạn như phần mềm tống tiền.

DataGuard sẽ chặn bất kỳ quyền truy cập không an toàn nào vào các thư mục được bảo vệ của bạn.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⋯.
3. Chọn **Cách ly và loại trừ**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   Chế độ xem **Kiểm soát ứng dụng và tệp** sẽ mở ra.
4. Chọn tab **Được bảo vệ**.
   Tác vụ này sẽ hiển thị cho bạn danh sách tất cả các thư mục hiện được bảo vệ.
5. Thêm hoặc xóa các thư mục khi cần.
   Để thêm thư mục được bảo vệ mới:
   a) Nhấp vào **Thêm mới**.
   b) Chọn thư mục bạn muốn bảo vệ.
   c) Nhấp vào **Chọn thư mục**.

   Mẹo: Do bạn phải cho phép một cách riêng rẽ tất cả các ứng dụng cần truy cập vào thư mục được bảo vệ, chúng tôi khuyên bạn không nên thêm các thư mục chứa các ứng dụng hoặc trò chơi đã cài đặt của bạn (Ví dụ: Thư mục Thư viện Steam). Nếu không, những ứng dụng này có thể không hoạt động đúng cách.

   Để xóa thư mục:
   a) Chọn thư mục trong danh sách.
   b) Nhấp vào **Xoá**.

Mẹo: Nhấp vào **Khôi phục mặc định** nếu bạn muốn hoàn tác mọi thay đổi mình đã thực hiện đối với danh sách các thư mục được bảo vệ kể từ khi cài đặt sản phẩm.

2.5 Ng□n □ng d□ng t□i xu□ng t□p □□c h□i

Bạn có thể ngăn ứng dụng trên máy tính của mình tải xuống tệp độc hại từ Internet.

Một số trang web chứa công cụ khai thác và tệp độc hại khác có thể gây hại cho máy tính của bạn. Với bảo vệ mạng nâng cao, bạn có thể ngăn mọi ứng dụng tải xuống các tệp độc hại trước khi chúng đến máy tính của bạn.

Để chặn bất kỳ ứng dụng nào tải xuống tệp độc hại:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.

2. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

3. Trên trang chính, chọn ⚙.
4. Chọn **Bảo vệ Chống phần mềm độc hại** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

5. Bật **Bảo vệ Mạng Nâng cao**.

   Lưu ý: Cài đặt này có hiệu lực ngay cả khi bạn tắt tường lửa.

2.6 S□ d□ng tích h□p AMSI □□ xác □□nh các cu□c t□n công d□a trên t□p l□nh

Giao diện Quét Chống phần mềm độc hại (AMSI) là một cấu phần của Microsoft Windows cho phép điều tra sâu rộng hơn đối với các dịch vụ tạo tập lệnh được tích hợp.

Lưu ý: Tích hợp AMSI chỉ có sẵn trên Windows 10.

Phần mềm độc hại nâng cao sử dụng các tập lệnh được che giấu hoặc mã hóa nhằm tránh các phương thức quét khác. Những phần mềm độc hại đó thường được tải trực tiếp vào bộ nhớ do đó phần mềm độc hại đó không sử dụng bất kỳ tệp nào trên thiết bị.

AMSI là giao diện mà các ứng dụng và dịch vụ đang chạy trên Windows có thể sử dụng để gửi các yêu cầu quét đến sản phẩm chống phần mềm độc hại được cài đặt trên máy tính. Giao diện đó cung cấp biện pháp bảo vệ bổ sung chống lại phần mềm độc hại sử dụng các tập lệnh hoặc macro trên các cấu phần chính của Windows, chẳng hạn như PowerShell và Office365 hoặc các ứng dụng khác để lẩn tránh việc bị phát hiện.

Để bật tích hợp AMSI trong sản phẩm:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Bảo vệ Chống phần mềm độc hại** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

4. Bật **Giao diện Quét Chống phần mềm độc hại (AMSI)**.
   Giờ đây, sản phẩm sẽ thông báo cho bạn về bất kỳ nội dung độc hại nào mà AMSI phát hiện và ghi nhật ký những phát hiện đó trong lịch sử sự kiện.

Ch□□ng
3

B□o v□ duy□t web c□a b□n

Chủ đề:

- Đang chặn các trang web độc hại
- Triển khai tiện ích mở rộng bảo vệ duyệt qua GPO
- Đang kiểm tra xem các tiện ích mở rộng trình duyệt có đang được sử dụng không

Tính năng bảo vệ duyệt giúp bạn duyệt Internet một cách an toàn bằng cách cung cấp xếp hạng an toàn cho trang web trên trình duyệt của bạn cũng như chặn quyền truy cập vào trang web bị xếp hạng độc hại.

3.1 □ang ch□n các trang web □□c h□i

Tính năng Bảo vệ Duyệt web sẽ chặn quyền truy cập vào các trang web độc hại khi được bật.

Để đảm bảo rằng Bảo vệ Duyệt web đã được bật:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Duyệt An toàn**.
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.
5. Bật **Bảo vệ Duyệt web**.
6. Nếu trình duyệt của bạn mở ra, hãy khởi động lại trình duyệt để áp dụng thiết lập đã thay đổi.

Lưu ý: Bảo vệ Duyệt web yêu cầu tiện ích mở rộng Bảo vệ Duyệt web đã được bật trong trình duyệt web bạn sử dụng.

3.1.1 Ch□n trang web □áng ng□ và b□ nghiêm c□m

Bảo vệ Duyệt web có thể ngăn bạn vô tình truy cập vào những trang web không đáng tin cậy hoặc chứa nội dung bị nghiêm cấm.

Đôi khi, bạn có thể duyệt đến một trang web chứa nội dung đáng ngờ, vi phạm hoặc bị nghiêm cấm. Ví dụ: trang web có thể là trang web spam, giả được xác định, chứa chương trình không mong muốn hoặc bất hợp pháp cho dù bạn ở bất cứ đâu.

Bạn có thể sử dụng tính năng Bảo vệ Duyệt web để tránh vô tình truy cập vào những trang web này.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Duyệt An toàn**.
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.
5. Đảm bảo rằng **Bảo vệ Duyệt web** đã được bật.
6. Nếu bạn muốn chặn trang web được đánh giá là đáng ngờ bên cạnh trang web được xem là độc hại, hãy chọn **Chặn trang web đáng ngờ**.
7. Nếu bạn muốn chặn trang web chứa nội dung bị nghiêm cấm, hãy chọn **Chặn trang web bị nghiêm cấm**.
8. Nếu trình duyệt của bạn mở ra, hãy khởi động lại trình duyệt để áp dụng thiết lập đã thay đổi.

Lưu ý: Bảo vệ Duyệt web yêu cầu tiện ích mở rộng Bảo vệ Duyệt web đã được bật trong trình duyệt web bạn sử dụng.

3.1.2 S□ d□ng bi□u t□□ng x□p h□ng danh ti□ng

Bảo vệ Duyệt web sẽ hiển thị xếp hạng an toàn trang web trên trang kết quả tìm kiếm khi bạn sử dụng Google, Bing, Yahoo hoặc DuckDuckGo.

Các biểu tượng được mã hoá màu hiển thị xếp hạng an toàn của trang web hiện tại. Xếp hạng an toàn của mỗi liên kết trên kết quả công cụ tìm kiếm sẽ xuất hiện với những biểu tượng giống nhau sau:

✓	Theo chúng tôi biết thì trang web này là an toàn. Chúng tôi không tìm thấy bất kỳ điều gì khả nghi trong trang web.

	Trang web khả nghi và chúng tôi khuyên bạn nên cẩn thận khi truy cập trang web này. Tránh tải xuống bất kỳ tệp nào hoặc cung cấp bất kỳ thông tin cá nhân nào.
	Trang web có hại. Chúng tôi khuyên bạn nên tránh truy cập trang web này. Ngoài ra, một quản trị viên đã chặn trang web này và bạn không thể truy cập trang web đó.
	Chúng tôi chưa phân tích trang web hoặc hiện không có thông tin cho trang web này.
	Quyền truy cập vào trang web này không bao giờ bị chặn.

Để xem các biểu tượng xếp hạng danh tiếng trong các kết quả tìm kiếm:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Duyệt An toàn**.
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

5. Đảm bảo rằng **Bảo vệ Duyệt web** đã được bật.
6. Chọn **Hiển thị xếp hạng uy tín cho trang web trong kết quả tìm kiếm**.
7. Nếu trình duyệt của bạn mở ra, hãy khởi động lại trình duyệt để áp dụng thiết lập đã thay đổi.

Lưu ý: Bảo vệ Duyệt web yêu cầu tiện ích mở rộng Bảo vệ Duyệt web đã được bật trong trình duyệt web bạn sử dụng.

