



Australian Government



SỔ TAY AN NINH MẠNG DÀNH CHO NỮ LÃNH ĐẠO



Ministry of Gender Equality
and Family



UN Women là tổ chức của Liên hợp quốc hoạt động vì mục tiêu bình đẳng giới và trao quyền cho phụ nữ. Là tổ chức toàn cầu đi đầu về bảo vệ phụ nữ và trẻ em gái, được thành lập nhằm thúc đẩy tiến độ trong việc đáp ứng nhu cầu của phụ nữ và trẻ em gái trên toàn thế giới.

UN Women hỗ trợ các Quốc gia thành viên Liên Hợp Quốc trong việc đặt ra các tiêu chuẩn toàn cầu để đạt được bình đẳng giới, đồng thời làm việc với các Chính phủ và các tổ chức xã hội để xây dựng luật pháp, chính sách, chương trình và dịch vụ cần thiết để đảm bảo các tiêu chuẩn được thực hiện hiệu quả và thực sự mang lại lợi ích cho phụ nữ và trẻ em gái trên toàn thế giới.

UN Women hoạt động trên toàn cầu nhằm hiện thực hóa tầm nhìn của các Mục tiêu Phát triển Bền vững đối với phụ nữ và trẻ em gái và ủng hộ sự tham gia bình đẳng của phụ nữ trong tất cả các khía cạnh của đời sống, tập trung vào bốn ưu tiên chiến lược: (i) Tăng cường vai trò lãnh đạo, sự tham gia của phụ nữ và thụ hưởng bình đẳng từ các hệ thống quản trị; (ii) Phụ nữ có thu nhập, công việc ổn định và tự chủ về kinh tế; (iii) Tất cả phụ nữ và trẻ em gái có một cuộc sống không có hình thức bạo lực; (vi) Nâng cao đóng góp và ảnh hưởng của phụ nữ và trẻ em gái trong việc xây dựng hòa bình bền vững, khả năng chống chịu, đồng thời được hưởng lợi bình đẳng từ việc phòng chống thiên tai và xung đột, cũng như các hoạt

động nhân đạo. UN Women đồng thời cũng điều phối việc thúc đẩy bình đẳng giới trong hệ thống Liên Hợp Quốc.

Thông báo Bản quyền

UN Women giữ quyền sở hữu trí tuệ (bao gồm cả bản quyền) đối với tất cả các sản phẩm do UN Women sản xuất, trực tiếp hoặc thông qua bên thứ ba, bao gồm nhân viên, chuyên gia tư vấn được thuê và các nhà cung cấp dịch vụ khác. Điều này có nghĩa là bản quyền của tất cả các sản phẩm nội dung và thông tin được sản xuất cho UN Women luôn thuộc về UN Women.

Thông báo bản quyền bao gồm ký hiệu bản quyền với năm xuất bản, tên UN Women và văn bản cấp phép, theo sau là số ISBN (nếu có). Văn bản bản quyền cũng có thể được bao gồm trong phần bên trong của bìa sau, mặc dù điều này ít phổ biến hơn. Thông tin bản quyền phải được đưa vào các ấn phẩm và trang web hướng ra bên ngoài như sau:

© 2023 UN Women. Đã đăng ký bản quyền.

Từ chối trách nhiệm

Các quan điểm thể hiện trong ấn phẩm này là quan điểm của các tác giả và không nhất thiết đại diện cho quan điểm của UN Women, của Liên Hợp Quốc hay của bất cứ tổ chức nào khác trực thuộc Liên Hợp Quốc.

MỤC LỤC

I. Lời nói đầu	8
II. Dẫn nhập	11
III. Nhận thức nguy cơ.....	15
1. An toàn an ninh mạng là gì?	15
2. Tình hình an ninh mạng của Việt Nam.....	17
3. Các cân nhắc về giới đối với An ninh mạng.....	19
4. Cảnh báo một số xu thế tấn công mạng trong thời gian tới.....	24
5. Nguyên lý của việc tấn công trên môi trường mạng	35
5.1. Lỗ hổng bảo mật	36
5.2. Các dạng tấn công thường gặp.....	37
IV. Phòng chống nguy cơ.....	53
1. Xác định nguy cơ	54
1.1. Lây nhiễm từ các thiết bị lưu trữ di động	54
1.2. Lây nhiễm qua email hoặc ứng dụng chat trên mạng xã hội.....	55
1.3. Lây nhiễm mã độc macro trên Office	56
1.4. Mã độc được gắn kèm trên phần mềm khác	57
1.5. Truy cập vào các trang web không an toàn.....	57
2. Phòng ngừa ở mức độ cá nhân người dùng.....	58
2.1. Bảo vệ bằng mật khẩu.....	58
2.2. Xác minh hai bước.....	59
2.3. Dùng các phần mềm Antivirus	61
2.4. Dùng tường lửa (Firewall).....	64
3. Phòng ngừa ở mức độ công ty, doanh nghiệp	66
3.1. Cần có người phụ trách an ninh thông tin.....	67
3.2. Những mối đe dọa nội bộ	67
3.3. Quy định với người lao động.....	69
3.4. Sử dụng dịch vụ An ninh mạng của doanh nghiệp	73

V. Phát hiện nguy cơ	74
1. Mã độc tống tiền.....	75
2. Tấn công phá hoại dữ liệu	77
3. Những dấu hiệu mơ hồ	78
VI. Ứng phó sự cố	81
1. Hãy bình tĩnh, suy nghĩ và hành động.....	81
2. Hãy tìm một chuyên gia	82
3. Trả tiền chuộc.....	83
4. Rút kinh nghiệm cho tương lai.....	85
VII. Khôi phục hệ thống	85
1. Khôi phục lại thiết bị khi không có trợ giúp của chuyên gia.....	86
1.1. Bước 1: Tìm hiểu điều gì đã hoặc đang xảy ra	86
1.2. Bước 2: Ngăn chặn cuộc tấn công	87
1.3. Bước 3: Chấm dứt và loại bỏ cuộc tấn công.....	88
2. Cách xử lý thông tin bị đánh cắp.....	97
VIII. Tổng kết	100
IX. Phụ lục	102
1. Pháp luật của Việt Nam về an toàn thông tin, an ninh mạng.....	102
1.1. Luật An toàn thông tin mạng	103
1.2. Luật An ninh mạng	105
2. Những địa chỉ đào tạo và cung cấp nguồn nhân lực về an ninh mạng	107
3. Mạng lưới nhà cung cấp dịch vụ an ninh mạng / cung cấp dịch vụ phòng vệ và bảo mật hệ thống mạng tại Việt Nam	110
4. Hướng dẫn sử dụng phần mềm Windows Security	117
4.1. Khởi động chương trình.....	118
4.2. Các tính năng của Windows Security	119
4.3. Thiết lập các tính năng chống virus và các mối đe dọa	121
4.4. Quản lý tường lửa và bảo mật mạng.....	127
X. Danh mục tài liệu tham khảo	132

DANH MỤC HÌNH VẼ

Hình 1. Quy trình xử lý an toàn thông tin	12
Hình 2. Khác biệt giữa an toàn thông tin và an ninh mạng	16
Hình 3. Mô hình kiểu tấn công người đứng giữa	45
Hình 4. Tấn công cướp trình duyệt Pharming dạng 1	52
Hình 5. Mô phỏng các bước tấn công của Pharming dạng 2.....	53
Hình 6. Ví dụ một thông báo lừa đảo của tin tặc trên Excel	57
Hình 7. Giao diện trang web hỗ trợ tạo mật khẩu ngẫu nhiên.....	59
Hình 8. Khóa bảo mật cho tính năng xác minh hai bước	61
Hình 9. Tính năng Firewall	65
Hình 10. Dữ liệu bị mã hóa khi máy tính bị nhiễm Ransomware	76
Hình 11. Thông báo tổng tiền của tin tặc trên thiết bị nhiễm Ransomware.....	76
Hình 12. Cách khởi động ứng dụng Windows Security	91
Hình 13. Giao diện của ứng dụng Windows Security	92
Hình 14. Cách để tìm lựa chọn quét virus	92
Hình 15. Cách thiết lập lại trang nhà trên trình duyệt Chrome	96
Hình 16. Cửa sổ giao diện Windows Security.....	119
Hình 17. Giao diện phần Virus & threat protection.....	121
Hình 18. Giao diện phần Firewall & network protection	127

DANH MỤC TỪ VIẾT TẮT

UN Women	Cơ quan Liên hợp quốc về Bình đẳng giới và trao quyền cho phụ nữ
VWEC	Hội đồng Doanh nhân nữ Việt Nam
AI	Trí tuệ nhân tạo
APT	Tấn công có chủ đích
ATM	Máy giao dịch ngân hàng tự động
ATTT	An toàn thông tin
CNTT (IT)	Công nghệ thông tin
CSDL	Cơ sở dữ liệu
CD/DVD	Đĩa CD, DVD
DNNVV	Doanh nghiệp nhỏ và vừa
DDoS	Tấn công từ chối dịch vụ phân tán
DNS	Hệ thống tên miền
DoS	Tấn công từ chối dịch vụ
IoT	Internet vạn vật
OGBV	Bạo lực trên cơ sở giới trực tuyến
PIN	Số nhận dạng cá nhân
USB	Chuẩn phối ghép USB

I. Lời nói đầu

Trong thời đại công nghệ thông tin bùng nổ như hiện nay, kinh doanh online đang dần trở thành một xu hướng được rất nhiều cá nhân, doanh nghiệp coi trọng. Không chỉ giúp mở rộng phạm vi quảng bá, làm sâu và rộng hơn các biện pháp truyền thông cho các doanh nghiệp trong và ngoài nước, giảm chi phí vận hành, kết nối với các nhà cung cấp với chi phí thấp mà Mạng và công nghệ thông tin còn là những yếu tố quan trọng thúc đẩy sự phát triển của các doanh nghiệp nhỏ và vừa (DNNVV). Tuy nhiên bên cạnh những cơ hội, môi trường “mạng” – “Mạng” cũng đồng thời mang đến những rủi ro và thách thức vô cùng to lớn cho cá nhân người dùng cũng như các doanh nghiệp nói chung và doanh nghiệp do phụ nữ làm chủ nói riêng trong việc bảo đảm an toàn thông tin. Ngày càng có nhiều các cuộc tấn công mạng tinh vi có tổ chức với quy mô lớn hướng đến các doanh nghiệp và các tập đoàn lớn trong khi nhận thức về an ninh mạng của người dùng ở Việt Nam vẫn còn rất hạn chế. Nhiều công ty vẫn chỉ áp dụng các giải pháp đảm bảo an toàn thông tin mạng truyền thống, công nghệ không được cập nhật và chỉ khi bị tấn công mới thuê nhân lực để sửa chữa, phục hồi.

Tại Việt Nam, số DNNVV do phụ nữ làm chủ chiếm hơn 20% tổng số DNNVV cả nước, tuy nhiên bằng sự nhạy bén, linh hoạt nhưng cũng không kém phần quyết liệt, các lãnh đạo nữ đã thể hiện

bản lĩnh trong việc lãnh đạo doanh nghiệp. Đặc biệt, trong giai đoạn phục hồi kinh tế hiện nay, các nữ doanh nhân đang trở thành những người truyền năng lượng tích cực cho tổ chức, đưa doanh nghiệp vượt qua khó khăn, phát triển ổn định. Mặc dù đã khẳng định được vai trò của mình trong nền kinh tế nhưng thực tế, các DNNVV do nữ làm chủ đang gặp rất nhiều khó khăn và rào cản cả về tài chính và phi tài chính.

Với sự hỗ trợ của dự án “*Hỗ trợ doanh nghiệp do nữ làm chủ, hiệp hội, hội, câu lạc bộ doanh nhân nữ sử dụng và khai thác thông tin, dữ liệu an toàn trên không gian mạng*” của Cơ quan Liên hợp quốc về Bình đẳng giới và trao quyền cho phụ nữ (UNWOMEN) trong khuôn khổ chương trình khu vực “*Phụ nữ, Hòa bình và An ninh mạng: Thúc đẩy Hòa bình và An ninh của Phụ nữ trong Thế giới số*”, Hội đồng Doanh nhân nữ Việt Nam (VWEC) cùng nhóm chuyên gia đã xây dựng cuốn “*Sổ tay An ninh mạng dành cho nữ lãnh đạo*” với mong muốn cung cấp cho doanh nhân nữ, nữ lãnh đạo doanh nghiệp/tổ chức những hiểu biết nhất định về vấn đề an toàn an ninh mạng khi tham gia trên môi trường Mạng, cách phòng tránh, cách nhận biết nguy cơ bị tấn công cũng như những biện pháp cần thực hiện sau khi bị tấn công mạng. Chúng tôi hy vọng sẽ giúp được đa số người dùng Mạng tránh được những nguy cơ tiềm ẩn đằng sau những cú click chuột tưởng chừng như vô hại trên môi trường mạng.

Chúng tôi xin gửi lời cảm ơn chân thành tới các chuyên gia tư vấn – TS. Lê Quang Minh, Phó Viện trưởng Viện Công nghệ thông tin, Đại học Quốc gia Hà Nội, trưởng nhóm tư vấn; ThS. Nguyễn Thị Ngọc Hân, Phòng An toàn Hệ thống thông tin, Viện Công nghệ thông tin và các chuyên gia đã đồng hành cùng VWEC và UN Women để hoàn thành cuốn sổ tay này.

Cuối cùng, chúng tôi xin gửi lời cảm ơn chân thành tới Chính phủ Australia và Bộ Ngoại giao Australia vì đã hỗ trợ cho UN Women và dự án “*Phụ nữ, Hòa bình và an ninh mạng: Thúc đẩy Hòa bình và An ninh của Phụ nữ trong Thế giới số*” trong việc xây dựng cuốn sổ tay này.

Xin trân trọng cảm ơn!

II. Dẫn nhập

Một câu hỏi đang được đặt ra: bạn cần nâng cao khả năng tự bảo vệ của bản thân như thế nào để trở nên an toàn hơn trong môi trường Mạng?