3.1.3 B□n ph□i làm gì khi m□t trang web b□ ch□n

Trang chặn tính năng bảo vệ duyệt web sẽ xuất hiện khi bạn cố truy cập trang web đã được xếp hạng là có hại.

Khi trang chặn tính năng bảo vệ duyệt web xuất hiện:

1. Nếu bạn muốn vào trang web, hãy chọn **Cho phép trang web trên máy tính này**. Bạn cần quyền quản trị viên để cho phép các trang web bị chặn.
   Các **Thêm trang web được phép** cửa sổ mở ra, hiển thị địa chỉ mà bạn sắp cho phép.
2. Chọn **OK**.

Trang web bị chặn sẽ mở ra. Ngoài ra, sản phẩm còn thêm trang web vào danh sách các trang web được phép.

Nếu bạn nghĩ rằng trang web bị chặn là an toàn và không nên bị chặn gì cả, bạn có thể gửi trang web đó để phân tích ở đây.

Lưu ý: Nếu trang chặn không xuất hiện, hãy đảm bảo rằng tiện ích mở rộng Bảo vệ Duyệt web đã được bật trong trình duyệt web bạn sử dụng.

3.1.4 Các tr□□ng h□p ngo□i l□ c□a trang web.

Danh sách ngoại lệ trang web hiển thị các trang web cụ thể được phép hoặc đã bị chặn.

Lưu ý: Nếu quản trị viên của bạn đã chặn hoàn toàn trang web hoặc nếu trang web đó chứa nội dung đã bị chặn thì bạn không thể truy cập vào trang web đó ngay cả khi bạn đã thêm trang web đó vào danh sách **Được phép**.

Để xem và chỉnh sửa ngoại lệ trang web:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Duyệt An toàn** > **Cài đặt Sửa**.
4. Chọn **Xem các trường hợp ngoại lệ của trang web**.

Nếu trang web bạn muốn sửa đã được liệt kê dưới dạng được phép hoặc bị từ chối và bạn muốn chuyển trang web đó từ danh sách này sang danh sách khác:

a) Tuỳ thuộc vào danh sách trang web bạn muốn sửa, hãy chọn tab **Được phép** hoặc **Bị từ chối**.
b) Nhấp chuột phải vào trang web trên danh sách và chọn **Cho phép** hoặc **Từ chối**.

Nếu trang web không được bao gồm trong một trong các danh sách đó:

a) Chọn tab **Được phép** nếu bạn muốn cho phép trang web hoặc tab **Bị từ chối** nếu bạn muốn chặn trang web.
b) Chọn **Thêm** để thêm trang web mới vào danh sách.
c) Nhập địa chỉ của trang web bạn muốn thêm rồi chọn **OK**.
d) Trong hộp thoại **Ngoại lệ của trang web**, hãy chọn **Đóng**.

5. Chọn **OK** để quay lại trang chính.

Để thay đổi địa chỉ của trang web được phép hoặc bị chặn, nhấp chuột phải vào trang web trên danh sách và chọn **Sửa**.

Để xoá trang web được phép hoặc bị chặn khỏi danh sách, hãy chọn trang web và nhấp vào **Xoá**.

3.2 Tri□n khai ti□n ích m□ r□ng b□o v□ duy□t qua GPO

Hướng dẫn cách cài đặt tiện ích mở rộng WithSecure Browsing Protection trong Google Chrome, Microsoft Edge và Mozilla Firefox.

Lưu ý: Các hướng dẫn là Elements Endpoint Protection -cụ thể và dành cho người dùng quản trị viên.

WithSecure Bảo vệ duyệt web là một tiện ích mở rộng dành cho các trình duyệt web cung cấp hỗ trợ giao thức HTTPS cho các trình duyệt đã cài đặt.WithSecure sản phẩm an ninh.

Lưu ý: Hỗ trợ HTTP được cung cấp mà không cần sử dụng tiện ích mở rộng.

Tiện ích mở rộng cho phépVớiSecurechặn trang hỗ trợ nội dung web không mong muốn, biểu tượng xếp hạng và chế độ Tìm kiếm an toàn cho các công cụ tìm kiếm khi sử dụng HTTPS. Với tư cách là quản trị viên, bạn có thể bậtVớiSecuree Bật Bảo vệ duyệt web và buộc bật tính năng này bằng cách sử dụng Chính sách nhóm Windows.

3.2.1 Cách cài □□t ti□n ích m□ r□ng b□o v□ duy□t web WithSecure trên Google Chrome

Các hướng dẫn này là dành riêng cho Elements Endpoint Protection và dành cho người dùng quản trị viên.

Để cài đặt và bật tiện ích mở rộng bảo vệ duyệt web:

1. Tải về mới nhất Mẫu chính sách nhóm Google Chrome Tệp ADMX.
2. Sao chép các tệp mẫu quản trị Chrome sau đây và thư mục ngôn ngữ của ngôn ngữ được sử dụng trong hệ thống của bạn vào `C:\Windows\PolicyDefinitions` danh mục:

   `policy_templates/windows/admx/chrome.admx and google.admx`

3. Sao chép các tệp và thư mục ngôn ngữ của ngôn ngữ được sử dụng trong hệ thống của bạn vào thư mục SYSVOL:
   `\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`.
   Ví dụ:`\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`.

   

   Lưu ý: Nếu chưa có thư mục PolicyDefinitions, bạn cần tạo nó.

4. Mở bảng điều khiển Quản lý chính sách nhóm Windows (`gpmc.msc`) và tạo chính sách nhóm mới hoặc chỉnh sửa chính sách hiện tại của bạn.

   

   Lưu ý: Để biết thêm thông tin, hãy tham khảo Tạo và quản lý Cửa hàng trung tâm cho các Mẫu quản trị chính sách nhóm trong Windows.

5. Đi đến `Computer Configuration/Policies/Administrative Templates/Google/Google Chrome/Extensions/Configure the list of Force-Installed apps and extensions` và chỉnh sửa chính sách như sau:
   a) Lựa chọn **Đã bật** để bật chính sách.
   b) Trong Tùy chọn, chọn **Trình diễn...** và nhập giá trị sau:

```
jmjjnhpacphpjmnnlnccpfmhkcloaade
```

> **Lưu ý:** Để biết thêm thông tin, xem cách đặt chính sách trình duyệt Chrome.

Khi chính sách nhóm được kích hoạt, tính năng Bảo vệ duyệt web an toàn sẽ được bật và buộc phải bật.

3.2.2 Cách cài đặt tiện ích mở rộng bảo vệ trình duyệt WithSecure trong Microsoft Edge (Chromium)

Các hướng dẫn này là dành riêng cho Elements Endpoint Protection và dành cho người dùng quản trị viên.

> **Lưu ý:** Tiện ích mở rộng WithSecure Browser được cài đặt từ Google Store thông qua Đối tượng chính sách nhóm của Microsoft (GPO). Thiết bị phải là thành viên của miền Microsoft Active Directory nếu không việc cài đặt này không thể thực hiện được.

Để cài đặt và bật tiện ích mở rộng bảo vệ trình duyệt:

1. Sử dụng tệp chính sách Microsoft Edge để thực hiện những việc sau:
   a) Đi đến Mẫu chính sách nhóm Microsoft Edge (Chromium) Tệp ADMX.
   b) Lựa chọn **Tải xuống Chính sách Windows** trong phiên bản và bản dựng của trình duyệt cũng như hệ điều hành của bạn, sau đó chọn **Chấp nhận và tải xuống**.
   c) Giải nén tệp cab mà bạn đã tải xuống.
   d) Từ các thư mục đã giải nén, sao chép vào cả hai `C:\Windows\PolicyDefinitions` thư mục và thư mục SYSVOL của bạn (`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`) các tệp và thư mục sau:
      - Tệp mẫu quản trị Microsoft Edge (Chromium):`msedge.admx` Và `msedgeupdate.admx`
      - Thư mục ngôn ngữ của ngôn ngữ được sử dụng trong hệ thống của bạn

> **Lưu ý:** Nếu chưa có thư mục PolicyDefinitions, bạn cần tạo nó.

2. Mở bảng điều khiển Quản lý chính sách nhóm Windows (gpmc.msc) và thực hiện một trong các thao tác sau:

> **Lưu ý:** Để biết thêm thông tin, hãy tham khảo Định cấu hình cài đặt chính sách Microsoft Edge trên Windows.