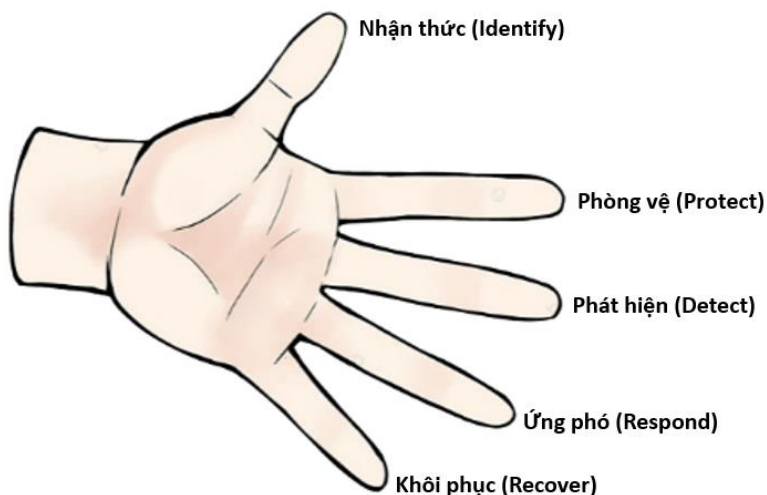
Câu trả lời chỉ có thể là

- **tăng nhận thức,**
- **biết cách phòng và chống các nguy cơ bị tấn công,**
- **phát hiện nhanh khi bị tấn công,**
- **sau đó là xử lý sự cố và**
- **giảm tác hại do bị tấn công Mạng nhỏ nhất có thể.**

Cuốn sổ tay này sẽ giúp bạn làm được điều đó qua một chu trình dẫn dắt người đọc tự tìm hiểu, đánh giá và xác định biện pháp phòng bị, tự vệ và phản công khi muốn tự vệ khỏi những nguy cơ bị tấn công hay xâm phạm trên mạng. Cuốn sổ tay sẽ trình bày làm 5 phần:

- **Identify** - nhận thức nguy cơ. (Mục III)
- **Protect** - Phòng chống nguy cơ.
- **Detect** - phát hiện sự cố.
- **Respond** - ứng phó sự cố.
- **Recover** - phục hồi hệ thống.

trung ứng với 5 ngón trong hình bàn tay dưới đây:



Hình 1. Quy trình xử lý an toàn thông tin

Ngón tay thứ nhất: vấn đề Identify (nhận thức nguy cơ) – chúng tôi đặt ở ngón tay cái, ngón tay quan trọng nhất. Chúng tôi muốn đề cập đến những hiểu biết về an toàn thông tin. Người đọc cần biết rằng môi trường Mạng không chỉ chứa vô vàn những kho tàng thông tin thú vị, nhiều điều mới lạ tha hồ khám phá mà còn đầy rẫy những cạm bẫy, những nguy hiểm rình rập ngay cạnh họ. Đó là những vụ lừa đảo trên mạng xã hội; những thông tin xấu, độc, sai sự thật; những vụ mạo danh, lừa đảo, xâm hại, lấy cắp thông tin cá nhân, xâm phạm quyền riêng tư, v.v.

Không phải người dùng Mạng nào cũng biết về các nguy hiểm trên mạng. Theo thống kê của Kaspersky năm 2020 thì gần 40% người dùng Mạng tại Đông Nam Á không quan tâm đến **bảo mật mạng**. Điều này cho thấy việc nhận thức được nguy cơ về an ninh mạng là vô cùng cần thiết.

Người dùng Mạng cần phải có kiến thức để nhận biết là có nguy cơ hay không, và phải tự nhận rõ nguy cơ mất an toàn Mạng và rủi ro bị xâm phạm thông tin cá nhân hay của công ty/tổ chức, thì mới chuẩn bị các biện pháp để phòng tránh. Nếu không thì sự không đề phòng sẽ làm cho cá nhân, công ty/cơ quan sẽ bị tấn công bất cứ khi nào.

Ngón tay thứ hai: là ngón tay hành động, dùng để bóp cò khi bắn súng, ngón tay Protect – Phòng vệ. Giống như khi biết là có nguy cơ bị ăn trộm thì người ta sẽ lắp hàng rào, trong CNTT cũng vậy, khi biết là có nguy cơ mất an ninh mạng thì người dùng sẽ thiết lập các biện pháp bảo vệ. Đó sẽ là những hướng dẫn để người đọc biết để chủ động ngăn chặn những

Lưu ý: Những cách thức để bảo vệ mình trên mạng như đặt mật khẩu mạnh, sử dụng phần mềm diệt virus, không sử dụng đường truyền internet tự do, không trao cho người khác mật khẩu của mình hay của công ty/cơ quan, không tiếp cận các trang mạng không an toàn, đặt các thiết đặt tường lửa (firewall), đào tạo nhân lực đầy đủ về phòng vệ an ninh mạng, v.v.

khả năng có thể bị xâm phạm. Việc cảnh báo được thực hiện càng sớm thì sẽ càng giảm được những tổn hại, mất mát mà vụ tấn công mạng có thể gây ra. Sự ứng phó kịp thời (ngay lập tức) và hiệu quả (ngăn chặn ngay và đầy đủ) là quan trọng nhất trong việc phòng vệ an ninh Mạng.

Ngón tay thứ ba là ngón tay dài nhất của bàn tay, chúng tôi đặt nó là ngón tay với bước Detect - Phát hiện. Hệ thống bảo vệ có một tác dụng quan trọng nhất, đó là cảnh báo, là phát hiện và báo cho chủ nhân biết rằng họ đang bị tấn công trong thời gian ngắn nhất có thể.

Ngón tay thứ tư: ngón Respond - Ứng phó, nằm trên ngón đeo nhẫn, văn hóa phương tây thường gọi là ngón tay kết hôn. Ý nghĩa mà chúng tôi muốn đề cập chính là sự phối hợp khi ứng phó sự cố an toàn thông tin. Khi ứng cứu sự cố thì cần phải có sự phối hợp, khi bạn gặp sự cố hãy nghĩ đến sự phối hợp của nhiều bên (nhân viên IT của tổ chức/công ty, chuyên gia, Trung tâm Ứng cứu khẩn cấp không gian mạng (VNCERT), Bộ Công an, Bộ Quốc phòng, v.v.) để ứng phó tốt nhất sự cố vừa xảy ra.

Ngón tay út: ngón Recover – Khôi phục sau sự cố, là câu chuyện của việc phục hồi, cần làm sao để khôi phục lại hệ thống, giảm thiểu rủi ro. Ngón tay út là ngón tay nhỏ nhất, là mong muốn thiệt hại nhỏ nhất. Khôi phục sự cố, giảm thiểu rủi ro và mất mát về thông tin quan trọng của cá nhân hay của công ty/tổ chức.

Với ý tưởng về cuốn sổ tay như trên, chúng tôi hi vọng nội dung đề cập trong cuốn sổ tay sẽ cung cấp cho độc giả những thông tin đơn giản, dễ hiểu, và thiết thực để những kiến thức nhỏ này sẽ giúp bạn an toàn hơn trên không gian mạng.

III. Nhận thức nguy cơ

Đầu tiên, chúng ta cần tìm hiểu một số khái niệm về an toàn an ninh mạng, tình hình an ninh mạng của Việt Nam và những xu thế an ninh mạng trong thời gian tới.

Sau đó chúng tôi sẽ giới thiệu nguyên lý và những cách thức tin tặc thực hiện những vụ tấn công trên môi trường mạng.

1. An toàn an ninh mạng là gì?

Cybersecurity – an ninh mạng được hiểu nôm na là “*việc cá nhân hay tổ chức thực hiện các hoạt động hay thói quen để bảo vệ các hệ thống kết nối Internet như phần cứng, phần mềm và dữ liệu khỏi các mối đe dọa mạng, và để tránh hoặc chống lại việc truy cập trái phép vào trung tâm dữ liệu và các hệ thống máy tính khác của cá nhân, công ty hay tổ chức*”.

Luật An toàn thông tin mạng 2015 đã định nghĩa: “*An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng*”.

tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.”

Theo khoản 1 Điều 2 Luật An ninh mạng 2018 định nghĩa an ninh mạng như sau: "*An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.*"

Cả an toàn thông tin lẫn an ninh mạng đều nhằm mục đích bảo vệ thông tin. An toàn thông tin đề cập đến một lĩnh vực rộng lớn hơn. Ngoài việc bảo vệ dữ liệu khỏi những mối đe dọa thì nó xử lý các thông tin kỹ thuật số và thông tin tương tự. Trong khi an ninh mạng tập trung vào thông tin kỹ thuật số và giải quyết các vấn đề tội phạm mạng, tấn công mạng, gian lận mạng, thực thi pháp luật, ...



Hình 2. Khác biệt giữa an toàn thông tin và an ninh mạng

2. Tình hình an ninh mạng của Việt Nam.

Những năm qua, Việt Nam đã có nhiều chủ trương đẩy mạnh ứng dụng, phát triển công nghệ thông tin phục vụ phát triển kinh tế – xã hội, bảo đảm quốc phòng, an ninh và đã đạt được nhiều thành tựu rất quan trọng. Cơ sở hạ tầng viễn thông, công nghệ thông tin được xây dựng khá đồng bộ; hầu hết các ngành đang số hóa cơ sở dữ liệu và ứng dụng công nghệ thông tin để nâng cao hiệu quả quản lý, giảm thiểu thủ tục hành chính. Kinh tế số được hình thành và phát triển nhanh, ngày càng trở thành bộ phận quan trọng của nền kinh tế; xuất hiện nhiều hình thức kinh doanh, dịch vụ mới xuyên quốc gia, dựa trên nền tảng công nghệ số và Mạng và theo ITU, khoảng cách giới kỹ thuật số ở Việt Nam năm 2021 là 9 điểm, chỉ có 57% phụ nữ sử dụng Mạng so với 66% nam giới.

Bên cạnh những thuận lợi đã có thì Việt Nam cũng đang phải đối mặt với nhiều thách thức đối với an ninh quốc gia, trật tự an toàn xã hội đến từ không gian mạng. Đặc biệt, trong năm 2021 và đầu năm 2022, trước diễn biến phức tạp của tình hình dịch bệnh COVID-19, mọi hoạt động, tương tác, quan hệ, giao dịch của toàn xã hội chủ yếu thông qua môi trường mạng, kéo theo hoạt động sử dụng không gian mạng để thực hiện các hành vi vi phạm pháp luật tăng mạnh. Với tốc độ phát triển và ứng dụng công nghệ thông tin nhanh chóng như hiện nay, tình hình an ninh mạng của Việt Nam sẽ tiếp tục có nhiều diễn biến phức tạp, tội phạm mạng tiếp tục gia tăng, hoạt động

rộng khắp trên mọi lĩnh vực. Trong 6 tháng đầu năm 2022, Bộ Công an đã phát hiện, xử lý 840 chuyên án, vụ việc liên quan tội phạm lừa đảo, chiếm đoạt tài sản qua mạng (tăng 42% so với 6 tháng cuối năm 2021). Phụ nữ bị ảnh hưởng nhiều hơn bởi các cuộc tấn công mạng.

Trước tình hình trên, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (ANM&PCTPCNC) đã tham mưu với Đảng, Nhà nước, Bộ Công an ban hành, triển khai thực hiện nhiều chủ trương, chính sách, pháp luật và các giải pháp kịp thời về bảo đảm an ninh

mạng, phòng, chống tội phạm sử dụng công nghệ cao, nhất là khẩn trương xây dựng, đề xuất ban hành các văn bản hướng dẫn thi hành Luật An ninh mạng, các quy định về bảo vệ dữ liệu cá nhân, xử phạt vi phạm hành chính trên lĩnh vực an ninh mạng. Đồng thời tiếp tục rà soát những vấn đề mới đang đặt ra trong cuộc Cách mạng công nghiệp lần thứ tư để đề xuất hoàn thiện hệ thống chính sách, pháp luật đảm bảo phù hợp với các chuẩn mực quốc tế, quyền của người dùng, cũng như các cam kết về nhân quyền.

Lưu ý: Tội phạm mạng phổ biến nhất đối với phụ nữ có thể gồm:

- tống tiền trên mạng, đe dọa,
- khiêu dâm trên mạng,
- đăng và xuất bản nội dung khiêu dâm tục tĩu,
- theo dõi,
- bắt nạt,
- phi báng,
- biến hình và thiết lập hồ sơ giả mạo.

Việc chủ động, tích cực tham gia cuộc Cách mạng công nghiệp lần thứ tư và chuyển đổi số quốc gia là yêu cầu tất yếu khách quan nhằm mang lại cơ hội cho phát triển kinh tế – xã hội, đồng thời giải quyết hiệu quả những thách thức về an ninh quốc gia, trật tự an toàn xã hội của đất nước. Mặc dù phụ nữ có nguy cơ rủi ro trên mạng chiếm tỷ lệ cao, nhưng điều quan trọng là phải đưa ra các biện pháp bảo vệ phù hợp để đảm bảo rằng phụ nữ không bị bỏ lại phía sau trong quá trình phát triển này.

Nhìn nhận đúng đắn những nguy cơ, thách thức từ không gian mạng sẽ giúp chúng ta chủ động bảo vệ quyền và lợi ích hợp pháp khi tham gia vào không gian số, xã hội số.

3. Các cân nhắc về giới đối với an ninh mạng

Các mối đe dọa trên mạng ngày càng trở nên phức tạp khi các công nghệ và ứng dụng được sử dụng bởi các tổ chức và nhân viên của họ đã phát triển vượt bậc. Trong bối cảnh này, các tác nhân đe dọa (những người có khả năng tài chính cao hoặc có nhu cầu cần thông tin cao) đang sử dụng các công cụ tinh vi (ví dụ: Trí tuệ nhân tạo – artificial intelligence) để nhắm mục tiêu vào nhiều loại thiết bị, hệ thống và ứng dụng - nghĩa là bối cảnh mối đe dọa liên tục thay đổi. Sự phát triển nhanh chóng này về cả công nghệ và phương tiện để phá hoại chúng khiến cho các mối đe dọa mới khó bị phát hiện và ngăn chặn, do đó khiến các tác nhân đe dọa khai thác lỗ hổng dễ dàng hơn và người dân khó duy trì an ninh hơn.

Cách thức mà nam giới và phụ nữ bị tấn công trên mạng khác nhau trong lĩnh vực an ninh mạng bởi nhiều nguyên nhân và đôi khi rủi ro mạng họ trải nghiệm cũng khác nhau theo giới. Theo một nghiên cứu do UN Women thực hiện đã cho thấy:

- Phụ nữ và trẻ em gái là đối tượng bị tấn công nhiều hơn bởi ngôn từ kích động thù địch, bạo lực trên cơ sở giới trực tuyến (OGBV) cũng như lạm dụng tình dục trực tuyến và một số tội phạm mạng, đôi khi bị kẻ thù hay đối thủ của họ thực hiện quy trình bạo lực một cách có hệ thống để làm mất uy tín và mất tiếng nói của họ.
- Phụ nữ ít có khả năng tiếp cận các công cụ và tài nguyên kỹ thuật số hơn nam giới cũng như ít có khả năng được tuyển dụng hoặc đào tạo trong các lĩnh vực kỹ thuật, điều này có thể hạn chế khả năng của họ trong việc triển khai các biện pháp an toàn và an ninh mạng hiệu quả.
- Phụ nữ cũng có thể gặp khó khăn hơn khi tìm kiếm sự trợ giúp kỹ thuật hoặc hỗ trợ về các vấn đề an ninh mạng vì họ có thể phải đối mặt với sự phân biệt đối xử hoặc thiên vị.