- Tạo chính sách nhóm mới
- Đi đến `Computer Configuration/Policies/Administrative Templates/Microsoft Edge/Extensions/Control which extensions are installed silently` và chỉnh sửa chính sách như sau:

  a. Lựa chọn **Đã bật** để bật chính sách.
  b. Trong Tùy chọn, chọn **Trình diễn...** và nhập giá trị sau:

```
cpikpibllpjmpnchjajlibnmmomnnhnm
```

Khi chính sách nhóm được kích hoạt, tính năng Bảo vệ duyệt web an toàn sẽ được bật và buộc phải bật.

3.2.3 Cách cài đặt tiện ích mở rộng bảo vệ duyệt web WithSecure trên Mozilla Firefox

Các hướng dẫn này là dành riêng cho Elements Endpoint Protection và dành cho người dùng quản trị viên.

Để cài đặt và bật tiện ích mở rộng bảo vệ trình duyệt:

1. Tải về mới nhất Mẫu chính sách nhóm Mozilla Firefox Tệp ADMX.
2. Giải nén tệp cab và sao chép các tệp mẫu quản trị Mozilla Firefox sau đây và thư mục ngôn ngữ của ngôn ngữ được sử dụng trong hệ thống của bạn vào `C:\Windows\PolicyDefinitions` danh mục:
   `windows/mozilla.admx and firefox.admx`
3. Sao chép các tệp và thư mục ngôn ngữ của ngôn ngữ được sử dụng trong hệ thống của bạn vào thư mục SYSVOL:`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`.
   Ví dụ:`\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`.

   Lưu ý: Nếu chưa có thư mục PolicyDefinitions, bạn cần tạo nó.
4. Mở bảng điều khiển Quản lý chính sách nhóm Windows (`gpmc.msc`) và tạo chính sách nhóm mới hoặc chỉnh sửa chính sách hiện tại của bạn.
5. Đi đến `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Extensions to install` và chỉnh sửa chính sách như sau:
   a) Lựa chọn **Đã bật** để bật chính sách.
   b) Trong Tùy chọn, chọn **Trình diễn...** và nhập giá trị sau:

   ```
   https://download.sp.f-secure.com/online-safety/fs_firefox_https.xpi
   ```

6. Đi đến `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Prevent extensions from being disabled or removed` và chỉnh sửa chính sách như sau:
   a) Lựa chọn **Đã bật** để bật chính sách.
   b) Trong Tùy chọn, chọn **Trình diễn...** và nhập giá trị sau:`ols@f-secure.com`.

Khi chính sách nhóm được kích hoạt, tính năng Bảo vệ duyệt web an toàn sẽ được bật và buộc phải bật.

3.3 Đang kiểm tra xem các tiện ích mở rộng trình duyệt có đang được sử dụng không

Duyệt web dựa trên danh tiếng **yêu cầu** các tiện ích mở rộng trình duyệt để có thể bảo vệ duyệt web, ngân hàng trực tuyến và mua sắm của bạn, đồng thời hiển thị cho bạn thông tin bảo mật trong khi bạn đang duyệt internet.

Sau khi bạn đã cài đặt sản phẩm trên máy tính của mình, sản phẩm sẽ cố gắng cài đặt các tiện ích mở rộng của trình duyệt một cách tự động. Khi bạn mở trình duyệt của mình, sản phẩm sẽ hiển thị thông báo về tiện ích mở rộng mới được cài đặt và bạn có thể cần phải bật tiện ích mở rộng đó.

Nếu tiện ích mở rộng Bảo vệ Duyệt web của WithSecure không được liệt kê trong trình duyệt của bạn, bạn cần cài đặt lại tiện ích mở rộng này theo cách thủ công.

Nếu bạn bỏ lỡ thông báo, chế độ xem chính của sản phẩm sẽ hiển thị cho bạn nếu tiện ích mở rộng của trình duyệt chưa được thiết lập. Cách dễ nhất để thiết lập tiện ích mở rộng cho trình duyệt của bạn là chọn **Thiết lập** từ thông báo được hiển thị trên chế độ xem chính của sản phẩm và làm theo hướng dẫn trên màn hình.

Tuy nhiên, nếu bạn không thấy thông báo trên chế độ xem chính của sản phẩm hoặc bạn đã bỏ lỡ thông báo đó, bạn có thể kiểm tra xem tiện ích mở rộng của trình duyệt đã được cài đặt cũng như được bật chưa bằng cách sau:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.

2. Trên trang chính, chọn ⚙.
3. Chọn **Chỉnh sửa cài đặt** trong màn hình bật lên ở góc dưới cùng bên trái.

Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

4. Chọn **Có** để cho phép ứng dụng thực hiện các thay đổi đối với thiết bị của bạn.
5. Chọn **Duyệt An toàn**.
6. Tùy thuộc vào trình duyệt web bạn sử dụng, hãy thực hiện như sau:
   - Nếu bạn sử dụng **Firefox**, trong **Phần bổ trợ và chủ đề** > **Tiện ích mở rộng**, hãy chọn **Thêm vào Firefox**. Tiện ích mở rộng sẽ được thêm và kích hoạt cho Firefox.
   - Nếu bạn sử dụng **Chrome**, trước tiên hãy chọn liên kết **Mở Cửa hàng Chrome Trực tuyến** trong **Tiện ích mở rộng trình duyệt**. Trang Bảo vệ Duyệt bằng WithSecure sẽ mở Cửa hàng Chrome Trực tuyến. Nếu tiện ích mở rộng đã được cài đặt trên Chrome nhưng bị tắt thì hãy đi tới **Tiện ích mở rộng** và bật tiện ích mở rộng đó. Nếu tiện ích mở rộng chưa được cài đặt, hãy chọn **Thêm vào Chrome** > **Thêm tiện ích mở rộng**. Tiện ích mở rộng sẽ được thêm vào cũng như được bật cho Chrome.
   - Nếu bạn sử dụng **Microsoft Edge**, trước tiên hãy chọn liên kết **Mở Tiện ích bổ sung Edge** bên dưới **Tiện ích mở rộng trình duyệt**. Trang Bảo vệ Duyệt web bằng WithSecure mở ra trong Tiện ích bổ sung Edge. Nếu tiện ích mở rộng đã được cài đặt trên Microsoft Edge nhưng bị vô hiệu hóa, hãy chọn **Bật** để bật tiện ích mở rộng đó. Nếu tiện ích mở rộng chưa được cài đặt, hãy chọn **Tải** > **Thêm tiện ích mở rộng**. Tiện ích mở rộng sẽ được thêm cũng như được bật cho Microsoft Edge.

Lưu ý: Bạn có thể cần cài đặt lại các tiện ích mở rộng sau khi nâng cấp sản phẩm hoặc cài đặt trình duyệt mới.

Bạn có thể kiểm tra xem tiện ích mở rộng của trình duyệt đã được bật hay chưa bằng cách mở trang kiểm tra sau trong trình duyệt của mình: https://unsafe.fstestdomain.com. Nếu trang khối sản phẩm mở ra thì tiện ích mở rộng của trình duyệt đang được sử dụng. Nếu bạn không thấy trang khối sản phẩm thì bạn cần bật tiện ích mở rộng trình duyệt theo cách thủ công.

Ch□□ng
4

B□o v□ d□ li□u nh□y c□m c□a b□n

Chủ đề:

Kiểm soát kết nối sẽ bổ sung một lớp bảo mật khác nhằm ngăn những kẻ tấn công can thiệp vào các giao dịch bí mật của bạn cũng như bảo vệ bạn khỏi hoạt động độc hại, ví dụ: khi bạn truy cập vào ngân hàng trực tuyến hay thực hiện giao dịch trực tuyến.

Kiểm soát kết nối tự động phát hiện các kết nối bảo mật đến các trang web ngân hàng trực tuyến và chặn mọi kết nối không đến trang web dự định. Khi bạn mở trang web ngân hàng trực tuyến, chỉ các kết nối đến các trang web ngân hàng trực tuyến hoặc đến các trang web được coi là an toàn cho ngân hàng trực tuyến mới được phép.

Nếu bạn cần truy cập vào trang web bị chặn để hoàn tất giao dịch đang diễn ra của mình thì bạn có thể tạm thời cho phép quyền truy cập vào trang bị chặn hoặc kết thúc phiên ***Kiểm soát kết nối***.

Kiểm soát kết nối hiện hỗ trợ các trình duyệt sau đây:

- Microsoft Edge (Chromium)
- Firefox
- Google Chrome

4.1 B□t Ki□m soát k□t n□i

Khi ***Kiểm soát kết nối*** được bật, tính năng này sẽ cung cấp thêm biện pháp bảo vệ cho các kết nối bảo mật của bạn.