Nghiên cứu về các mối quan ngại về an ninh mạng đối với phụ nữ và các tổ chức do phụ nữ lãnh đạo cho thấy các lỗ hổng an ninh mạng theo giới chủ yếu có khả năng bị ảnh hưởng bởi:

- a. **Thiếu kiến thức kỹ thuật số và kỹ năng kỹ thuật:** Phụ nữ có thể không có cùng trình độ chuyên môn kỹ thuật như đối thủ của họ do các chuẩn mực phân biệt đối xử về giới, khiến họ dễ bị tấn công mạng hơn như lừa đảo hoặc phần mềm độc hại.
- b. **Bảo vệ về mặt pháp lý chưa đầy đủ:** Nhiều quốc gia thiếu khung pháp lý đáp ứng giới để giải quyết bạo lực và quấy rối trên mạng, khiến phụ nữ không có quyền truy cứu thích đáng khi họ là mục tiêu tấn công.
- c. **Chuẩn mực xã hội và văn hóa:** Phụ nữ có thể phải đối mặt với các rào cản văn hóa và xã hội trong việc tiếp cận công nghệ hoặc phát biểu trực tuyến, điều này có thể hạn chế khả năng tham gia vào các cuộc tranh luận công khai và khiến họ dễ bị tấn công mạng hơn.
- d. **Phân biệt đối xử:** Phụ nữ thuộc nhiều nhóm bị thiệt thòi (chẳng hạn như phụ nữ LGBTQ+, phụ nữ khuyết tật, phụ nữ thuộc các nhóm tuổi khác nhau hoặc phụ nữ thuộc các nhóm dân tộc thiểu số hoặc tôn giáo) có thể phải đối mặt với sự phân biệt đối xử phức tạp và dễ bị tổn thương trong lĩnh vực kỹ thuật số.
- e. **Việc sử dụng phần mềm của bên thứ ba hoặc phần mềm không có giấy phép:** Các tổ chức có thể sử dụng phần mềm hoặc dịch vụ của bên thứ ba có chứa lỗ hổng bảo mật mà kẻ tấn công có thể khai thác, đặc biệt khi trình độ kỹ thuật số và

nhận thức về những vấn đề này còn thấp. Điều này có thể làm tổn hại đến tính bảo mật của dữ liệu và hoạt động của tổ chức.

- f. **Các chính sách và thủ tục xử lý vi phạm không phù hợp:** Các tổ chức có thể thiếu các chính sách và thủ tục rõ ràng để giải quyết các rủi ro mạng (và đặc biệt là cách thức mà nam giới và phụ nữ được đối xử hoặc cư xử khác nhau) khiến họ dễ bị tấn công hoặc vi phạm dữ liệu.
- g. **Một số chủ thể phi nhà nước chống phá:** Các chủ thể phi nhà nước như các nhóm cực đoan hoặc mạng lưới tội phạm có tổ chức có thể sử dụng các lỗ hổng này để tấn công hoặc quấy rối trên mạng nhắm vào phụ nữ.

Văn phòng UN Women khu vực Châu Á và Thái Bình Dương đã tiến hành nghiên cứu về các rủi ro an ninh mạng theo giới trên khắp Đông Nam Á trong giai đoạn 2022-2023. Những hành động đe dọa nhất được xác định bởi những người tham gia nghiên cứu là vi phạm dữ liệu, phần mềm gián điệp và vi rút. Nghiên cứu cho thấy rằng phụ nữ có thể là mục tiêu trọng yếu của các cuộc tấn công đó vì họ có thể không có quyền tiếp cận tới các công cụ và nguồn lực/hệ thống giúp tăng cường khả năng tự vệ và phục hồi thông tin và mạng. Trong khi các đối thủ có thể nhắm mục tiêu cụ thể vào các tổ chức ủng hộ bình đẳng giới và quyền của phụ nữ.

Nghiên cứu cũng cho thấy rằng nhìn chung, các nữ lãnh đạo ở một số tổ chức xã hội có thể có mức độ nhận thức về mối đe dọa an ninh mạng cao, cho thấy họ đã từng trải nghiệm về những rủi ro do các sự cố an ninh mạng gây ra cho cá nhân hoặc tổ chức của họ. Mặc dù vẫn cần có các sáng kiến nâng cao nhận thức, nhưng những phát hiện này cho thấy cần tập trung nhiều hơn vào các công cụ và nguồn lực giúp phụ nữ và các công ty/tổ chức của họ ngăn chặn và giảm thiểu tác động của các cuộc tấn công mạng và những tác hại mà chúng gây ra.

Vi phạm dữ liệu do hack dữ liệu và các hành vi ác ý khác cũng có thể gây ra nhiều tác động bất lợi hơn đối với phụ nữ vì điều này có thể làm trầm trọng thêm vấn đề bạo lực trên cơ sở giới trực tuyến (OGBV), chẳng hạn như việc lan truyền hình ảnh khiêu dâm và dữ liệu cá nhân của họ mà không được phép, hay doxing (Thông tin cá nhân này có thể bao gồm tên, địa chỉ, số điện thoại, thông tin về gia đình, v.v. xâm phạm quyền riêng tư, gây hại, hoặc đe dọa người bị doxx.)

Trên cơ sở đó, UN Women Việt Nam đã hợp tác với Hội đồng Doanh nhân nữ Việt Nam xây dựng một cuốn sổ tay nhằm đưa ra các khuyến nghị cụ thể cho phụ nữ Việt Nam nhằm tăng cường khả năng phục hồi mạng và an ninh kỹ thuật số cũng như mở rộng cơ hội cho phụ nữ tham gia vận động chính sách để đảm bảo rằng các luật và khung chính sách liên quan có tính đến giới.

4. Cảnh báo một số xu thế tấn công mạng trong thời gian tới.

Hiện tại đang có một số xu thế tấn công mạng đã, đang và sẽ xảy ra như sau:

4.1 Tin tặc gia tăng hoạt động tấn công có chủ đích

Tin tặc gia tăng hoạt động tấn công có chủ đích (APT) nhằm chiếm quyền điều khiển; tấn công DDoS; tấn công bằng mã độc, nhất là mã độc tống tiền nhằm vào các hệ thống thông tin trọng yếu. Mục tiêu tấn công là các cơ quan, ban ngành, tập đoàn kinh tế lớn, trọng yếu, nhằm đánh cắp dữ liệu cá nhân, dữ liệu khách hàng, thông tin tài liệu bí mật Nhà nước... Phụ nữ đặc biệt gặp rủi ro khi bị rò rỉ dữ liệu, vì dữ liệu bị rò rỉ có thể được sử dụng để tạo điều kiện cho bạo lực trên cơ sở giới trực tuyến (OGBV) và quấy rối trực tuyến, điều này có thể khiến họ nản lòng và mất uy tín để tiếp tục công việc và tham gia các hoạt động công khai.

4.2 Chiếm đoạt tài khoản

Đôi khi những kẻ tấn công không muốn làm gián đoạn hoạt động bình thường của nạn nhân mà thay vào đó tìm cách khai thác các hoạt động đó để thu lợi tài chính. Chúng sẽ thao túng dữ liệu trong quá trình trao đổi giữa hai bên hoặc làm giả mạo dữ liệu nằm trên hệ thống của nạn nhân. Có hai hình thức phổ biến là:

- Chiếm quyền sử dụng các tài khoản mạng xã hội (Zalo, Facebook, Tiktok...) để tiến hành gửi tin nhắn lừa đảo cho bạn bè người thân nhằm chiếm quyền tài khoản, lấy cắp thông tin, chiếm đoạt tài sản, bôi nhọ danh dự, tống tiền...

- Các ứng dụng, quảng cáo tín dụng đen xuất hiện trên các trang web, gửi tràn lan qua các kênh thư điện tử rác, tin nhắn SMS, mạng xã hội Facebook, Telegram, Zalo. Nạn nhân sẽ biến thành những con nợ trong khi chính nạn nhân cũng không biết.

4.3 Tấn công giả mạo

Tấn công giả mạo là hình thức tấn công mạng mà kẻ tấn công giả mạo thành một đơn vị uy tín để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng. Có hai kiểu phổ biến là:

- Giả mạo thương hiệu của các Tổ chức (Ngân hàng, cơ quan nhà nước, công ty tài chính, chứng khoán...) để gửi SMS lừa đảo cho nạn nhân.
- Giả mạo các trang web/blog chính thống (giao diện, địa chỉ tên miền/đường dẫn,) tạo uy tín lừa nạn nhân, thu thập thông tin cá nhân của người dân.

Phương thức tấn công này thường được tin tặc thực hiện thông qua email và tin nhắn. Người dùng khi mở email và click vào đường link giả mạo sẽ được yêu cầu đăng nhập. Nếu “mắc câu”, tin tặc sẽ có được thông tin ngay tức khắc.

4.4 Kiểu tấn công mạo danh

Một trong những nguy cơ lớn nhất mà Internet tạo ra là rất dễ dàng để mạo danh người khác. Trước khi có Internet, tội phạm không dễ để mạo danh một ngân hàng, cửa hàng và đề nghị mọi người đưa tiền cho chúng để có được một số phần thưởng hoặc lợi ích. Gửi thư và gọi điện có thể trở thành công cụ của kẻ lừa đảo, nhưng không có công cụ truyền thông nào vừa dễ dàng mà thuận lợi

nhu mạo danh trên Internet. Chỉ cần vài phút là kẻ phạm tội có thể tạo ra một website y như website của một ngân hàng, một cửa hàng hoặc một tổ chức chính phủ thật, thậm chí chúng còn tìm được những tên miền gần giống với tên miền của website thật.

Một số điển hình của dạng tấn công này là: Deceptive phishing, Spear phishing, CEO Fraud, Pharming, Dropbox Phishing và Google docs Phishing.

4.5 Tấn công phá hủy dữ liệu

Tấn công phá hủy dữ liệu là một dạng tấn công ở mức cao hơn nữa, vì tin tặc không chỉ muốn làm tê liệt hệ thống, ngắt kết nối hệ thống của nạn nhân, chúng còn muốn phá hủy dữ liệu của họ vì một lý do nào đó – ví dụ như người dùng từ chối trả tiền chuộc mà chúng yêu cầu.

Phần mềm độc hại Wiper là một điển hình của kiểu tấn công này. Những thiệt hại tài chính có thể xảy ra cho các bên bị ảnh hưởng, nhưng mục tiêu chính của nó không phải là lấy cắp tiền hoặc bán thông tin cho tội phạm mạng, mà là sự phá hủy. Điều này có nghĩa là trừ khi nạn nhân có các bản sao lưu, còn không thì khi đã bị dính Wiper thì nạn nhân sẽ mất quyền truy cập vào tất cả dữ liệu và phần mềm đã được lưu trữ trước đó trên thiết bị bị tấn công.

4.6 Kiểu tấn công trộm cắp dữ liệu

Nhiều vụ tấn công mạng hướng đến dữ liệu của nạn nhân, có thể là cá nhân, doanh nghiệp hoặc một tổ chức chính phủ. Có 2 dạng điển hình của kiểu tấn công này: Trộm cắp dữ liệu cá nhân và Trộm cắp dữ liệu doanh nghiệp.

Tội phạm có thể sử dụng dữ liệu bị đánh cắp từ cá nhân, doanh nghiệp cho một số mục đích bất chính:

- Thực hiện các giao dịch chứng khoán: Biết trước thông tin nội bộ của doanh nghiệp sẽ cho chúng nhiều lợi thế để lũng đoạn thị trường cổ phiếu, kiếm lợi nhuận phi pháp.
- Bán dữ liệu cho các đối thủ cạnh tranh vô đạo đức: Tội phạm ăn cắp thông tin quy trình bán hàng, tài liệu về sản phẩm, định hướng thị trường tương lai hoặc các thông tin nhạy cảm khác có thể bán dữ liệu đó cho các đối thủ cạnh tranh vô đạo đức.
- Rò rỉ dữ liệu cho giới truyền thông: Dữ liệu nhạy cảm có thể khiến nạn nhân xấu hổ và khiến cổ phiếu của họ giảm giá (có thể sau khi bán không một số cổ phiếu).
- Rò rỉ dữ liệu thuộc phạm vi điều chỉnh của các quy định về quyền riêng tư: Nạn nhân có thể bị phạt tiền.
- Ăn cắp và sử dụng tài sản trí tuệ: Các bên ăn cắp mã nguồn của phần mềm máy tính có thể tránh phải trả phí cấp phép cho chủ sở hữu hợp pháp của phần mềm.

4.7 Hoạt động phát tán thông tin xấu, độc hại, thông tin sai sự thật trên không gian mạng

Hoạt động này tiếp tục tác động đến mọi mặt của đời sống xã hội, xâm phạm nghiêm trọng đến quyền, lợi ích hợp pháp của các tổ chức, cá nhân. Nội dung sai lệch về phụ nữ và thông tin sai lệch là vấn đề nghiêm trọng vì nó gây ra sự căm ghét đối với phụ nữ và công việc của họ, đồng thời cuối cùng có thể khiến họ và doanh nghiệp của họ gặp rủi ro. Trong thời gian tới, hoạt động này sẽ tiếp tục gia

tăng, đòi hỏi người dùng nâng cao cảnh giác, thận trọng khi tiếp cận với những thông tin trên không gian mạng, tránh trở thành nạn nhân của tin giả.

4.8 Tội phạm lừa đảo chiếm đoạt tài sản qua mạng

Tội phạm lừa đảo chiếm đoạt tài sản qua mạng có xu hướng gia tăng, diễn biến ngày càng phức tạp với nhiều phương thức, thủ đoạn tinh vi, có tính chất xuyên quốc gia, gây thiệt hại lớn và bức xúc trong nhân dân. Phụ nữ có thể đặc biệt gặp rủi ro trước các kiểu tấn công này vì họ ít có khả năng tìm kiếm/có xu hướng ít tiếp cận với kiến thức kỹ thuật số và đào tạo an ninh mạng hơn so với nam giới. Một số thủ đoạn của tin tặc có thể kể đến như:

- Nhắn tin, gọi điện hoặc thông qua các trang mạng xã hội để quảng cáo, giới thiệu việc làm tại nhà, tuyên giúp việc theo giờ, tuyển người giao hàng,... nhưng phải chuyển trước một khoản tiền phí nhằm lừa đảo, chiếm đoạt số tiền đặt cọc, môi giới ban đầu mà người dân chuyển cho các đối tượng;
- Sử dụng các cuộc gọi dựa trên giao thức Mạng (dịch vụ VoIP) mạo danh cán bộ trong các cơ quan thực thi pháp luật (Công an, Viện Kiểm sát, Tòa án,...) gọi điện thông báo nạn nhân bị kiện vì nợ tiền hoặc có liên quan đến vụ án đang giải quyết và yêu cầu khai báo thông tin tài khoản, mật khẩu ngân hàng trên trang thông tin giả mạo, từ đó thu thập thông tin, chiếm đoạt tiền trong tài khoản của nạn nhân;

- Thông qua hoạt động thương mại điện tử, như: Tạo lập các website, sàn giao dịch, ứng dụng kiếm tiền trên mạng, giả mạo các trang quảng cáo, rao bán các mặt hàng trực tuyến sau đó chiếm đoạt số tiền đặt cọc của khách hàng hoặc chuyển mặt hàng không đúng giá trị thực tế như quảng cáo; Giả mạo người nước ngoài mua hàng để yêu cầu người bán thực hiện “giao dịch quốc tế giả” nhằm đánh cắp thông tin, tài khoản của người bán;
- Lừa đảo thông qua hình thức kinh doanh đa cấp hoặc qua các sàn giao dịch ảo (sàn chứng khoán, vàng, ngoại tệ, bất động sản) tự lập hoặc đứng ra làm đầu mối cho sàn giao dịch nước ngoài để lôi kéo khách hàng mở tài khoản giao dịch để chiếm đoạt tiền đầu tư;
- Thực hiện hành vi tấn công mạng, chiếm quyền điều khiển tài khoản mạng xã hội để nhắn tin lừa đảo đến danh sách bạn bè; giả mạo thông tin, tài khoản, hộp thư điện tử của các công ty, doanh nghiệp, sau đó thay đổi nội dung các thư điện tử, nội dung các giao dịch, hợp đồng thương mại để chiếm đoạt tài sản; hoặc giả mạo các trang thông tin điện tử, các dịch vụ trực tuyến nhằm lấy cắp thông tin tài khoản của khách hàng để rút tiền.