Kiểm soát kết nối sẽ chặn các kết nối không an toàn khi tính năng đó đang hoạt động. Ví dụ: khi bạn truy cập vào trang web của ngân hàng hoặc thực hiện thanh toán trực tuyến, ***Kiểm soát kết nối*** sẽ kích hoạt và chặn tất cả các kết nối không cần thiết cho ngân hàng trực tuyến, do đó, các kết nối đó không thể can thiệp vào các giao dịch bí mật của bạn.

Để bật ***Kiểm soát kết nối***:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Duyệt An toàn** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.
4. Bật **Kiểm soát Kết nối**.
5. Để điều chỉnh ***Kiểm soát kết nối*** cài đặt:
   - Xa lạ **Ngắt kết nối các ứng dụng không đáng tin cậy** nếu bạn không muốn ***Kiểm soát kết nối*** để đóng các kết nối đã mở của bạn. Nếu bạn không chọn cài đặt,***Kiểm soát kết nối*** đóng tất cả các kết nối Internet hiện tại của bạn khi nó kích hoạt.
   - Nếu bạn phải sử dụng một công cụ bên ngoài đang bị chặn bởi ***Kiểm soát kết nối***, xa lạ **Ngắt kết nối các công cụ dòng lệnh và tập lệnh**.

     Lưu ý: Chúng tôi khuyên bạn nên tiếp tục chọn cài đặt này trừ khi hoàn toàn không cần thiết do một số cuộc tấn công bằng phần mềm độc hại có thể sử dụng các cấu phần Windows được tích hợp, chẳng hạn như PowerShell, để giành quyền truy cập vào thông tin đăng nhập ngân hàng và thông tin cá nhân của bạn.
   - Chọn cách bạn muốn ***Kiểm soát kết nối*** để xử lý dữ liệu đã được sao chép vào khay nhớ tạm của bạn. Theo mặc định,***Kiểm soát kết nối*** xóa tất cả dữ liệu khỏi khay nhớ tạm để bảo vệ quyền riêng tư của bạn khi ***Kiểm soát kết nối*** phiên kết thúc.

     Xóa cài đặt này nếu bạn không muốn ***Kiểm soát kết nối*** để xóa khay nhớ tạm của bạn.
   - Theo mặc định, quyền truy cập từ xa vào thiết bị của bạn bị chặn trong phiên giao dịch ngân hàng của bạn. Các giao dịch ngân hàng luôn riêng tư và bảo mật, và bạn không bao giờ được đăng nhập vào ngân hàng trực tuyến của mình nếu ai đó có quyền truy cập từ xa vào thiết bị của bạn.

     Quan trọng: Không xóa cài đặt **Chặn truy cập từ xa trong phiên giao dịch ngân hàng** theo yêu cầu của bất kỳ ai trừ khi bạn biết cả người đang yêu cầu quyền truy cập và mục đích chính xác của yêu cầu.

4.2 S□ d□ng Ki□m soát k□t n□i

Khi ***Kiểm soát kết nối*** được bật, Kiểm soát kết nối sẽ tự động phát hiện thời điểm bạn truy cập vào trang web ngân hàng trực tuyến.

Khi bạn mở trang web ngân hàng trực tuyến trong trình duyệt của mình, chỉ báo ***Kiểm soát kết nối*** sẽ xuất hiện ở đầu màn hình. Tất cả các kết nối khác sẽ bị chặn trong khi bảo vệ ngân hàng đang hoạt động.

Mẹo: Nếu bạn không muốn làm gián đoạn các kết nối đang hoạt động khác của mình khi ***Kiểm soát kết nối*** kích hoạt, để thay đổi cài đặt, hãy chọn chỉ báo **Kiểm soát kết nối** rồi chọn ⚙ ở góc trên cùng bên phải của thông báo Kiểm soát kết nối.

Để kết thúc phiên ***Kiểm soát kết nối*** và khôi phục các kết nối khác của bạn:

1. Nhấp vào chỉ báo **Kiểm soát kết nối** ở đầu màn hình của bạn.

2. Nhấp vào **Kết thúc** trên thông báo.

Ch□□ng
5

Thi□t l□p ki□m soát n□i dung

Chủ đề:

- Chặn nội dung web

Bạn có thể giới hạn quyền truy cập vào nội dung không phù hợp nhằm tránh phải xem nội dung không mong muốn trên internet.

Internet có rất nhiều trang web thú vị, nhưng không phải tất cả đều chứa nội dung mà bạn có thể cho là mong muốn hoặc phù hợp.

Với trình chặn nội dung, bạn có thể đảm bảo không ai xem nội dung không phù hợp trên các máy tính bằng cách hạn chế những trang web có thể được xem và lên lịch thời gian có thể dành cho trực tuyến. Bạn cũng có thể chặn các liên kết đến nội dung người lớn hiển thị trong các kết quả của công cụ tìm kiếm.

5.1 Ch□n n□i dung web

Bạn có thể giới hạn các loại nội dung có thể được xem trong khi duyệt web.

Bạn có thể chặn quyền truy cập vào trang và trang web chứa nội dung không phù hợp.

Để chọn loại nội dung web cần chặn:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Kiểm soát Nội dung Web**.
4. Chọn người mà cài đặt áp dụng cho từ menu thả xuống.
5. Bật **Lọc nội dung** để giới hạn nội dung bạn chọn trên tất cả các trình duyệt.
   - Để chặn các trang web theo loại nội dung, hãy chọn **Chặn nội dung web**. Sau đó, chọn hộp kiểm bên cạnh loại nội dung bạn muốn chặn.
   - Để chỉ cho phép truy cập vào các trang web nhất định, hãy chọn **Chỉ cho phép các trang web đã chọn**. Sau đó, hãy chọn **Xem các trang web được phép** và nhập địa chỉ web mà bạn muốn cho phép.
6. Để ẩn nội dung người lớn khỏi kết quả tìm kiếm, hãy bật **Bộ lọc Kết quả Tìm kiếm**.

5.1.1 Danh m□c n□i dung

Bạn có thể chặn quyền truy cập vào một vài loại nội dung.

Nạo phá thai	Các trang web chứa thông tin hoặc hình ảnh về nạo phá thai, phòng khám và trung tâm nạo phá thai cũng như các chủ đề về nạo phá thai nói chung. Ví dụ: các diễn đàn thảo luận có thể ủng hộ sự sống hoặc ủng hộ sự lựa chọn.
Quảng cáo	Các liên kết web trỏ đến các tệp flash, văn bản, video hoặc hình ảnh khác nhau hoặc các tệp tương tự khác có chứa quảng cáo.
Người lớn	Các trang web nhằm vào đối tượng người lớn có nội dung mang tính gợi dục rõ ràng hoặc ám chỉ hành vi tình dục. Ví dụ: các trang web bán đồ chơi tình dục hoặc tranh khỏa thân nhắm vào hành vi tình dục.
Rượu và thuốc lá	Các trang web hiển thị hoặc quảng bá đồ uống có cồn hoặc thuốc lá và các sản phẩm thuốc lá, bao gồm cả các nhà sản xuất như nhà máy rượu, vườn nho và nhà máy bia. Ví dụ: các trang web quảng bá lễ hội bia và các trang web giới thiệu quán bar và câu lạc bộ đêm.
Người ẩn danh	Các trang web cho phép hoặc hướng dẫn mọi người cách bỏ qua bộ lọc mạng, kể cả các trang web dịch dựa trên web cho phép mọi người làm như vậy. Ví dụ: các trang web cung cấp danh sách những proxy công khai mà có thể được sử dụng để bỏ qua bộ lọc mạng có thể có.
Đấu giá	Các trang web của thị trường trực tuyến nơi mọi người có thể mua và bán sản phẩm hoặc dịch vụ của họ. Điều này bao gồm các trang web cung cấp danh sách các sản phẩm hoặc dịch vụ mặc dù giao dịch thực tế có thể diễn ra ở một nơi khác.
Ngân hàng	Các trang web của ngân hàng và các tổ chức tài chính khác, bao gồm các ngân hàng tiết kiệm và đầu tư, các trang web giao dịch chứng khoán cũng như giao dịch ngoại hối.
Blog	Các blog nơi mọi người hoặc tổ chức xuất bản thông tin và có thể chia sẻ tin tức, câu chuyện, video và ảnh. Do tính chất cá nhân, các chủ đề được đề cập trong blog có thể rất khác nhau và chúng có thể bao gồm bất kỳ chủ đề nào.
Trò chuyện	Cổng thông tin trực tuyến và trình nhắn tin nơi mọi người có thể trò chuyện với nhau qua văn bản, âm thanh hoặc video. Ví dụ: các ứng dụng trò chuyện và nhắn tin tức thời trên nền web cũng như các trang trò chuyện.
Hẹn hò	Các trang web cung cấp cổng thông tin để tìm đối tác lãng mạn hoặc bạn tình. Ví dụ: các trang web mai mối hoặc trang web đặt cô dâu qua thư.

Ma túy	Các trang web quảng bá việc sử dụng ma túy. Ví dụ: các trang web cung cấp thông tin về việc mua, trồng hay bán bất kỳ dạng nào trong số các chất này.
Giải trí	Các trang web liên quan đến ngành giải trí, chẳng hạn như chương trình truyền hình, sách, truyện tranh, phim và rạp hát cũng như phòng trưng bày nghệ thuật. Ví dụ: hướng dẫn chương trình truyền hình và đài phát thanh cũng như các trang web đánh giá âm nhạc, truyền hình và phim.
Cờ bạc	Các trang web mà tại đó mọi người có thể cá cược trực tuyến bằng tiền thật hoặc một số hình thức tín dụng. Ví dụ: các trang web xổ số và đánh bạc trực tuyến, blog và diễn đàn có chứa thông tin về đánh bạc trực tuyến hoặc trong đời sống thực tế.
Trò chơi	Các trang web trò chơi trực tuyến và các trang web nơi mọi người có thể chơi, tải xuống hoặc mua trò chơi.
Tấn công	Các trang web khuyến khích việc tìm kiếm và khai thác điểm yếu trong hệ thống máy tính hoặc mạng máy tính để kiếm lợi nhuận, thử thách hoặc giải trí. Ví dụ: các trang web chứa hướng dẫn tấn công cũng như công cụ tấn công.
Hận thù	Các trang web thể hiện thành kiến với một tôn giáo, chủng tộc, quốc tịch, giới tính, tuổi tác, tình trạng khuyết tật hoặc xu hướng tình dục nào đó. Ví dụ: các trang web thúc đẩy việc gây hại cho con người, động vật hay tổ chức hoặc có chứa phần mô tả hay hình ảnh về hành vi hành hung thể xác đối với bất kỳ đối tượng nào trong số đó.
Tải xuống bất hợp pháp	Các trang web sao chép trái phép phần mềm hoặc chia sẻ tệp trái phép. Ví dụ: các trang web cung cấp quyền truy cập bất hợp pháp hoặc đáng ngờ vào phần mềm cũng như các trang web phát triển và phân phối những chương trình có thể làm ảnh hưởng đến mạng và hệ thống.
Tìm việc làm	Các trang web của các cơ quan việc làm và nhà thầu cũng như nơi mọi người có thể tìm kiếm công việc mới. Ví dụ: công cụ tìm kiếm nghề nghiệp, nhóm mạng lưới nghề nghiệp và trang web việc làm.
Dịch vụ thanh toán	Các trang web xử lý hoạt động thanh toán giữa các trang mua sắm và ngân hàng hoặc các dịch vụ tài chính khác, chẳng hạn như thẻ tín dụng. Chúng bao gồm các trang web có thể được sử dụng để thanh toán nói chung.
Gian lận	Các trang web dụ dỗ mọi người bằng cách hứa hẹn các giải thưởng sau khi họ điền vào bản khảo sát, chơi đố vui hoặc thực hiện các hành động tương tự.
Mua sắm	Các trang web nơi mọi người có thể mua bất kỳ sản phẩm hoặc dịch vụ nào, bao gồm các trang web chứa danh mục các mặt hàng tạo điều kiện mua và đặt hàng trực tuyến cũng như các trang web cung cấp thông tin về việc đặt hàng và mua các mặt hàng trực tuyến.
Mạng xã hội	Các cổng mạng nhìn chung sẽ kết nối mọi người hoặc với một nhóm người nhất định để giao tiếp xã hội, tiếp xúc kinh doanh và nhiều mục đích khác. Ví dụ: các trang web mà tại đó bạn có thể tạo hồ sơ thành viên để chia sẻ sở thích cá nhân và nghề nghiệp. Trong đó bao gồm cả các trang web truyền thông xã hội như Twitter.
Tải xuống phần mềm	Cổng thông tin trực tuyến để tải xuống các phần mềm khác nhau.
Thư rác	Các trang web được thu thập từ thư rác.
Phương tiện truyền phát	Các trang web cung cấp nội dung âm thanh hoặc video phát trực tuyến miễn phí hoặc thông qua mô hình đăng ký.
Bạo lực	Các trang web có thể kích động bạo lực hoặc chứa hình ảnh hay video bạo lực và khủng khiếp. Ví dụ: các trang web chứa thông tin về cưỡng hiếp, quấy rối, hút thuốc lá, bom, tấn công, giết người và tự tử.
Vũ khí	Các trang web có chứa thông tin, hình ảnh hoặc video về vũ khó hay bất cứ vật gì có thể được sử dụng làm vũ khí gây hại cho con người hoặc động vật, kể cả các tổ chức thúc đẩy những vũ khí này, chẳng hạn như câu lạc bộ săn bắn. Danh mục này bao gồm vũ khí đồ chơi như súng bắn sơn, súng hơi và súng BB.

Thư trên nền web Các trang web cho phép mọi người tạo và truy cập vào tài khoản email của họ thông qua trình duyệt web. Ví dụ: điều này bao gồm Yahoo! Mail và Gmail cũng như các dịch vụ thư web cục bộ được liên kết với ISP.

Ch□□ng
6

S□ d□ng b□ l□c k□t qu□ tìm ki□m

Chủ đề:

- Bật bộ lọc kết quả tìm kiếm

Bộ lọc kết quả tìm kiếm ẩn nội dung người lớn bằng cách đảm bảo rằng Google, Yahoo, Bing và YouTube sử dụng mức độ "nghiêm ngặt" của Tìm kiếm an toàn.

Mặc dù điều này không thể chặn tất cả nội dung không phù hợp và tục tĩu xuất hiện trong kết quả tìm kiếm của bạn, nhưng nó giúp bạn tránh hầu hết các tài liệu như vậy.

6.1 Bật bộ lọc kết quả tìm kiếm

Bạn có thể bật bộ lọc kết quả tìm kiếm để chặn nội dung khiêu dâm khỏi các kết quả tìm kiếm.

Để bật bộ lọc kết quả tìm kiếm:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Kiểm soát Nội dung Web**.
4. Bật **Bộ lọc Kết quả Tìm kiếm**.

Khi bộ lọc kết quả tìm kiếm được bật, bộ lọc đó sẽ ghi đè thiết lập chế độ Tìm kiếm An toàn trên các trang web mà mọi người đã đăng nhập vào tài khoản người dùng Windows đó.

Ch□□ng
7

Qu□n lý t□p trung

Chủ đề:

- Mở Trình xem sự kiện trong Windows

Sản phẩm này được chạy ở chế độ được quản lý tập trung, trong đó cài đặt sản phẩm được điều khiển từ xa bởi chuyên gia đáng tin cậy.

Trong chế độ được quản lý tập trung:

- một số hoặc tất cả các cài đặt sản phẩm có thể được đặt từ xa.
- một vài trong số các cài đặt này có thể bị khoá, vì vậy bạn không thể tự thay đổi chúng.

Trang **Quản lý tập trung** > **Cài đặt** sẽ hiển thị thông tin về máy tính của bạn. Bạn có thể cần phải cung cấp thông tin này cho quản trị viên CNTT của mình nếu xảy ra sự cố với cài đặt sản phẩm.

Dùng Trình xem sự kiện trong Windows để xem các lỗi đã ghi.

7.1 M Trình xem s ki n trong Windows

Nếu nghi ngờ có sự cố với sản phẩm này, bạn có thể dùng Trình xem sự kiện trong Windows để kiểm tra xem lỗi đã được ghi chưa.

Trình xem sự kiện trong Windows lưu trữ chi tiết về các sự kiện nhập của hệ thống, bao gồm chi tiết về các tác vụ và lỗi của sản phẩm này.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Quản lý tập trung**.
4. Nhấp **Mở Trình xem Sự kiện**.
   Trình xem sự kiện trong Windows mở ra.
5. Để tìm thông báo từ sản phẩm này, hãy nhấp vào **Nhật ký Windows** và chọn **Ứng dụng** hoặc **Hệ thống**.

   👉 **Lưu ý:** Bạn có thể nhấp **Nguồn** để sắp xếp các thông báo theo nguồn của chúng. Việc này giúp tìm kiếm các thông báo từ sản phẩm này dễ dàng hơn.

Ch□□ng
8

T□□ng l□a là gì

Chủ đề:

- Thay đổi thiết đặt Tường lửa của Windows
- Sử dụng tường lửa cá nhân

Tường lửa ngăn những kẻ xâm nhập và các ứng dụng độc hại xâm nhập vào máy tính của bạn từ internet.