4.9 Hoạt động tổ chức đánh bạc bằng trò chơi trực tuyến

Hoạt động tổ chức đánh bạc bằng trò chơi trực tuyến và đánh bạc qua hình thức đặt cược tài chính qua quyền chọn nhị phân BO...

Người chơi sẽ chọn cặp ngoại hối, tiền kỹ thuật số để đặt cược dự đoán cặp tỉ giá đó tăng hay giảm trong một đơn vị thời gian; khi đặt cược thắng, người chơi nhận về số tiền bằng số tiền cược sau khi trừ đi phí của sàn (từ 5%-10% số tiền cược), nếu thua, người chơi sẽ mất toàn bộ tiền đã đặt cược. Người chơi có thể đăng ký làm đại lý (hay còn gọi là đầu Line IB) của sàn, kêu gọi, lôi kéo người chơi mới tham gia vào sàn theo mô hình đa cấp để hưởng tiền thưởng, hoa hồng. Đây thực chất đều là hành vi tổ chức đánh bạc và đánh bạc trên không gian mạng, tiềm ẩn nguy cơ cao chiếm đoạt tài sản của người tham gia.

4.10 Hoạt động cho vay “tín dụng đen” trên không gian mạng với lãi suất cao

Hoạt động cho vay “tín dụng đen” trên không gian mạng với lãi suất cao để thu lời bất chính tiềm ẩn nhiều nguy cơ đe dọa đến an ninh trật tự tại nhiều địa phương trên cả nước. Hiện nay, trên không gian mạng có khoảng trên 200 ứng dụng cho vay trực tuyến (thông qua website, qua các ứng dụng trên GooglePlay, AppStore).

4.11 Hoạt động vi phạm pháp luật trên lĩnh vực thương mại điện tử

Hoạt động vi phạm pháp luật trên lĩnh vực thương mại điện tử tiếp tục diễn biến phức tạp, các đối tượng sử dụng mạng xã hội, sàn thương mại điện tử để rao bán hàng giả, hàng nhái, hàng lậu, vũ khí, vật liệu nổ, công cụ hỗ trợ, chất gây nghiện, giấy tờ giả; lợi dụng

hoạt động thương mại điện tử để thực hiện hành vi lừa đảo, chiếm đoạt tài sản, gây bức xúc trong xã hội.

4.12 Sự bùng nổ của các thiết bị thông minh, trí tuệ nhân tạo (AI)

Sự bùng nổ của các thiết bị thông minh, trí tuệ nhân tạo (AI), nhất là ứng dụng trên điện thoại thông minh sẽ là một mối đe dọa an ninh mạng, trật tự an toàn xã hội, do người dùng cấp quá nhiều quyền truy cập, cũng như cung cấp thông tin cá nhân trên mạng xã hội, ứng dụng, v.v. dẫn đến tình trạng bị chiếm đoạt, lợi dụng vi phạm pháp luật. Đặc biệt, mối đe dọa đến từ các thiết bị IoT vẫn là vấn đề lớn, hiện chưa có giải pháp tổng thể đảm bảo an toàn, an ninh mạng, bảo vệ bí mật nhà nước cho các thiết bị IoT, do đó nhiều vụ lộ, lọt thông tin cá nhân nhạy cảm, riêng tư, v.v. đã bị phát tán trên mạng hoặc được truy cập bởi các tác nhân khác mà không có sự đồng ý của người dùng.

Nhiều báo cáo cho thấy rằng các hệ thống AI phổ biến chứa thành kiến giới có thể tái diễn sự bất bình đẳng và các chuẩn mực phân biệt đối xử. Ví dụ, các hệ thống nhận dạng khuôn mặt và giọng nói đã được phát hiện là kém hơn trong việc nhận dạng khuôn mặt và giọng nói của phụ nữ so với nam giới. Các thuật toán trên mạng xã hội có thể gây bất lợi cho phụ nữ và các tổ chức/công ty của phụ nữ, ví dụ: những người làm việc về các vấn đề sức khỏe của phụ nữ (chẳng hạn như cho con bú) đã trải qua tình trạng cảm theo dõi vì

nội dung họ đã đăng được thuật toán AI phân loại là khiêu dâm, trong khi thực tế nội dung đó bao gồm các mô tả trung tính về cơ thể phụ nữ. Hơn nữa, ước tính chỉ có 28% lực lượng lao động AI toàn cầu là phụ nữ; trong khi nhận thức về các vấn đề giới trong AI ngày càng được nâng cao, thì vai trò lãnh đạo của phụ nữ còn thấp trong lĩnh vực này đang làm chậm tiến trình tạo ra sự thay đổi tích cực. Mặc dù, các cơ quan chức năng đã cảnh báo về nguy cơ bị chiếm đoạt thông tin, tài liệu, song người dùng lại chủ quan, thiếu kiến thức, ý thức bảo mật nên tạo điều kiện thuận lợi cho tin tặc và các đối tượng xấu tấn công, chiếm đoạt, thu thập hình ảnh, dữ liệu cá nhân sử dụng vào mục đích bất chính.

4.13 Đánh cắp mật khẩu

Tội phạm có thể đánh cắp mật khẩu theo nhiều cách khác nhau. Hai phương pháp phổ biến bao gồm:

- Trộm cắp cơ sở dữ liệu mật khẩu: Tội phạm sử dụng tài khoản của người dùng có được từ 1 cơ sở dữ liệu bị đánh cắp (có được khi vi phạm hoặc được mua từ các trang web đen) để truy cập vào tài khoản người dùng tại một tổ chức khác.
- Tấn công lừa đảo xã hội: là dạng tấn công phi kỹ thuật nhằm vào người dùng. Tin tặc sẽ thuyết phục người dùng tiết lộ thông tin truy cập hoặc các thông tin có giá trị cho chúng để đạt được 1 thứ gì đó rất hấp dẫn, khai thác các điểm yếu cố hữu của người dùng như cả tin, ngây thơ, tò mò và lòng tham.

Một số kỹ thuật xã hội mà tin tặc thường sử dụng gồm:

- Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng, từ đó thuyết phục hoặc đánh lừa nạn nhân cung cấp thông tin;
- Kẻ tấn công có thể mạo danh là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân, hoặc tổ chức;

Kẻ tấn công có thể lập trang web giả các trang web của các tổ chức để đánh lừa người dùng cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng, v.v.

4.14 Tấn công hỗn hợp

Một cuộc tấn công hỗn hợp (Blended Attacks) thường sử dụng nhiều phương thức lây nhiễm. Ví dụ, một cuộc tấn công hỗn hợp có thể kết hợp các phương pháp lây lan của virus và worms để làm tăng mức độ nghiêm trọng của thiệt hại và tốc độ lây lan. Sâu Nimda thực sự là một ví dụ kinh điển cho cách thức tấn công này: Nó sử dụng 4 phương thức sau:

- Email: Khi người dùng ở 1 hệ thống có lỗ hổng bảo mật mở mở 1 tệp đính kèm (đã bị nhiễm) trên email, Nimda lập tức khai thác lỗ hổng đó để hiển thị trên trình duyệt web của nạn nhân để mở ra 1 trang html cơ bản để gửi/nhận mail mới. Sau đó, nó tìm kiếm toàn bộ địa chỉ thư điện tử trên máy nạn nhân để tiếp tục gửi những bản sao của nó tới các địa chỉ mà nó quét được.
- Windows Shares: Lợi dụng tính năng chia sẻ files của Windows, Nimda sau khi thâm nhập vào máy nạn nhân,

sẽ tìm kiếm trên hosts những file được chia sẻ và dùng NetBIOS như 1 cơ chế vận chuyển Nimda để lây nhiễm cho files. Nếu bạn mở file thì Bingo! Nimda đã chui trót lọt vào máy của bạn.

- Web Servers: Nimda sẽ quét các máy chủ sử dụng IIS (Internet Information Service của Microsoft) và tìm kiếm lỗ hổng bảo mật đã được phát hiện nhưng chưa được vá lỗi. Nếu tìm thấy lỗ hổng: Lập tức nó sao chép chính nó lên các máy chủ web đó và trên mọi tệp tin có thể lây nhiễm trên các máy chủ đó. Phương thức này cực kỳ hiệu quả, bởi sẽ có nhiều máy khách trở đến máy chủ bị nhiễm để lấy thông tin (chẳng hạn, đọc báo mạng, nhưng trang báo mạng đó trước đó đã bị nhiễm Nimda), nên phương thức này lây lan rất nhanh chóng.
- Web clients: Nếu nạn nhân sử dụng 1 trình duyệt web có lỗi bảo mật để truy cập tới máy chủ bị nhiễm virus nêu trên, thì máy của nạn nhân sẽ bị lây nhiễm ngay lập tức (nếu lỗi bảo mật trên thuộc danh sách những lỗi mà Nimda xác định sẽ tấn công).

Lưu ý: Tóm tắt các xu thế tấn công mạng

1. Tin tặc gia tăng hoạt động tấn công có chủ đích.
2. Chiếm đoạt tài khoản
3. Tấn công giả mạo
4. Tấn công mạo danh
5. Tấn công phá hủy dữ liệu
6. Tấn công trộm cắp dữ liệu

7. Hoạt động phát tán thông tin xấu, độc hại, thông tin sai sự thật trên không gian mạng tiếp tục tác động đến mọi mặt của đời sống xã hội.
8. Tội phạm lừa đảo chiếm đoạt tài sản qua mạng.
9. Hoạt động tổ chức đánh bạc bằng trò chơi trực tuyến.
10. Hoạt động cho vay “tín dụng đen” trên không gian mạng với lãi suất cao.
11. Hoạt động vi phạm pháp luật trên lĩnh vực thương mại điện tử.
12. Tấn công qua các thiết bị thông minh, trí tuệ nhân tạo (AI).
13. Đánh cắp mật khẩu
14. Tấn công hỗn hợp

5. Nguyên lý của việc tấn công trên môi trường mạng

Để truy cập vào Mạng, người dùng có thể dùng nhiều loại thiết bị khác nhau như máy tính để bàn (desktop), máy tính xách tay (laptop), máy tính bảng, điện thoại thông minh (smartphone), v.v. có kết nối Mạng. Việc vào các trang web, tải và cài đặt các ứng dụng, tham gia các mạng xã hội, v.v. từ các loại thiết bị nói trên hầu như không có sai biệt đáng kể. Do đó trong cuốn sổ tay này chúng tôi không đề cập cụ thể đến loại thiết bị mà người dùng sử dụng, chỉ gọi chung là thiết bị.

Đề tấn công vào thiết bị của người dùng, tin tặc (hacker) thường khai thác lỗ hổng bảo mật hoặc điểm yếu trong hệ thống, tạo thành các mối đe dọa hoặc các cuộc tấn công. Mỗi đe dọa là bất kỳ hành động nào có thể gây hư hại đến các tài sản hay tài nguyên hệ thống như phần cứng, phần mềm, cơ sở dữ liệu, dữ liệu, v.v. Chúng ta không thể triệt tiêu được hết các mối đe dọa vì đó là yếu tố khách quan, nhưng có thể giảm thiểu các lỗ hổng bảo mật tồn tại trong hệ thống, qua đó giảm thiểu khả năng bị khai thác để thực hiện tấn công.

Các cuộc tấn công qua mạng thường cố gắng gây tổn hại hoặc giành quyền kiểm soát hay quyền truy nhập vào các tài liệu và hệ thống quan trọng trong mạng máy tính của doanh nghiệp hoặc cá nhân.

5.1. Lỗ hổng bảo mật

Lỗ hổng bảo mật có thể xuất hiện trên phần cứng và phần mềm của hệ thống, trên thực tế trong số các lỗ hổng bảo mật được phát hiện hơn 95% là các lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng. Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng bao gồm:

- Lỗi tràn bộ đệm (Buffer overflow);
- Lỗi không kiểm tra đầu vào (Unvalidated input);
- Các vấn đề với kiểm soát truy cập (Access-control problems);

- Các điểm yếu trong xác thực, trao quyền hoặc các hệ mật mã (Weaknesses in authentication, authorization, or cryptographic practices); và
- Các lỗ hổng bảo mật khác.

Ngoài khai thác lỗ hổng bảo mật trên hệ thống thiết bị của người dùng, tin tặc còn sử dụng một số cách tấn công phi kỹ thuật dựa trên những điểm yếu cố hữu của người dùng để tạo nên những cuộc tấn công. Sau đây, chúng ta sẽ tìm hiểu một số dạng tấn công thường gặp.

5.2. Các dạng tấn công thường gặp

Tấn công qua mạng là vấn đề phổ biến và thường xuyên được các bên truyền thông đại chúng đưa tin. Về vấn đề giới, một rủi ro đáng kể đó là vi phạm dữ liệu của các tạp chí y khoa, ví dụ: tại một quốc gia ở Nam Mỹ, nơi phá thai là bất hợp pháp trừ khi cần thiết về mặt y tế (tuy nhiên vẫn còn bị kỳ thị), hồ sơ bệnh nhân đã bị rò rỉ (bao gồm cả dữ liệu phá thai y tế) và phụ nữ bị xác định và nhắm mục tiêu với sự căm ghét.

Đa phần các cuộc tấn công qua mạng được đề cập này đều ảnh hưởng tới hàng nghìn, nếu không muốn nói là hàng triệu người. Các cuộc tấn công qua mạng thường nhắm vào các nền tảng mạng xã hội, website lưu trữ dữ liệu cá nhân.