Tường lửa chỉ cho phép kết nối Internet an toàn từ máy tính của bạn và chặn các xâm nhập từ internet.

8.1 Thay □□i thi□t □□t T□□ng l□a c□a Windows

Khi tường lửa được bật, tường lửa giới hạn quyền truy cập vào và ra khỏi máy tính của bạn. Một số ứng dụng có thể yêu cầu bạn cho phép chúng vượt qua tường lửa để hoạt động đúng cách.

Sản phẩm sử dụng Tường lửa của Windows để bảo vệ máy tính của bạn.

Để thay đổi thiết đặt Tường lửa của Windows:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên chế độ xem chính, hãy chọn **Vi-rút & Mối đe dọa**.
3. Chọn **Cài đặt Tường lửa của Windows**.

Để biết thêm thông tin về Tường lửa của Windows, hãy tham khảo tài liệu Microsoft Windows.

8.2 S□ d□ng t□□ng l□a cá nhân

Sản phẩm được thiết kế để hoạt động với Tường lửa Windows. Các tường lửa cá nhân khác yêu cầu thiết lập bổ sung để hoạt động với sản phẩm.

Sản phẩm sử dụng Tường lửa Windows cho các chức năng tường lửa cơ bản, chẳng hạn như kiểm soát lưu lượng truy cập mạng đến và giữ mạng cục bộ của bạn tách biệt khỏi Internet công cộng. Ngoài ra, DeepGuard giám sát các ứng dụng đã cài đặt và ngăn các ứng dụng khả nghi đăng nhập vào internet khi không có sự cho phép của bạn.

Nếu bạn thay Tường lửa Windows bằng một tường lửa cá nhân, hãy đảm bảo rằng tường lửa cá nhân đó cho phép lưu lượng truy cập mạng đi và đến cho tất cả các quá trình của WithSecure và rằng cho phép tất cả các quá trình của WithSecure khi tường lửa cá nhân nhắc bạn thực hiện như vậy.

Mẹo: Nếu tường lửa cá nhân của bạn có chế độ lọc thủ công, hãy sử dụng chế độ lọc đó để cho phép tất cả các quá trình của WithSecure.

Ch□□ng
9

Gi□ cho ph□n m□m c□a b□n □□□c c□p nh□t

Bạn có thể sử dụng sản phẩm để kiểm tra phần mềm được cài đặt trên máy tính của mình cũng như cài đặt mọi bản cập nhật bị thiếu.

Lưu ý: Quản trị viên của bạn có thể giới hạn cài đặt các bản cập nhật phần mềm trên các máy tính được quản lý.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn .
   Chế độ xem **Cập nhật phần mềm** hiển thị các bản cập nhật chưa được cài đặt.
3. Chọn **Nhấp vào đây để quản lý các bản cập nhật của bạn**.

   Lưu ý: Bạn cần có quyền quản trị để cài đặt các bản cập nhật bị thiếu.
4. Chọn **Kiểm tra ngay bây giờ** nếu bạn muốn xem liệu có sẵn bản cập nhật mới nào không.
5. Chọn bản cập nhật bạn muốn cài đặt.
6. Chọn **Cài đặt bản cập nhật được chọn**.
   Tab **Cài đặt** hiển thị cho bạn trạng thái và tiến trình cho từng bản cập nhật được chọn.

Ch□□ng
10

Cách s□ d□ng b□n c□p nh□t

Chủ đề:

- Xem cập nhật mới nhất
- Cập nhật định nghĩa phần mềm độc hại trên các máy chủ Bảo mật Khách hàng bị cô lập
- Thay đổi thiết lập kết nối

Các bản cập nhật giúp máy tính của bạn được bảo vệ khỏi các mối đe dọa mới nhất.

Sản phẩm tự động truy xuất các bản cập nhật mới nhất về máy tính của bạn khi thiết bị của bạn được kết nối với internet. Sản phẩm đó sẽ phát hiện lưu lượng truy cập mạng và không làm phiền việc sử dụng internet khác của bạn ngay cả khi kết nối mạng chậm.

10.1 Xem c□p nh□t m□i nh□t

Xem ngày và giờ của cập nhật mới nhất.

Khi cập nhật tự động được bật, sản phẩm sẽ tự động nhận được các cập nhật mới nhất khi bạn kết nối với internet.

Để xem thông tin chi tiết về các cập nhật mới nhất cho các sản phẩm đã cài đặt của bạn:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Cập nhật**.
4. Bạn sẽ thấy thông tin chi tiết về các bản cập nhật mới nhất trong **Kết nối**.
5. Để kiểm tra các cập nhật mới nhất theo cách thủ công, hãy chọn **Kiểm tra bây giờ**.
   Sản phẩm sẽ tự động cài đặt các bản cập nhật mới nhất nếu có sẵn.

   👉 **Lưu ý:** Kết nối internet của bạn phải đang hoạt động khi bạn muốn kiểm tra các bản cập nhật mới nhất.

10.2 C□p nh□t □□nh ngh□a ph□n m□m □□c h□i trên các máy ch□ B□o m□t Khách hàng b□ cô l□p

Nếu bạn đã cài đặt Client Security trên máy chủ không có kết nối mạng, bạn có thể cập nhật định nghĩa phần mềm độc hại bằng công cụ được cung cấp cùng với Trình quản lý chính sách.

Công cụ tải xuống các bản cập nhật đi kèm với Trình quản lý chính sách và có thể được trích xuất bằng các tập lệnh được cung cấp. Khi bạn chạy nó trên bất kỳ máy nào có quyền truy cập Internet, công cụ sẽ tải xuống các bản cập nhật mới nhất và các khác biệt bắt buộc để tạo một kho lưu trữ tất cả trong một.

Theo mặc định, công cụ này sử dụng `data\updates` thư mục để lưu trữ các tệp nhị phân cập nhật đã tải xuống. Nó cũng lưu trữ lịch sử cập nhật để sử dụng làm tài liệu tham khảo cho việc tải các khác biệt có liên quan về phiên bản mới nhất.

Ngoài các tệp nhị phân cập nhật, bạn cũng cần có `fsaua-update_32` công cụ để nhập các bản cập nhật đã chuẩn bị. Công cụ này được bao gồm trong gói cài đặt Client Security:`C:\Program Files (x86)\F-Secure\Client Security\fsaua-update_32.exe`.

Để cập nhật định nghĩa phần mềm độc hại:

1. Chạy lệnh sau trên máy Trình quản lý chính sách để chuẩn bị công cụ:
   - Các cửa sổ:`<F-Secure installation folder> \Máy ch  qu n lý 5\bin\prepare-fspm-def  nh-update-tool.bat<destination folder>`
   - Linux:`/opt/f-secure/fspms/bin/prepare-fspm-def  nh-update-tool<destination folder>`
2. Chuyển các tệp nhị phân đã chuẩn bị sang máy có truy cập Internet, nếu cần.
3. Sửa đổi cấu hình công cụ, nếu cần:
   - `conf\channels.json`: phần này chứa danh sách các kênh sẽ được cập nhật. Theo mặc định, nó bao gồm các bản cập nhật cho tất cả các máy khách được hỗ trợ do Trình quản lý chính sách quản lý, vì vậy chúng tôi khuyên bạn chỉ nên để lại các phiên bản Bảo mật máy khách cần thiết cho môi trường của mình.
4. Chạy công cụ:
   - Các cửa sổ:`fspm-  nh ngh a-update-tool.bat`
   - Linux:`công c  c p nh t-  nh ngh a fspm`

   Kho lưu trữ kết quả chứa tập hợp đầy đủ các định nghĩa và điểm khác biệt mới nhất đối với phiên bản này. Nếu tất cả dữ liệu đều được cập nhật thì không có bản lưu trữ nào được tạo.

5. Chuyển kho lưu trữ đã chuẩn bị (`data\f-secure-updates.zip` theo mặc định) vào thư mục máy chủ bị cô lập trên máy chủ Bảo mật khách hàng bị cô lập:`C:\Program Files (x86)\F-Secure\Client Security`
6. Khởi chạy bản cập nhật trên máy chủ bị cô lập: Chạy `C:\Program Files (x86)\F-Secure\Client Security\fsaua-update_32.exe` với đặc quyền của quản trị viên.

10.3 Thay □□i thi□t l□p k□t n□i

Các hướng dẫn về cách thay đổi cách máy tính của bạn kết nối với internet cũng như cách bạn muốn xử lý các cập nhật trong khi sử dụng các mạng di động.