Dưới đây là một số cuộc tấn công qua mạng và trở thành xu hướng trong vài năm trở lại đây¹:

- **CNA Financial**: Công ty bảo hiểm CNA đã gặp phải một cuộc tấn công bằng mã độc tổng tiền vào Tháng Ba 2021 khiến các nhân viên không thể truy nhập các hệ thống và tài nguyên nội bộ. Tin tặc cũng đánh cắp dữ liệu quý giá và theo báo cáo, CNA Financial đã phải chi trả một khoản dàn xếp trị giá 40 triệu USD.
- **Colonial Pipeline**: Vào ngày 07/05/2021, khi Công ty Colonial Pipeline bị xâm nhập, toàn bộ mọi hoạt động đều bị ngưng lại để đối phó với cuộc tấn công. Để khôi phục hệ thống máy tính dùng cho việc quản lý các đường ống dẫn dầu xuyên suốt đông nam Hoa Kỳ, Colonial Pipeline đã phải trả cho tin tặc số tiền chuộc là 75 bitcoin (tương đương với 4,4 triệu USD vào thời điểm đó). Cuộc tấn công qua mạng này là cuộc tấn công lớn nhất trong lịch sử Hoa Kỳ nhắm tới hạ tầng dầu khí.
- **Tiền ảo**: Vào Tháng Ba và Tháng Tư 2022, ba giao thức cho vay khác nhau đều bị tấn công qua mạng. Trong khoảng thời gian một tuần, tin tặc đã đánh cắp số tiền ảo trị giá 15,6 triệu

¹ <https://www.microsoft.com/en/security/business/security-101/what-is-a-cyberattack>

USD từ Inverse Finance, 625 triệu USD từ Ronin Network (nền tảng chú trọng vào trò chơi) và 3,6 triệu USD từ Ola Finance.

Sau đây chúng tôi xin trình bày một số dạng tấn công phổ biến.

a. Tấn công vào mật khẩu

Tấn công vào mật khẩu (***Password attack***) là dạng tấn công điển hình nhằm đánh cắp và chiếm đoạt tài khoản của người dùng để lạm dụng. Kiểu tấn công này đã có từ lâu, có nhiều dạng biến tướng và vẫn thường xuyên có nhiều người bị mắc bẫy.

Có 3 dạng tấn công mật khẩu phổ biến:

- ***Brute Force Attack*** (tấn công dò mật khẩu): tin tặc sử dụng một công cụ mạnh mẽ, có khả năng thử nhiều username và password cùng lúc (từ dễ đến khó) cho tới khi đăng nhập thành công. VD: đặt mật khẩu đơn giản như 123456, password123, daylamatkhou, v.v rất dễ bị tấn công brute force.
- ***Dictionary Attack*** (tấn công từ điển): là một biến thể của Brute Force Attack, tuy nhiên tin tặc nhắm vào các từ có nghĩa thay vì thử tất cả mọi khả năng. Nhiều người dùng có xu hướng đặt mật khẩu là những từ đơn giản VD: motconvit, iloveyou. Đây là lý do khiến Dictionary Attack có tỉ lệ thành công cao hơn.

- **Key Logger Attack** (tấn công Key Logger): Tấn công Key Logger nguy hiểm hơn 2 cách tấn công trên, do việc đặt mật khẩu phức tạp không giúp ích gì trong trường hợp này. Để tấn công, tin tặc cần phải sử dụng một mã độc (malware) đính kèm vào máy tính (hoặc điện thoại) nạn nhân, phần mềm đó sẽ ghi lại tất cả những ký tự mà nạn nhân nhập vào máy tính và gửi về cho tin tặc. Phần mềm này được gọi là Key Logger.

	Mật khẩu yếu	Mật khẩu mạnh
Ví dụ	123456789	Anh@1325 Tp-1@8/5^^
Lý do	Chỉ gồm các từ hoặc các số Dễ dàng bị lộ	Có chữ hoa, chữ thường, số và các ký hiệu đặc biệt
Dạng tấn công	Tấn công từ điển Tấn công trực tiếp	Tấn công Key Logger Tấn công trực tiếp

Trên đây chỉ là các dạng tấn công mật khẩu trực tiếp. Kiểu tấn công này thường được phát tán qua các phần mềm không có bản quyền, phần mềm giả mạo, hoặc lây nhiễm qua các tệp tin lấy mã bẻ khóa phần mềm (kengen) trên Mạng.

Theo thống kê của BKAV cuối năm 2022, trong năm loại mã độc phổ biến thì mã độc đánh cắp mật khẩu và tài khoản PasswordStealer có mức độ ảnh hưởng nhỏ hơn với hơn nửa triệu máy tính, nhưng lại nguy hiểm khi xuyên thủng cơ chế bảo mật hai lớp hiện nay. Tin tặc dùng cookies đánh cắp được để đăng nhập tài khoản và thực hiện hàng loạt thao tác như đổi số điện thoại, email khôi phục, đặt mật khẩu mới, đăng xuất ra khỏi các thiết bị khác nhằm chiếm tài khoản; có tới 15.000 biến thể của mã độc này xuất hiện ở Việt Nam, đánh cắp và chiếm đoạt nhiều tài khoản Facebook, Gmail, tài khoản ngân hàng, ví điện tử... của nạn nhân.

Tin tặc có thể tấn công gián tiếp thông qua việc lừa đảo người dùng tự cung cấp mật khẩu (Tấn công giả mạo Phishing), tiêm nhiễm mã độc, tấn công vào cơ sở dữ liệu – kho lưu trữ mật khẩu người dùng của các dịch vụ.

b. Tấn công bằng mã độc (Malware)

Tấn công bằng mã độc (***Malicious code attack***) là dạng tấn công sử dụng các mã độc (Malware) làm công cụ để tấn công vào hệ thống thiết bị của nạn nhân. Tin tặc có thể khai thác những lỗ hổng bảo mật, hoặc nguy trang dưới dạng tệp đính kèm email hoặc chương trình tin cậy, lừa người dùng tải, cài đặt và chạy các mã độc như các phần mềm quảng cáo (Adwave), phần mềm gián điệp (Spyware), các loại mã độc như virus, worm, trojan, spyware, rootkit, ransomware, để tạo điều kiện cho tin tặc đột nhập vào máy tính/mạng máy tính.

Một số dạng tấn công phổ biến:

- Tấn công vào mật khẩu
- Tấn công bằng mã độc (Malware)
- Tấn công từ chối dịch vụ và tấn công từ chối dịch vụ phân tán
- Tấn công kiểu người đứng giữa
- Tấn công sử dụng các kỹ thuật xã hội
- Tấn công APT
- Tấn công Pharming

Trong quá trình sử dụng Mạng, những thao tác sau có thể khiến bạn bị nhiễm mã độc:

- Truy cập các trang web độc hại, tải trò chơi, file nhạc nhiễm mã độc, cài đặt thanh công cụ/phần mềm từ nhà cung cấp lạ, mở tệp đính kèm email độc hại hoặc các dữ liệu tải xuống không được quét bởi phần mềm bảo mật.

- Tải nhằm các ứng dụng độc hại nguy trang dưới dạng các ứng dụng hợp pháp, các thông báo cảnh báo khi cài đặt ứng dụng, đặc biệt khi ứng dụng yêu cầu quyền truy cập email hoặc thông tin cá nhân.
- Tải ứng dụng ở các nguồn không đáng tin cậy.
- Vô tình cài đặt các phần mềm bổ sung đi kèm với ứng dụng chứa mã độc.
- Không sử dụng các chương trình bảo mật cũng là lý do khiến mã độc xâm nhập dễ dàng hơn.

c. Tấn công từ chối dịch vụ và tấn công từ chối dịch vụ phân tán

Tấn công từ chối dịch vụ (***Denial of Service – DoS***) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy cập các tài nguyên mạng. Kiểu tấn công này thường nhằm vào các máy chủ của các công ty, doanh nghiệp nhằm làm dịch vụ ngừng hoạt động, giảm hiệu năng hệ thống hoặc nghẽn băng thông đường truyền mạng.

Tấn công từ chối dịch vụ phân tán (***Distributed Denial of Service – DDoS***) là một loại tấn công DoS đặc biệt, nhằm mục tiêu vào các website và máy chủ, cố gắng làm cạn kiệt tài nguyên của ứng dụng, và gây gián đoạn các dịch vụ mạng. Điểm khác biệt chính giữa DDoS và DoS là phạm vi tấn công: trong khi số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm, thì số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc hàng trăm ngàn

máy. Đồng thời, các máy tham gia tấn công DDoS có thể đến từ rất nhiều vị trí địa lý khác nhau, phân tán trên toàn cầu. Do vậy, việc phòng chống tấn công DDoS gặp nhiều khó khăn hơn so với việc phòng chống tấn công DoS. Ví dụ: hàng trăm cửa sổ bật lên, quảng cáo và kể cả website bị gặp sự cố đều có thể góp phần tạo nên cuộc tấn công DDoS trên máy chủ bị xâm phạm.

Các cuộc tấn công DDoS là một vài trong số các mối đe dọa trên mạng phổ biến nhất hiện nay, chúng có phạm vi mục tiêu rộng, hướng tới mọi loại ngành và công ty thuộc mọi quy mô trên toàn cầu. Mặc dù không có cách nào để phát hiện được cuộc tấn công DDoS, vẫn có một vài dấu hiệu cho thấy mạng Mạng của doanh nghiệp bạn đang bị tấn công:

- Lưu lượng truy cập web của doanh nghiệp tăng lên đột biến, có vẻ như không đến từ đâu và xuất phát từ cùng một địa chỉ hoặc dải IP.
- Mạng hoạt động trở nên chậm và bất thường.
- Các dịch vụ trên mạng Mạng của doanh nghiệp không phục vụ, hoặc đáp ứng chậm những yêu cầu mà người dùng gửi đến.

d. Tấn công kiểu người đứng giữa

Tấn công kiểu người đứng giữa (***Man in the middle attack – MITM***) là hiểu đơn giản là một loại tấn công mạng mà tin tặc sẽ đứng giữa người dùng và ứng dụng. Tin tặc sẽ chặn và kiểm soát

toàn bộ quá trình giao tiếp giữa hai bên để người dùng tin rằng họ vẫn đang trực tiếp liên lạc với nhau. Mục đích chính của dạng tấn công này là đánh cắp thông tin, tin tặc sẽ nắm bắt hết mọi thông tin trao đổi kể cả những thông tin nhạy cảm như số tài khoản, số thẻ tín dụng, hoặc thông tin nhạy cảm khác trong các ứng dụng trò chuyện và giao dịch... để đánh cắp danh tính, chuyển tiền hay gây ra các vụ lừa đảo và lấy được những thông tin có thể sử dụng để tống tiền và bôi nhọ một người.



Hình 3. Mô hình kiểu tấn công người đứng giữa

Người dùng các ứng dụng doanh nghiệp SaaS, trang web thương mại điện tử,... chính là mục tiêu của các vụ tấn công dạng này. Kiểu tấn công MITM phổ biến nhất hiện nay là Man in the Browser, tin tặc sẽ tập trung vào việc lây nhiễm trình duyệt và cài những mã độc vào thiết bị của nạn nhân để đánh cắp thông tin.

Dưới đây là ví dụ điển hình về tấn công MITM mà bạn nên biết:

- **Ứng dụng di động của Equifax:** Năm 2017, MITM tấn công Equifax, hậu quả để lại là thông tin của 150 triệu người Mỹ bị

rò rỉ. Qua vụ việc này, người dùng đã phát hiện ra ứng dụng điện thoại của công ty không phải lúc nào cũng dùng HTTPS. Đây chính là lỗ hổng để tin tặc ăn cắp dữ liệu một cách đơn giản và nhanh chóng.

- **Tấn công phần mềm quảng cáo Superfish Visual Search:** Năm 2015, máy tính Lenovo đã ra mắt phần mềm quảng cáo có tên là Superfish Visual Search. Phần mềm này chèn quảng cáo mặc định nên người dùng dễ bị tấn công MITM. Vào tháng 2 năm 2015, bản phát hành cập nhật của Microsoft Windows Defender đã loại bỏ lỗ hổng này.

e. Tấn công sử dụng các kỹ thuật xã hội

Tấn công sử dụng các kỹ thuật xã hội (***Social engineering attack***) là dạng tấn công phi kỹ thuật nhằm vào người dùng. Dạng tấn công này sử dụng các hình thức thao túng hành vi con người thay vì tập trung khai thác các lỗ hổng bảo mật của thiết bị. Qua đó, tin tặc có thể đạt được các mục đích của mình như xâm nhập vào hệ thống, truy cập thông tin quan trọng,... mà không cần phải thực hiện những kỹ thuật tấn công quá phức tạp.

Tấn công phi kỹ thuật không giới hạn hình thức, phương thức, nạn nhân và thủ phạm. Bất kỳ ai đều có thể là tội phạm và bất kỳ ai đều có thể là nạn nhân. Chính vì vậy bạn cần phải nâng cao cảnh giác và đề ý từ các chi tiết nhỏ nhất.

Bất kỳ một chuyên gia bảo mật nào cũng đều cho rằng con người chính là điểm yếu nhất của hệ thống bảo mật bởi con người có nhiều cảm xúc và những cảm xúc đó không thể kiểm soát được như những hệ thống máy móc. Bạn có thể xây dựng một hệ thống phòng thủ kiên cố với rất nhiều hàng rào, khóa cửa, camera an ninh,.. nhưng lại mất đề phòng với một người bạn mới quen hoặc một thợ kỹ thuật sửa chữa đồ gia dụng. Sẽ ra sao nếu như họ chính là tên tội phạm giả mạo? Bạn hoàn toàn không kiểm soát được những rủi ro mà tên tội phạm đó đem tới. Trừ khi bạn cảnh giác với hành vi và thói quen sử dụng các nền tảng truyền thông xã hội, sử dụng Mạng và các ứng dụng công nghệ trực tuyến, đồng thời nhận thức được các rủi ro liên quan đến mạng. Các cách duy nhất là:

- Biết các hình thức tấn công mạng khác nhau,
- Nhận thức được các tội phạm trực tuyến do xã hội tạo ra,
- Nhận thức được những rủi ro và tác hại mà tội phạm mạng sẽ gây ra cho bạn, gia đình bạn, công ty và tổ chức của bạn.
- Biết cách thức, ai, ở đâu có thể giúp bạn ngăn chặn, bảo vệ và phục hồi khỏi các cuộc tấn công và tổn hại trên mạng.

Các tâm lý hành vi được tội phạm Social Engineering khai thác thường là khía cạnh về nghĩa vụ đạo đức, lòng tin, đe dọa, tính tham lam, thiếu hiểu biết, tò mò, tự mãn,...

Có rất nhiều hình thức khác nhau của kiểu tấn công này, nhưng có thể điếm qua một số kỹ thuật xã hội mà tin tặc thường sử dụng như:

- **Phishing** là hình thức Social Engineering phổ biến nhất mà tin tặc tạo ra các email/trang web mạo danh các công ty, tổ chức (ngân hàng, bộ công thương,...)/trang mạng xã hội nổi tiếng (Facebook, Twitter,...) hoặc ứng dụng để người dùng nhập thông tin cần thiết, thực hiện các lệnh chuyển tiền...;
- **Baiting**: Đây là hình thức tấn công phi kỹ thuật thường xảy ra giữa những người có mối liên hệ xã hội, người quen. Khi có được sự tin nhiệm của nạn nhân, tin tặc tiến hành gửi/mượn usb hoặc các thiết bị công nghệ có chứa mã độc khiến người dùng sử dụng thiết bị đó để đăng nhập vào hệ thống công ty;
- **Vishing**: Vishing là hình thức lừa đảo mạo danh thông qua điện thoại. Trong hình thức này, tin tặc gọi điện cho đối tượng tấn công, đóng giả làm một thực thể uy tín để chiếm đoạt lòng tin. Bằng cách đó, người bị lừa sẽ không mấy may nghi ngờ và cung cấp cho chúng các thông tin nhạy cảm như số tài khoản ngân hàng, mật khẩu quan trọng... Phiên bản mới nhất của dạng lừa đảo này là áp dụng công nghệ Deepfake. Công nghệ này có thể bắt chước các đặc điểm như khuôn mặt hoặc giọng nói bằng AI mà tội phạm có thể sử dụng để lừa đảo người thân hoặc đồng nghiệp của một người bằng cách đóng giả họ.