Nhà cung cấp dịch vụ internet có thể cung cấp hoặc yêu cầu bạn sử dụng proxy. Proxy hoạt động như trung gian giữa máy tính của bạn và internet. Proxy sẽ chặn tất cả các yêu cầu vào Internet để xem liệu proxy có thể hoàn thành yêu cầu bằng cách sử dụng bộ nhớ đệm của mình không. Các proxy được sử dụng để cải thiện hiệu suất, lọc các yêu cầu và ẩn máy tính của bạn khỏi internet nhằm nâng cao độ bảo mật.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Cập nhật** > **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi một số cài đặt.

4. Trong **Thiết lập proxy thủ công**, chọn xem máy tính của bạn có đang sử dụng máy chủ proxy để kết nối với internet hay không.
   - Chọn **Không sử dụng** nếu máy tính của bạn được kết nối trực tiếp với internet.
   - Chọn **Sử dụng thiết lập của trình duyệt** để sử dụng cùng một thiết lập proxy HTTP mà bạn đã định cấu hình trong trình duyệt web của mình.
   - Chọn **Địa chỉ tùy chỉnh** rồi thêm địa chỉ proxy và số **Cổng** để định cấu hình cài đặt proxy HTTP của bạn theo cách thủ công.

Ch□□ng
11

Quy□n riêng t□

Chủ đề:

- Dữ liệu Bảo mật
- Cải thiện sản phẩm

Phần này sẽ giải thích Security Cloud là gì và cách bạn có thể đóng góp dữ liệu ẩn danh và giúp chúng tôi cải thiện sản phẩm.

11.1 D□ li□u B□o m□t

Dịch vụ gửi các truy vấn về các hoạt động độc hại tiềm ẩn hoặc trên các thiết bị được bảo vệ tới WithSecure ***Đám mây bảo mật*** .

WithSecure Security Cloud là một hệ thống dựa trên đám mây để phân tích mối đe dọa mạng được vận hành bởi WithSecure. Chúng tôi thu thập lượng dữ liệu tối thiểu để cung cấp cho bạn các dịch vụ bảo mật mà bạn đã đăng ký và để cung cấp sự bảo vệ chất lượng cao cho người dùng của chúng tôi.

Với Đám mây bảo mật, WithSecure có thể duy trì tổng quan cập nhật về toàn cảnh mối đe dọa toàn cầu và bảo vệ khách hàng của chúng tôi chống lại các mối đe dọa mới ngay khi họ được tìm thấy lần đầu tiên.

Đám mây bảo mật chỉ thu thập dữ liệu có thể chứa thông tin về tệp hoặc trang web đã bị WithSecure chặn vì lý do bảo mật. Dữ liệu bảo mật không được sử dụng cho các mục đích tiếp thị được cá nhân hóa.

Đóng góp dữ liệu

Với tư cách là người đóng góp, bạn cho phép Security Cloud lưu giữ dữ liệu bảo mật giúp chúng tôi tăng cường biện pháp bảo vệ bạn trước các mối đe dọa mới và đang phát sinh. Dữ liệu được thu thập theo cách này chỉ được lưu giữ trong một thời gian giới hạn và sẽ bị xóa sau khoảng thời gian đó.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Đi tới trang cài đặt **Quyền riêng tư**.
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   

5. Trong **Security Cloud**, hãy chọn **Cho phép phân tích sâu hơn**.

11.2 C□i thi□n s□n ph□m

Bạn có thể giúp chúng tôi cải thiện sản phẩm bằng cách gửi dữ liệu sử dụng.

Để gửi dữ liệu sử dụng:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Đi tới trang cài đặt **Quyền riêng tư**.
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

   

5. Trong **Cải tiến sản phẩm**, hãy chọn **Gửi dữ liệu sử dụng không được cá nhân hóa**.

   Lưu ý: Bạn có thể đọc Tuyên bố về Quyền riêng tư của chúng tôi tại đây.

   

Ch□□ng
12

H□ tr□ k□ thu□t

Chủ đề:

- Tôi có thể tìm thấy thông tin phiên bản của sản phẩm ở đâu?
- Sử dụng công cụ hỗ trợ
- Gỡ lỗi các vấn đề về sản phẩm
- Lừa đảo qua điện thoại và phải làm gì nếu bạn cho rằng mình là mục tiêu

Tại đây, bạn có thể tìm thấy thông tin có thể giúp bạn giải quyết các sự cố kỹ thuật của mình.

Nếu bạn có câu hỏi về sản phẩm hoặc vấn đề với sản phẩm, trước khi liên hệ với bộ phận hỗ trợ khách hàng của chúng tôi, hãy truy cập Cộng đồng WithSecure và xem liệu bạn có thể tìm thấy câu trả lời cho câu hỏi của mình ở đó không.

12.1 Tôi có thể tìm thấy thông tin phiên bản của sản phẩm ở đâu?

Bộ phận hỗ trợ khách hàng của chúng tôi có thể yêu cầu thông tin về phiên bản sản phẩm của bạn nếu bạn cần liên hệ với chúng tôi.

Để xem thông tin phiên bản hiện có:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Hỗ trợ**.
4. Tìm thông tin về sản phẩm hiện được cài đặt trong **Thông tin phiên bản**.

12.2 Sử dụng công cụ hỗ trợ

Trước khi liên hệ với bộ phận hỗ trợ, hãy chạy công cụ hỗ trợ để thu thập thông tin cơ bản về phần cứng, hệ điều hành, cấu hình mạng và phần mềm được cài đặt.

Nếu bạn gặp sự cố kỹ thuật với sản phẩm bảo mật của mình, bộ phận hỗ trợ khách hàng của chúng tôi có thể yêu cầu bạn tạo và gửi tệp WSDIAG cho bộ phận hỗ trợ kỹ thuật của chúng tôi. Tệp chứa thông tin có thể được sử dụng để khắc phục sự cố và giải quyết các sự cố cụ thể đối với máy tính của bạn.

Bạn có thể tạo tệp bằng cách sử dụng Công cụ Hỗ trợ. Công cụ thu thập thông tin về hệ thống của bạn và cấu hình của nó. Thông tin bao gồm chi tiết sản phẩm, nhật ký hệ điều hành và cài đặt hệ thống. Lưu ý rằng một phần thông tin có thể được bảo mật. Thông tin thu thập được được lưu trữ trong một tệp được lưu trên màn hình máy tính của bạn.

Để chạy công cụ hỗ trợ:

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Hỗ trợ**.
4. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.
5. Chọn **Chạy công cụ hỗ trợ**.
6. Chọn **Chạy chẩn đoán** trên cửa sổ **Công cụ Hỗ trợ**.
   Công cụ hỗ trợ sẽ khởi động và hiển thị quá trình thu thập dữ liệu.

Khi công cụ chạy xong, nó sẽ lưu dữ liệu đã thu thập vào kho lưu trữ trên máy tính của bạn. Bạn có thể gửi dữ liệu đã thu thập (tệp chẩn đoán) tại đây:
https://www.withsecure.com/en/support/contact-support/email-support .

Mẹo: Nếu bạn không thể truy cập Công cụ hỗ trợ thông qua sản phẩm, hãy đi tới Công cụ hỗ trợ trang web trở xuống **Công cụ hỗ trợ (WSDIAG) cho Windows**, lựa chọn **Tải xuống** và lưu `wsdiag_standalone.exe` tập tin, ví dụ như trong thư mục Tải xuống của bạn. Bấm đúp vào tập tin để chạy công cụ.

12.3 Gỡ lỗi các vấn đề về sản phẩm

Ghi nhật ký gỡ lỗi giúp bộ phận hỗ trợ khách hàng của chúng tôi phân tích và giải quyết các vấn đề, nếu có, trong sản phẩm.

Bạn có thể tạm thời cấp cho bộ phận hỗ trợ khách hàng của chúng tôi quyền cụ thể để phân tích các vấn đề trong sản phẩm. Lưu ý rằng thông tin được thu thập bằng cách ghi nhật ký gỡ lỗi có thể được coi là nhạy cảm.

WebView2 là một công nghệ được sử dụng để nhúng nội dung web vào các ứng dụng gốc. Ví dụ: trang đăng nhập tài khoản của chúng tôi sử dụng công nghệ WebView2.

Nếu bạn gặp khó khăn với các chế độ xem web được nhúng, trình gỡ lỗi bảng điều khiển WebView2 có thể giúp bộ phận hỗ trợ khách hàng của chúng tôi phân tích các vấn đề về chế độ xem web cho bạn.

Để cấp cho bộ phận hỗ trợ của chúng tôi quyền tạm thời để gỡ lỗi các vấn đề về sản phẩm:

Lưu ý: Chỉ bật **Gỡ lỗi đăng nhập** khi nhân viên hỗ trợ khách hàng của chúng tôi yêu cầu bạn làm như vậy.