- **Piggybacking**: là hình thức Social Engineering mà tin tặc lừa người có thẩm quyền để đột nhập vào công ty. Trong hình thức này, tin tặc đóng giả là nhân viên chính thức/người thân/thợ sửa chữa/người có thẩm quyền, yêu cầu thông tin quan trọng hoặc các thông tin cần thiết để xâm nhập hệ thống, gắn các thiết bị theo dõi hoặc trực tiếp tấn công hệ thống/chiếm đoạt tài sản.
- **Nghe trộm/camera ẩn**: Trong một vài trường hợp, kẻ xấu có thể nghe trộm cuộc gọi, cuộc sống sinh hoạt hàng ngày bằng cách cài trộm các thiết bị tinh vi như camera hay micro ẩn vào đối tượng bị theo dõi. Tội phạm có thể nhắm mục tiêu cụ thể là phụ nữ để ghi lại các cuộc thảo luận hoặc hình ảnh/video thân mật và sử dụng chúng mà không có sự đồng ý.
- **Pop-up window**: Với hình thức này, hacker tạo ra các cửa sổ Pop-up hiện lên máy tính lừa người dùng bấm vào link, đổi hướng trang web, yêu cầu người dùng nhập thông tin cá nhân hoặc tải phần mềm chứa mã độc.

Khi bị tấn công Social Engineering, bạn có thể gặp phải một số hậu quả nghiêm trọng như:

- **Mất dữ liệu**: Các thông tin về hợp đồng kinh tế, hợp đồng vay vốn, chiến lược kinh doanh, marketing, thậm chí là bảng lương... đều là những thông tin hết sức nhạy cảm và có thể ảnh hưởng đến toàn bộ công ty. Đơn giản hơn, các dữ liệu về

công việc bạn mất bao nhiêu công sức để soạn có thể bị lấy cắp và xóa hết...

- **Mất niềm tin xã hội:** Khi bị tấn công phi kỹ thuật, thông tin nội bộ của một tổ chức bị lộ ra ngoài có thể gây hoang mang dư luận. Doanh nghiệp (ngân hàng, bảo hiểm,...) nắm các thông tin cá nhân quan trọng của khách hàng, khi doanh nghiệp bị tấn công có thể dẫn đến thông tin cá nhân khách hàng bị lộ, khách hàng sẽ không còn niềm tin đối với doanh nghiệp. Hoặc bạn là một cá nhân, bạn có thể bị lộ những hình ảnh nhạy cảm, riêng tư, gây mất hình tượng,...
- **Mất quyền riêng tư:** Bị lấy thông tin cá nhân như địa chỉ, số điện thoại, thói quen sinh hoạt,... dẫn tới nhiều hệ lụy phiền toái. Nhiều người phàn nàn vì họ liên tục nhận được các cuộc gọi điện thoại “mời chào” cho vay tín dụng, bảo hiểm,... thậm chí một vài người bị theo dõi và tấn công.
- **Thất thoát tài chính:** Các tài khoản ngân hàng có thể bị rút tiền trực tiếp; Các đơn hàng/tiền có thể bị cố tình gửi nhầm sang địa chỉ mà tội phạm mạng xác định từ trước...
- **Hoạt động kinh doanh bị ảnh hưởng:** Nếu bị tấn công mạnh vào máy chủ website hoặc máy chủ hệ thống mạng, hệ thống rất có thể bị đánh sập, website của công ty, tổ chức có thể bị treo (tạm ngừng hoạt động dịch vụ).

f. Tấn công APT

APT là tấn công có chủ đích hướng mục tiêu vào mạng hoặc các máy tính riêng lẻ. Khác với tấn công đại trà tập trung vào các máy tính cá nhân được bảo vệ kém nhất, tấn công chủ đích tìm kiếm cơ hội xâm nhập vào một hệ thống xác định bất kể mức độ bảo vệ.

Tấn công chủ đích vào doanh nghiệp hầu hết thường được thực hiện theo đặt hàng của đối thủ cạnh tranh hoặc từ cá nhân có khả năng kiếm tiền từ thông tin lấy được.

Khi thực hiện tấn công chủ đích, những tin tặc sử dụng mọi phương tiện như mã độc được thiết kế cho mục đích cụ thể, tấn công vào các máy chủ web và cơ sở hạ tầng mạng, kỹ nghệ xã hội, nội gián.... APT là loại tấn công phức tạp, trình độ cao và dai dẳng với mục đích chiếm quyền kiểm soát hệ thống trong thời gian lâu nhất có thể. APT thường được thực hiện trên các đối tượng được bảo vệ tốt, khi những phương pháp đơn giản không có hiệu quả hoặc dễ làm lộ tin tặc.

g. Tấn công Pharming

Tấn công Pharming là một kỹ thuật mà tin tặc sử dụng để tấn công máy tính cá nhân hoặc các máy chủ. Cụ thể, chúng sẽ hướng người dùng đến các trang web giả mạo để đánh cắp thông tin cá nhân như: số thẻ tín dụng, số tài khoản ngân hàng hay mật khẩu tài khoản, v.v của họ. Có hai dạng tấn công pharming:

(1) Kẻ tấn công thường sử dụng sâu, vi rút hoặc các mã độc cài đặt vào hệ thống nạn nhân để kiểm soát trình duyệt của người dùng; và

(2) Kẻ tấn công cũng có thể tấn công vào hệ thống phân giải tên miền để thay đổi kết quả truy vấn: thay thế địa chỉ IP của website hợp pháp thành địa chỉ IP của website độc hại.

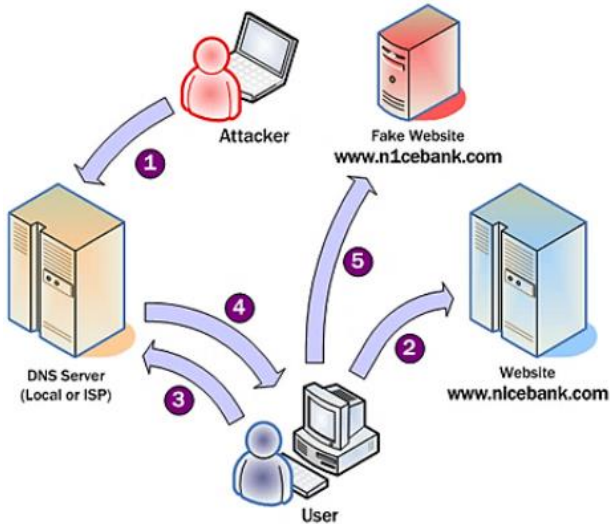
Hình 4 minh họa cửa sổ trình duyệt của người dùng bị tấn công dạng (1), khi người dùng nhập địa chỉ trang Google.com và gõ Enter, thì trình duyệt lại tải và nạp trang adventureinsecurity.com. Trong trường hợp này, trình duyệt của nạn nhân đã bị cài đặt trình cắm (plug-in hoặc add-on) độc hại có khả năng kiểm soát trình duyệt.



Hình 4. Tấn công cướp trình duyệt Pharming dạng 1

Hình 5 minh họa các bước tấn công của dạng (2), trong đó kẻ tấn công xâm nhập vào máy chủ DNS chỉnh sửa địa chỉ IP của website hợp pháp thành địa chỉ IP của webserver của chúng. Kết quả

là trình duyệt người dùng bị chuyển hướng yêu cầu tải website của kẻ tấn công. Người dùng nạn nhân thậm chí không hề phát hiện ra dấu hiệu bất thường hay nguy hiểm nào. Hầu như không có phần mềm bảo vệ nào có thể xử lý được loại tấn công này.



Hình 5. Mô phỏng các bước tấn công của Pharming dạng 2

IV. Phòng chống nguy cơ

Không có giải pháp xử lý và khắc phục sự cố sau vi phạm nào có thể mang lại mức độ bảo vệ tốt bằng việc ngăn chặn và phòng ngừa vi phạm đúng cách. Phòng ngừa không chỉ giúp bạn khôi phục tốt hơn mà còn giúp đảm bảo rằng bạn có thể phát hiện ra bị tấn công sớm nhất có thể. Nếu không có sự phòng ngừa thích hợp, bạn thậm chí có thể không xác định được rằng bạn đã bị tấn công, chứ chưa

nói đến khả năng ngăn chặn được cuộc tấn công có thể tới bất kỳ lúc nào.

1. Xác định nguy cơ

Để phòng chống nguy cơ, chúng ta cần nắm được những cách thức cơ bản để tin tặc có thể lây nhiễm những mã độc vào trong hệ thống thiết bị của nạn nhân.

1.1. Lây nhiễm từ các thiết bị lưu trữ di động

Nhiều sâu máy tính phát tán bằng cách lây nhiễm qua các thiết bị lưu trữ di động như ổ USB, các đĩa cứng di động, hoặc qua các thiết bị công nghệ. Mã độc có thể tự động cài đặt khi bạn kết nối thiết bị bị nhiễm với thiết bị của bạn.

Để tránh loại lây nhiễm này, **bạn cần:**

- Thận trọng với mọi thiết bị lưu trữ di động không phải của bạn. Chẳng hạn nếu tự dung lại nhặt được 1 USB nào đó, bạn không nên thử USB đó trên

Lưu ý: Xác định nguy cơ:

- Lây nhiễm từ các thiết bị lưu trữ di động
- Lây nhiễm qua email hoặc ứng dụng chat trên mạng xã hội
- Lây nhiễm mã độc macro trên Office
- Mã độc được gắn kèm trên phần mềm khác
- Truy cập vào các trang web không an toàn

những thiết bị có dữ liệu quan trọng của bạn. Đôi khi, tin tặc sẽ cố ý để các USB bị nhiễm vào những khu vực phổ biến và nếu ai đó cầm lấy và cắm vào thiết bị của họ, thì đã bị mắc bẫy.

- Bạn nên thực hiện quét virus thiết bị lưu trữ di động bất kỳ ngay trước khi có ý định sử dụng nó.

1.2. Lây nhiễm qua email hoặc ứng dụng chat trên mạng xã hội

Khi đã lây nhiễm vào máy nạn nhân, virus có thể tự tìm ra danh sách các địa chỉ thư điện tử sẵn có trên máy và nó tự động gửi đi hàng loạt thư có nhiễm virus cho những địa chỉ trong danh sách đó. Nếu chủ nhân của những máy nhận được thư có chứa virus mà ko phát hiện ra, tiếp tục để lây nhiễm vào máy, thì virus lại tiếp tục tìm danh sách địa chỉ và gửi đi theo cách thức ở trên. Chính vì vậy mà số lượng phát tán có thể tăng theo cấp số nhân khiến cho trong 1 thời gian ngắn có đến hàng triệu máy tính bị lây nhiễm, có thể làm tê liệt nhiều cơ quan trên thế giới chỉ trong thời gian ngắn. Cách lây nhiễm này còn được tái hiện trên các ứng dụng chat trên các mạng xã hội như Facebook Messenger, Zalo...

Có 3 phương thức lây nhiễm qua thư điện tử hoặc ứng dụng chat bao gồm:

- ***Lây nhiễm vào các file đính kèm theo thư điện tử*** (attached mail). Máy tính của người dùng sẽ không bị nhiễm virus cho tới khi file đính kèm bị nhiễm virus được kích hoạt (do đặc

điểm này các virus thường được "trá hình" bởi các tiêu đề hấp dẫn như sex, thể thao hay quảng cáo bán phần mềm với giá vô cùng rẻ).

- ***Lây nhiễm do mở 1 liên kết trong thư điện tử.*** Các liên kết trong thư điện tử có thể dẫn đến 1 trang web được cài sẵn virus, cách này thường khai thác các lỗ hổng của trình duyệt và hệ điều hành. Hay nói cách khác, nếu mở một liên kết trong thư điện tử thì thiết bị có thể bị lây nhiễm virus.
- ***Lây nhiễm ngay khi mở để xem thư điện tử (Zero-click):*** Hình thức tấn công này vô cùng nguy hiểm vì nó không yêu cầu bất cứ hành vi nhấp chuột hoặc tương tác nào của nạn nhân để hoạt động, cũng không cần lừa đảo hoặc thuyết phục người dùng nhấp vào bất kỳ liên kết hay tệp tin nào, chỉ cần mở thư điện tử thì đã tự động bị lây nhiễm mà không hề có một dấu hiệu cảnh báo nào. Kiểu tấn công này thường khai thác các lỗ hổng trong hệ thống. Trên thực tế thì các ứng dụng email và nhắn tin trực tuyến như iMessage của Apple là đích ngắm của tin tặc để thực hiện kiểu tấn công này.

1.3. Lây nhiễm mã độc macro trên Office

Bộ phần mềm Office là một bộ công cụ văn phòng được dùng vô cùng phổ biến, vì thế tin tặc đã lựa chọn là công cụ để giải mã độc làm bàn đạp để chúng đưa những phần mềm độc hại vào hoặc thực hiện tấn công thiết bị của bạn.

Một thủ thuật phổ biến của tội phạm mạng là gửi thông báo cho bạn rằng bạn sắp bị tính phí một dịch vụ nào đó mà bạn chưa từng đăng ký. Khi bạn liên hệ với họ để thông báo rằng bạn yêu cầu hủy dịch vụ, họ sẽ yêu cầu bạn tải xuống một tệp Excel họ cung cấp và điền một số chi tiết. Nếu bạn tải xuống và mở tệp, thì tệp Excel sẽ hiển thị cảnh báo như sau:



Cảnh báo Bảo mật

Một số nội dung hiện hoạt đã bị tắt. Bấm để biết thêm chi tiết.

Bật Nội dung

Hình 6. Ví dụ một thông báo lừa đảo của tin tặc trên Excel

Trường hợp này bạn không nên chọn “Bật Nội dung”, nếu không mã độc macro sẽ được kích hoạt và tấn công thiết bị của bạn.

1.4. Mã độc được gắn kèm trên phần mềm khác

Một số mã độc có thể được cài đặt cùng lúc với các chương trình khác mà bạn tải xuống. Ví dụ như một số thanh công cụ hoặc chương trình hiển thị quảng cáo mỗi khi bạn duyệt web. Thông thường bạn có thể chọn không sử dụng hoặc không cài đặt những ứng dụng bổ sung này bằng cách bỏ chọn hộp kiểm trong quá trình cài đặt, tuy nhiên nếu khi cài đặt bạn không để ý thì rất có thể bị mắc phải lỗi này.

1.5. Truy cập vào các trang web không an toàn

Khi truy cập vào các trang web không có độ tin cậy cao, đồng nghĩa với việc người dùng chấp nhận rủi ro là sẽ có khả năng bị các

mã độc lây nhiễm sang máy tính của bạn. Đó là do mã độc lợi dụng những lỗ hổng bảo mật trong trình duyệt web để lây nhiễm sang thiết bị của bạn.

2. Phòng ngừa ở mức độ cá nhân người dùng

Để phòng ngừa điều này ở mức độ cá nhân người dùng, chúng tôi có đưa ra một vài khuyến nghị như sau:

2.1. Bảo vệ bằng mật khẩu

Mật khẩu là phòng tuyến đầu tiên chống lại hành vi truy nhập trái phép vào các tài khoản, thiết bị và dữ liệu trực tuyến. Mật khẩu càng mạnh thì càng tăng khả năng bảo vệ tài sản của người dùng.

Cách tối ưu để bảo vệ mật khẩu:

- Sử dụng mật khẩu mạnh trên mọi thiết bị và tài khoản.
- Luôn hoài nghi với các liên kết và tệp đính kèm.
- Che giấy tờ, màn hình thiết bị và bàn phím để ngăn kẻ xấu đánh cắp mật khẩu bằng cách nhìn lén qua vai của đối tượng.
- Tránh truy nhập vào dữ liệu cá nhân và tài chính bằng WiFi công cộng.
- Cài đặt phần mềm chống vi-rút và chương trình chống phần mềm có hại trên mọi thiết bị.

Hãy làm theo các hướng dẫn sau để tạo mật khẩu mạnh:

- Sử dụng tối thiểu từ 8 đến 12 ký tự.
- Sử dụng tổ hợp các chữ cái, số và ký hiệu.

- Sử dụng tối thiểu một chữ hoa.
- Sử dụng mật khẩu khác nhau cho từng tài khoản.

Có một số trang web hỗ trợ cho người dùng cách tạo ra những mật khẩu theo mong muốn, ví dụ như trang <https://passwordsgenerator.net/> có giao diện như hình dưới đây:



Trình tạo Mật khẩu Ngẫu nhiên

Độ dài Mật khẩu:

Dùng Ký hiệu: (ví dụ @\$%)

Dùng Số: (ví dụ 123456)

Dùng các Ký tự viết Thường: (ví dụ abcdefgh)

Dùng các Ký tự viết Hoa: (ví dụ ABCDEFGH)

Loại trừ các Ký tự Giống nhau: (ví dụ i, l, 1, L, o, 0, O)

Loại trừ các Ký tự Nhập nhãng: ({ } [] () \ ' " ~ , ; . < >)

Tạo Trên Máy của Bạn: (KHÔNG tạo trên đám mây)

Chọn tự động: (tự động chọn mật khẩu)

Lưu Cài đặt của Tôi: (lưu toàn bộ cài đặt trên vào cookie)

Để đăng Tài Cài đặt của Tôi:

Mật khẩu Mới của Bạn:

Ghi nhớ mật khẩu của bạn: Ghi nhớ mật khẩu của bạn nhờ các chữ cái đầu của mỗi từ trong câu này.

Hình 7. Giao diện trang web hỗ trợ tạo mật khẩu ngẫu nhiên

2.2. Xác minh hai bước

Dù đã đặt mật khẩu mạnh cho mỗi tài khoản là khác nhau, bạn vẫn có nguy cơ bị mất mật khẩu này khi truyền qua mạng không

dây công cộng không an toàn, chẳng hạn như khi ở một quán cà phê Mạng.

Để tự bảo vệ mình, bạn có thể sử dụng chế độ xác minh hai bước (hay chứng thực hai lớp, bảo mật hai lớp), có nghĩa là ngoài mật khẩu, bạn cần một thông tin khác để đăng nhập vào website hay dịch vụ. Điều này sẽ khiến cho kẻ gian gặp khó khăn hơn trong việc truy cập tài khoản của bạn ngay cả khi đã biết được mật khẩu.

Tính năng này thường được các bên dịch vụ cung cấp sẵn, bạn chỉ cần thiết lập cá nhân hóa để sử dụng. Ví dụ như các ngân hàng thường đề nghị khách hàng thiết lập tính năng xác thực hai lớp cho các tài khoản Smart Banking, Google cũng cung cấp dịch vụ xác thực 2 lớp cho tài khoản Gmail.

Có 3 lựa chọn loại xác minh 2 bước:

1. Dùng mã xác minh bằng các ứng dụng xác thực như Google Authenticator hoặc Duo Mobile.
2. Dùng tin nhắn văn bản (SMS) để nhận mã xác minh.
3. Dùng khóa bảo mật vật lý. Với phương thức này người dùng phải trang bị thêm 1 thiết bị khóa như Yubico, Yubikey, Google Titan...

Google
<https://support.google.com/accounts/answer/>

Sử dụng khóa bảo mật cho tính năng Xác minh 2 bước
 Khắc phục vấn đề với NFC. Đảm bảo bạn thực hiện những bước sau: Bật NFC trên thiết bị của bạn; Thêm khóa vào tài khoản của bạn; Xóa mọi thứ có thể đang chặn tin ...

Microsoft
<https://support.microsoft.com/vi-vn> · Translate this page

Thiết lập khóa bảo mật làm phương pháp xác minh của bạn
 Khóa bảo mật là thiết bị thực dụng sử dụng với mã PIN duy nhất để đăng nhập vào tài khoản cơ quan hoặc trường học của bạn. Vì khóa bảo mật yêu cầu bạn phải có ...
 Khóa bảo mật: Xác minh 2 bước và xác thực ... Tài khoản email: Chỉ đặt lại xác thực bằng ...
 Câu hỏi về bảo mật: Chỉ đặt lại xác thực bằng ... Authenticator dụng: Xác minh 2 bước và xả...

guongnghe.com
<https://guongnghe.com/khoa-bao-...> · Translate this page

Khóa bảo mật và các cách kết nối an toàn
 Jul 15, 2022 — Khóa bảo mật là một thiết bị phần cứng cỡ nhỏ có tác dụng bổ sung thêm lớp bảo vệ cho các tài khoản trực tuyến như Facebook, Email, iCloud...
 ★★★★★ Rating: 5 · 4 votes

Sponsored

		
Khóa bảo mật Yubico... ₫790,000 Gu Công N... ★★★★★ (92)	Khóa bảo mật Yubico... ₫2,290,000 Gu Công N... ★★★★★ (19)	Khóa bảo mật Yubikey 5... ₫1,590,000 Gu Công N... ★★★★★ (174)
		
Khóa bảo mật Yubico... ₫790,000 Shopee	Khóa bảo mật Yubico... ₫990,000 Gu Công N...	Khóa bảo mật Yubico... ₫1,690,000 Gu Công N...

Hình 8. Khóa bảo mật cho tính năng xác minh hai bước

2.3. Dùng các phần mềm Antivirus

Phần mềm diệt virus (Anti-virus) là một giải pháp bảo mật được cung cấp bởi các công ty đảm bảo an ninh mạng. Nó là một công cụ chạy trên các thiết bị có tính năng tự động phát hiện, loại bỏ các virus máy tính, mã độc chạy trong thiết bị. Nó ngăn người dùng truy cập các trang web có khả năng lây nhiễm virus, mã độc vào máy tính hoặc ngăn không cho mở các email có chứa các mã độc được đính kèm với chúng. Ngoài ra, phần mềm diệt virus còn có thể khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus trong tương lai.

Phần mềm antivirus thường hoạt động theo nguyên lý như sau:

- Các công ty xây dựng phần mềm này biên soạn một cơ sở dữ liệu về các loại virus và mã độc đã biết và dạy phần mềm cách phát hiện, ngăn cản và loại bỏ chúng.
- Khi các tệp, chương trình và ứng dụng chạy vào và ra khỏi máy tính của bạn, phần mềm antivirus sẽ so sánh chúng với cơ sở dữ liệu của nó để tìm các kết quả phù hợp. Các kết quả tương tự hoặc giống hệt với cơ sở dữ liệu sẽ bị cô lập, quét và loại bỏ.

Phòng ngừa:

- Bảo vệ bằng mật khẩu
- Xác minh hai bước
- Dùng các phần mềm Antivirus
- Dùng tường lửa (Firewall)

Quan trọng là thay đổi hành vi sử dụng mạng internet và luôn có nguyên tắc trong việc sử dụng mạng cho cá nhân và công ty một cách an toàn nhất và theo quy trình bảo mật của công ty/tổ chức.

- Bạn có thể đặt các tùy chỉnh để phần mềm sẽ thực hiện chạy tự động thường xuyên hoặc có thể quét thủ công tệp, thư mục hoặc phần dữ liệu nào đó tùy theo ý của bạn.
- Một số phần mềm diệt vi-rút sẽ yêu cầu sự cho phép của bạn trước khi "dọn dẹp" một tệp để loại bỏ mã độc. Nếu bạn thích cách tiếp cận đơn giản hơn, bạn có thể điều chỉnh cài đặt để phần mềm tự động xóa các tệp độc hại.

Trên thị trường có rất nhiều loại phần mềm diệt virus, miễn phí hay trả phí, trong nước hoặc ngoài nước đều có. Hầu hết các phần mềm chống vi-rút đều thực hiện các chức năng giống nhau, vì vậy

việc lựa chọn giữa nhãn hiệu này và nhãn hiệu khác hoàn toàn tùy thuộc vào khả năng chi phí của mỗi người. Nhiều chưa hẳn là tốt,

Lưu ý: Mặc dù phần mềm chống vi-rút rất quan trọng, nhưng chúng có thể gây lo ngại về quyền riêng tư và điều quan trọng là phải lựa chọn phần mềm một cách cẩn thận. Một số phần mềm có thể bán dữ liệu của bạn cho các tác nhân bên thứ ba, giải mã lưu lượng truy cập web được mã hóa, cài đặt các chương trình không mong muốn và một số phần mềm có thể được sử dụng cho mục đích gián điệp. Một số chương trình cũng có thể được khởi chạy để thực sự thu thập dữ liệu cho tin tặc và kẻ thù. Các chương trình chống vi-rút miễn phí có xu hướng rủi ro hơn.

nhưng nên cài đặt ít nhất một phần mềm diệt virus trên thiết bị của mình.

Một ứng dụng Antivirus được tích hợp sẵn trong tất cả Hệ điều hành Windows tính từ Windows 7, đó là sản phẩm Windows Security. Ưu điểm của phần mềm này là có sẵn theo bộ cài của Hệ điều hành Windows và cũng đồng thời tự động được cập nhật theo yêu cầu của hãng Microsoft nên cũng rất tiện sử dụng. Tuy nhiên nếu người dùng cài đặt thêm một ứng dụng chống virus khác, thì phần mềm này mặc dù vẫn ở trên thiết bị, nhưng sẽ tự động tắt đi chế độ chạy mặc định.

Hướng dẫn chi tiết về sử dụng ứng dụng Windows Security được trình bày trong phần Phụ lục của Sổ tay này.

2.4. Dàng tường lửa (Firewall)

Tường lửa là một hệ thống ngăn chặn truy cập trái phép vào mạng. Tường lửa Firewall hoạt động giống như một người giữ cổng ở lối vào mạng, kiểm tra nhận dạng của tất cả những người cố gắng truy cập vào. Mọi nỗ lực truy cập trái phép đều bị chặn tự động.

Trước khi bạn có thể hiểu chính xác lý do tại sao tường lửa quan trọng, trước tiên bạn cần hiểu cách thức dữ liệu được gửi giữa các máy tính.

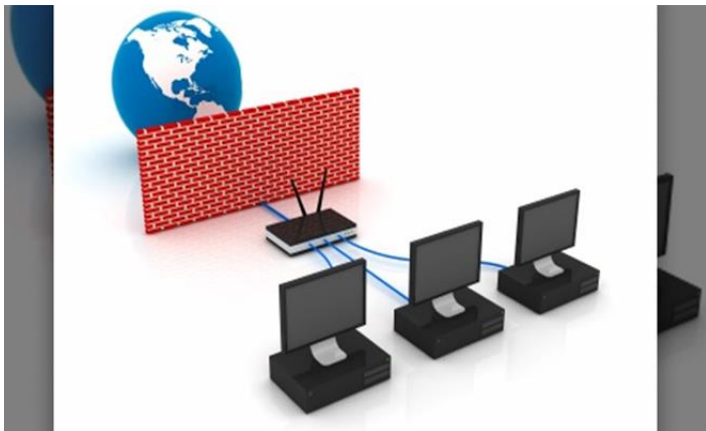
Ví dụ khi bạn gửi email một tài liệu đến các đồng nghiệp. Máy tính của bạn chia tài liệu thành các phần nhỏ gọi là các gói, sau

đó gửi từng gói tài liệu tới máy tính đồng nghiệp của bạn. Toàn bộ quá trình có thể hoàn thành chỉ trong vài giây.

Tuy nhiên không phải lúc nào quy trình này cũng được thực hiện một cách hoàn hảo. Các gói có thể bị hỏng hoặc mất trong quá trình chuyển, hoặc có thể bị tin tặc chặn và sửa đổi.

Sự xuất hiện của tường lửa như tạo thêm một lớp bảo vệ quan trọng vào cơ chế truyền dữ liệu. Tường lửa nằm giữa máy tính của bạn và Mạng, kiểm tra mọi gói tin đi qua. Bất kỳ gói tin nào bị làm giả, đến từ một nguồn trái phép hoặc không nhận dạng được thì sẽ bị chặn tự động.

Ngoài ra, tường lửa còn giám sát tất cả dữ liệu vào/ra, ngăn chặn tin tặc xâm nhập vào máy tính hoặc các thiết bị kết nối Mạng khác của bạn.



Hình 9.Tính năng Firewall

Tường lửa không giống như phần mềm Antivirus, nó không kiểm tra xem các gói dữ liệu đến có chứa mã độc hay không? Nhưng nó sẽ tự động chặn những lưu lượng mạng đáng ngờ hoặc ngăn chặn các ứng dụng thực hiện giao tiếp không mong muốn thông qua công Mạng.

Tường lửa được sử dụng cho cả doanh nghiệp và cá nhân. Các tổ chức hiện đại kết hợp chúng vào hệ thống SIEM (security information and event management) cùng với các thiết bị an ninh mạng khác. Việc vận hành hệ thống SIEM ở doanh nghiệp cần phải có đội ngũ có trình độ CNTT mới thực hiện được.

3. Phòng ngừa ở mức độ công ty, doanh nghiệp

Năm 2019, Bộ Thông tin và Truyền thông đã phát hành Tài liệu hướng dẫn triển khai Hoạt động giám sát An toàn thông tin trong cơ quan, tổ chức nhà nước,² trong tài liệu có hướng dẫn rất chi tiết các nội dung gồm: Hướng dẫn phương án triển khai hoạt động giám sát an toàn thông tin; thiết lập, quản lý vận hành hệ thống giám sát an toàn hệ thống thông tin; thuê dịch vụ giám sát an toàn thông tin và hướng dẫn kết nối với hệ thống kỹ thuật của Trung tâm Giám sát

² https://mic.gov.vn/Upload_Moi/VanBan/2973-CATTTT.pdf

an toàn không gian mạng quốc gia. Đối với các tổ chức, doanh nghiệp thì đây là một tài liệu hay và rất chi tiết đáng để tham khảo.