1. Mở Bảo mật Máy khách của WithSecure từ menu **Bắt đầu** của Windows.
2. Trên trang chính, chọn ⚙.
3. Chọn **Cài đặt Sửa**.

   Lưu ý: Bạn cần quyền quản trị để thay đổi cài đặt.

4. Ở dưới **Công cụ**, chọn công tắc chuyển đổi để bật **Gỡ lỗi đăng nhập**.
   Sau khi bật ghi nhật ký gỡ lỗi, tùy chọn **Trình gỡ lỗi bảng điều khiển WebView2** trở nên hiển thị.
5. Nếu bạn muốn bật **Trình gỡ lỗi bảng điều khiển WebView2**, hãy chọn công tắc chuyển đổi.
   Khi bạn vào chế độ xem web được nhúng, cửa sổ bảng điều khiển sẽ mở ra.
6. Ngay sau khi bộ phận hỗ trợ khách hàng của chúng tôi hoàn tất việc phân tích vấn đề, hãy tắt **Gỡ lỗi đăng nhập** bằng cách chọn nút chuyển đổi.

12.4 L□a □□o qua □i□n tho□i và ph□i làm gì n□u b□n cho r□ng mình là m□c tiêu

Không may là lừa đảo qua điện thoại đang gia tăng với những kẻ lừa đảo sử dụng kỹ thuật xã hội để nhắm mục tiêu nạn nhân của chúng.

Chủ đề này là để giúp bạn xác định những cuộc gọi này và trong trường hợp xấu nhất - nếu bạn đã được nhắm mục tiêu - cung cấp cho bạn một số thông tin về những việc cần làm tiếp theo.

L□a □□o qua □i□n tho□i là gì?

Cuộc gọi điện thoại có thể bắt đầu dưới dạng cuộc gọi lạnh hoặc thông qua quảng cáo hoặc liên kết kích hoạt cửa sổ bật lên trên máy tính của bạn. Sau đó, những cửa sổ bật lên này thúc giục bạn gọi đến số hỗ trợ kỹ thuật được quảng cáo; cửa sổ bật lên có thể xuất hiện đột ngột và không dễ dàng để loại bỏ.

Làm th□ nào tôi có th□ nh□n ra m□t trò l□a □□o qua □i□n tho□i?

Những loại cuộc gọi này thường tuân theo một mô hình nhất định: Những kẻ lừa đảo thường cho rằng máy tính của bạn có vấn đề, giả sử là vi-rút - trong khi nó thực sự không xảy ra - và sau đó chúng lừa bạn trả tiền cho một dịch vụ không tồn tại. Họ khiến bạn mất cảnh giác và chơi theo cảm xúc của bạn. Đây là tình huống cơ bản:

- Những kẻ lừa đảo qua điện thoại tuyên bố đến từ một công ty nổi tiếng, chẳng hạn như Microsoft, ngân hàng của bạn hoặc thậm chí là nhà điều hành mạng của bạn. Khi họ sử dụng một cái tên có uy tín, điều này giúp bạn cảm thấy thoải mái hơn. Họ cũng có vẻ hiểu biết và sử dụng các thuật ngữ kỹ thuật, khiến chúng có vẻ hợp pháp và đáng tin cậy.
- Vì nguy cơ có vẻ có thật và bạn cảm thấy lo lắng về khả năng có thể có vi-rút máy tính, bạn đã cho những kẻ lừa đảo truy cập vào máy tính của mình. Họ thuyết phục bạn để họ cài đặt một ứng dụng cho phép họ truy cập vào máy tính của bạn bằng các công cụ truy cập từ xa.
- Khi những kẻ lừa đảo có quyền truy cập vào máy tính của bạn, chúng sẽ giả vờ sửa vi-rút và cũng có thể yêu cầu thông tin đăng nhập cá nhân của bạn. Khi những kẻ lừa đảo đã "khắc phục" vấn đề, chúng sẽ yêu cầu bạn đăng nhập vào ngân hàng trực tuyến của mình hoặc yêu cầu bạn điền vào biểu mẫu có thông tin chi tiết về thẻ tín dụng của bạn. Những kẻ lừa đảo tính phí bạn cho dịch vụ không có thật, kết quả là nhiều hơn bạn tưởng. Trên thực tế, rất khó để biết họ thực sự tính phí bạn là bao nhiêu.

Ph□i làm gì n□u b□n ngh□ r□ng b□n □ã b□ l□a

Nếu bạn cho rằng mình đang bị lừa đảo và bạn nhận ra tình huống mà chúng tôi đã mô tả ở trên, hãy làm như sau:

- Hành động không chậm trễ.
- Liên hệ ngay với công ty phát hành thẻ tín dụng hoặc ngân hàng của bạn, báo cáo hành vi lừa đảo và hủy bất kỳ ngân hàng hoặc thẻ tín dụng nào. Nếu bạn hành động kịp thời, họ thậm chí có thể dừng giao dịch và đảo ngược các khoản phí.
- Báo cáo lừa đảo cho cơ quan thích hợp.
- Thay đổi tất cả mật khẩu của bạn trên mọi trang web hoặc dịch vụ mà bạn cho rằng có thể đã bị ảnh hưởng.
- Gỡ cài đặt bất kỳ phần mềm bên thứ ba, không xác định nào.
- Quét toàn bộ máy tính của bạn: Mở sản phẩm bảo mật của bạn, sau đó chọn **Vi rút & Đe doạ** > **Quét toàn bộ máy tính**.

Nh□ng □i□u c□n nh□ v□ các cu□c g□i □i□n tho□i không mong mu□n

- Nếu bạn nhận được cuộc gọi kiểu này, hãy nghĩ: tôi đã yêu cầu cái này chưa?

  👉 **Lưu ý:** Thông thường, bộ phận hỗ trợ khách hàng sẽ gọi cho bạn nếu bạn đã liên hệ với họ và tạo phiếu hỗ trợ.

- Các phiên từ xa thường được sử dụng trong hỗ trợ kỹ thuật như một cách để hỗ trợ bạn giải quyết các vấn đề.

  👉 **Ghi nhớ:** Chỉ cho phép các phiên từ xa với những người hoặc công ty bạn biết và tin tưởng. Chỉ cho phép các phiên từ xa nếu bạn đã liên hệ trước với nhà cung cấp dịch vụ của mình và có trường hợp hỗ trợ hợp lệ với họ. Ngoài ra, hãy bảo vệ dữ liệu truy cập từ xa của bạn như bạn sẽ bảo vệ bất kỳ mật khẩu nào khác.

- Không bao giờ cấp quyền truy cập vào thiết bị của bạn cho những người bạn không biết. Việc cấp cho những kẻ lừa đảo quyền truy cập từ xa có nghĩa là bạn giao quyền quản trị cho máy tính của mình. Ngay cả khi bạn đã cài đặt phần mềm chống vi-rút, phần mềm này không còn có thể bảo vệ bạn vì những kẻ lừa đảo chiếm quyền kiểm soát máy tính của bạn.
- Microsoft đã thông báo cho người dùng của mình rằng họ không bao giờ đưa số điện thoại vào thông báo lỗi hoặc thông báo cảnh báo phần mềm của họ.
- Không bao giờ tự do chuyển giao bất kỳ thông tin cá nhân hoặc chi tiết thẻ tín dụng.
- Kết thúc cuộc gọi ngay lập tức.
- Những cuộc gọi điện thoại kiểu này là bất hợp pháp và khi có nghi ngờ, hãy chuyển đến cơ quan có liên quan để xử lý hành vi gian lận và báo cáo.

S□n ph□m b□o m□t có th□ tr□ giúp nh□ th□ nào?

Với sản phẩm bảo mật được cài đặt, máy tính của bạn sẽ được bảo vệ khỏi vi rút, trojan và phần mềm tống tiền. Các tính năng Bảo vệ Duyệt, Bảo vệ ngân hàng và Bảo vệ công cụ truy cập từ xa cũng bổ sung thêm một lớp bảo vệ khác và đảm bảo rằng bạn có thể duyệt và thực hiện ngân hàng trực tuyến của mình một cách an toàn.

Nếu bạn đã được nhắm mục tiêu và bạn đã cài đặt sản phẩm bảo mật, bạn có thể ngay lập tức chạy quét toàn bộ máy tính để giúp phát hiện bất kỳ ứng dụng nào có thể đã được cài đặt bởi những kẻ lừa đảo; chúng được gọi là Ứng dụng Không mong muốn Tiềm ẩn (PUA). Tuy nhiên, sản phẩm không thể bảo vệ bạn khỏi những kiểu lừa đảo qua điện thoại này.

Hãy cảnh giác và giữ an toàn.