Dưới đây là một số khuyến cáo cần thực hiện với các doanh nghiệp, tổ chức như sau:

3.1. Cần có người phụ trách an ninh thông tin

Công ty, tổ chức nào cũng cần phải có người thực hiện nhiệm vụ này. Đó có thể chính là một lãnh đạo của công ty, hoặc có thể là một nhân viên khác nhưng việc này cần được công khai rõ ràng. Bạn có thể tuyển dụng người quản trị CNTT để giám sát mọi vấn đề về hệ thống mạng trong doanh nghiệp, nhưng nếu không tìm được ai có đủ khả năng và đủ tin tưởng thì nên thuê dịch vụ của một đơn vị chuyên nghiệp. Đơn vị này sẽ trợ giúp cho doanh nghiệp bạn tùy theo mức độ yêu cầu, có thể chỉ là bên hỗ trợ bộ phận CNTT nội bộ giám sát các mạng và hệ thống của doanh nghiệp, tư vấn đầu tư một hệ thống an ninh mạng đáng tin cậy, hoặc thực hiện được các hoạt động đảm bảo an toàn thông tin cần thiết như định kỳ cài đặt các bản vá bảo mật, thường xuyên rà soát và phát hiện những lỗi bảo mật có thể xảy ra và đưa ra những tư vấn hoặc hành động cần thiết ngay khi phát hiện ra những cuộc tấn công nhằm vào doanh nghiệp của bạn.

3.2. Những mối đe dọa nội bộ

Các biện pháp đảm bảo an toàn thông tin, an ninh mạng thường tập trung vào các mối đe dọa bên ngoài tổ chức hơn là mối đe dọa từ những cá nhân không đáng tin cậy ở bên trong. Các mối

đe dọa nội bộ hiện có xu hướng ngày càng phức tạp và gia tăng mức độ ảnh hưởng đến nhiều ngành nghề, lĩnh vực khác nhau. Theo số liệu của Báo cáo Mối đe dọa nội bộ năm 2020³, 68% tổ chức cho rằng hệ thống của họ dễ bị tấn công bởi yếu tố nội bộ, 63% tổ chức cho rằng người dùng CNTT khi được trao đặc quyền sẽ gây ra rủi ro bảo mật lớn nhất đến các tổ chức.

Có thể thấy, nhân sự nội bộ đặc biệt nguy hiểm vì không giống như những người bên ngoài cần xâm nhập vào tổ chức, họ thường có quyền truy cập hợp pháp vào hệ thống mạng và máy tính mà họ cần để thực hiện công việc hàng ngày. Nếu việc ủy quyền này bị lạm dụng hoặc bị lợi dụng để gây hại cho hệ thống CNTT của cơ quan, tổ chức, hậu quả có thể rất nghiêm trọng, ảnh hưởng đến uy tín và chi phí khắc phục của cơ quan.

Để giảm thiểu các nguy cơ mất an toàn, an ninh thông tin liên quan đến nhân sự nội bộ, một số biện pháp có thể thực thi như:

- Xác định và bảo vệ các tài sản quan trọng: những tài sản này bao gồm sơ đồ thiết kế hệ thống CNTT, cơ sở vật chất, dữ liệu, ứng dụng và con người. Cần hình thành sự hiểu biết toàn diện về các tài sản quan trọng của hệ thống CNTT tại cơ quan, tổ chức cũng như

³ Holger Schulze, Insider Threat Report 2020, Cybersecurity Insider, 2020

đặt ra những câu hỏi: Chúng ta sở hữu những tài sản quan trọng nào? Mức độ ưu tiên hoặc quan tâm của chúng ta đối với tài sản đó là gì? Chúng ta hiểu gì về trạng thái hiện tại của từng tài sản? Từ đó xếp hạng các tài sản theo thứ tự ưu tiên và xác định tình trạng hiện tại của từng tài sản cần bảo vệ. Các tài sản có mức độ ưu tiên cao nhất phải được bảo vệ ở mức cao nhất khỏi các mối đe dọa đến từ nội bộ.

- Thực thi các chính sách: xác định cụ thể các chính sách, quy định, quy chế của doanh nghiệp, tổ chức có thể triển khai, thực thi và tránh gây hiểu nhầm. Mọi người dùng cũng như nhân sự vận hành, quản trị phải quen thuộc với các thủ tục bảo mật, quy chế, quy định của pháp luật cũng như hiểu về các quyền, trách nhiệm và nghĩa vụ của họ đối với công việc hiện tại.

- Thúc đẩy thay đổi văn hóa: đảm bảo an ninh, bảo mật không chỉ về giải pháp kỹ thuật, quy định, quy chế mà còn về thái độ và niềm tin. Để chống lại sự cấu thả và giải quyết các tác nhân gây ra hành vi xấu, cần có giải pháp đào tạo, giáo dục phù hợp các nhân sự nội bộ về các vấn đề bảo mật, hình thành thói quen làm việc đảm bảo an toàn, an ninh và bảo mật thông tin, cũng như những bước cần thực hiện khi xảy ra vi phạm dữ liệu.

3.3. Quy định với người lao động

Một số quy tắc đề cập sau đây có thể tham khảo để đưa vào trong sổ tay nhân viên hoặc quy định đối với người lao động của doanh nghiệp, tổ chức:

- Nhân viên của công ty được kỳ vọng sử dụng công nghệ một cách có trách nhiệm, phù hợp và hiệu quả khi cần thiết để thực hiện trách nhiệm nghề nghiệp của họ.
- Việc sử dụng các thiết bị của công ty, cũng như truy cập Mạng và email của công ty, do công ty cung cấp cho nhân viên, là dành cho các hoạt động liên quan đến công việc. Việc sử dụng cho mục đích cá nhân ở mức tối thiểu được chấp nhận với điều kiện là việc nhân viên sử dụng như vậy không vi phạm bất kỳ quy tắc nào khác được mô tả trong tài liệu này và không cản trở công việc của họ.
- Mỗi nhân viên chịu trách nhiệm đối với bất kỳ phần cứng và phần mềm máy tính nào do công ty cung cấp cho họ, bao gồm cả việc bảo vệ các mục đó khỏi trộm cắp, mất mát hoặc hư hỏng.
- Mỗi nhân viên chịu trách nhiệm về tài khoản của mình do công ty cung cấp, bao gồm cả việc bảo vệ quyền truy cập vào tài khoản.
- Nghiêm cấm nhân viên chia sẻ bất kỳ tài sản nào do công ty cung cấp được sử dụng để xác thực (mật khẩu, thiết bị xác thực phần cứng, mã PIN, v.v.) và chịu trách nhiệm bảo vệ các tài sản đó.
- Nhân viên có trách nhiệm đảm bảo rằng phần mềm bảo mật đang chạy trên tất cả các thiết bị do công ty cung cấp. Nhân viên không được gỡ bỏ hoặc tắt các hệ thống bảo mật đó và

phải thông báo ngay cho bộ phận CNTT của công ty nếu nghi ngờ rằng bất kỳ phần nào của hệ thống bảo mật có thể bị xâm phạm, không hoạt động hoặc trục trặc.

- Nhân viên có trách nhiệm đảm bảo rằng phần mềm bảo mật luôn được cập nhật. Tất cả các thiết bị do công ty trang bị đều bật tính năng Tự động cập nhật; nhân viên không được tắt tính năng này.
- Nhân viên có trách nhiệm cập nhật thiết bị của họ với các bản vá lỗi hệ điều hành, trình điều khiển và ứng dụng mới nhất khi nhà cung cấp phát hành các bản vá lỗi đó.
- Thực hiện bất kỳ hoạt động bất hợp pháp nào cho dù hành vi liên quan có phải là trọng tội, tội nhẹ hoặc vi phạm luật dân sự hay không thì đều bị nghiêm cấm.
- Các tài liệu có bản quyền thuộc về bất kỳ bên nào không phải là công ty thì nhân viên không được lưu trữ hoặc truyền tải mà không được công nhận bằng văn bản của chủ sở hữu bản quyền. Tài liệu mà công ty đã cấp phép có thể được truyền tải theo sự cho phép của các giấy phép liên quan.
- Nghiêm cấm gửi hàng loạt email không mong muốn (thư rác).
- Nghiêm cấm việc sử dụng các nguồn lực của công ty để thực hiện bất kỳ nhiệm vụ nào không phù hợp với sứ mệnh của công ty — ngay cả khi nhiệm vụ đó không trái pháp luật. Điều này bao gồm, nhưng không giới hạn, việc truy cập hoặc

truyền tài liệu khiêu dâm, thô tục, ngôn từ kích động thù địch, tài liệu phi báng, tài liệu phân biệt đối xử, hình ảnh hoặc mô tả bạo lực, đe dọa, bắt nạt trên mạng, tài liệu liên quan đến hack, tài liệu bị đánh cắp, v.v.

- Quy tắc trên không áp dụng cho những nhân viên có công việc đòi hỏi phải làm việc với tài liệu đó, và chỉ áp dụng trong phạm vi cần thiết hợp lý để họ thực hiện nhiệm vụ công việc của mình. Ví dụ: nhân viên chịu trách nhiệm định cấu hình bộ lọc email của công ty có thể gửi email cho nhau mà không vi phạm quy tắc trước đó về việc thêm vào cấu hình bộ lọc các thuật ngữ khác nhau liên quan đến ngôn từ kích động thù địch và thô tục.
- Tất cả việc sử dụng Wi-Fi công cộng với các thiết bị của công ty phải tuân thủ chính sách Wi-Fi công cộng của công ty.
- Nhân viên phải sao lưu máy tính của họ bằng cách sử dụng hệ thống sao lưu của công ty như đã thảo luận trong chính sách sao lưu của công ty.
- Nhân viên không được sao chép hoặc sao lưu dữ liệu từ thiết bị của công ty vào máy tính cá nhân và/hoặc thiết bị lưu trữ của họ.
- Bất kỳ và tất cả mật khẩu cho bất kỳ và tất cả các hệ thống được sử dụng trong công việc của nhân viên phải là duy nhất và không được sử dụng lại trên bất kỳ hệ thống nào khác. Tất cả các mật khẩu phải là mật khẩu mạnh.

- Dữ liệu có thể được mang ra khỏi văn phòng chỉ vì mục đích kinh doanh và phải được mã hóa trước khi xóa. Quy tắc này áp dụng cho dù dữ liệu nằm trên ổ cứng, SSD, CD/DVD, ổ USB hay trên bất kỳ phương tiện nào khác hoặc được truyền qua Mạng. Bất kỳ và tất cả dữ liệu như vậy phải được trả lại cho văn phòng (hoặc hủy theo quyết định riêng của công ty) ngay sau khi hoàn tất việc sử dụng từ xa hoặc sau khi nhân viên chấm dứt việc làm, tùy theo thời điểm nào đến sớm hơn.
- Trong trường hợp xảy ra vi phạm hoặc sự kiện an ninh mạng khác hoặc bất kỳ thảm họa tự nhiên hoặc nhân tạo nào, không nhân viên nào ngoài người phát ngôn được chỉ định chính thức của công ty có thể thay mặt công ty phát biểu trước giới truyền thông.

3.4. Sử dụng dịch vụ An ninh mạng của doanh nghiệp/công ty

Khi doanh nghiệp cân nhắc đến việc tự xây dựng hệ thống An ninh mạng của mình hay theo phương án thuê dịch vụ giám sát an toàn thông tin thì cần xem xét một số vấn đề sau:

Về ưu điểm: Chi phí ban đầu để triển khai hệ thống không lớn; tận dụng được đội ngũ chuyên gia chuyên nghiệp có trình độ cao của doanh nghiệp; được hỗ trợ việc giám sát 24/7/365; dễ dàng mở rộng hay thay đổi công nghệ giám sát theo khả năng cung cấp dịch vụ của doanh nghiệp và không mất nhiều thời gian như hình thức triển khai đầu tư hệ thống.

Về hạn chế: Hiệu quả của hoạt động giám sát phụ thuộc hoàn toàn vào năng lực của bên cung cấp dịch vụ; thông tin giám sát có thể cần gửi về hệ thống giám sát của bên cung cấp dịch vụ tiềm ẩn nguy cơ lộ lọt dữ liệu của hệ thống ra bên ngoài.

Do đó, doanh nghiệp căn cứ vào yêu cầu thực tế của mình để xác định phạm vi cung cấp dịch vụ, yêu cầu cũng như trách nhiệm của mỗi bên.

Việc có đơn vị giám sát sẽ giảm bớt gánh nặng cập nhật phần mềm, tiến hành đào tạo, nâng cao nhận thức cho nhân viên cũng như trong trường hợp một cuộc tấn công ransomware xảy ra hoặc mạng của doanh nghiệp gặp sự cố, họ có thể giảm thời gian chết bằng cách nhanh chóng khôi phục dữ liệu do sử dụng các bản sao lưu thường xuyên và an toàn.

Một số địa chỉ tin cậy tại Việt Nam cung cấp dịch vụ an ninh mạng chúng tôi để trong phần Phụ lục của Sổ tay này.

V. Phát hiện nguy cơ

Việc phát hiện ra nguy cơ ở mỗi lần bị tấn công là một phép thử tốt cho hệ thống an toàn an ninh mà bạn đã xây dựng. Với người dùng cá nhân, nếu hệ thống phòng vệ hoạt động tốt, bạn sẽ được cảnh báo sớm nhất có thể như ngay khi kết nối thiết bị lạ vào máy tính, hoặc khi bạn định tải một tệp tin trên mạng về máy tính. Với các doanh nghiệp thì đó là việc hệ thống duy trì hoạt động tốt, luôn nhận

được cảnh báo và cập nhật, vá lỗi những lỗ hổng hệ thống từ phòng giám sát an ninh của đơn vị hay từ bên cung cấp dịch vụ giám sát.

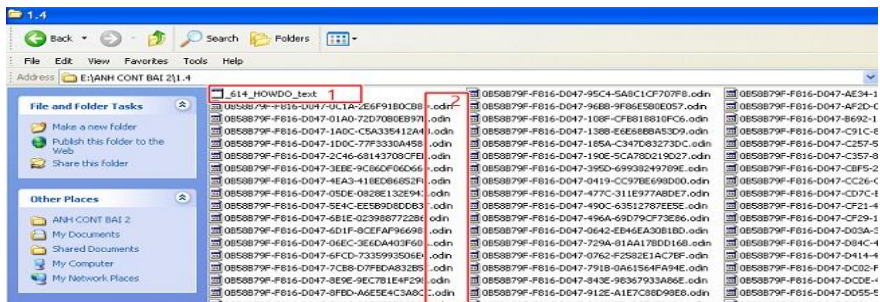
Tuy nhiên, bất chấp những nỗ lực để bảo vệ hệ thống máy tính và dữ liệu, bạn vẫn có thể bị tấn công mạng. Một số dấu hiệu cho thấy hệ thống của bạn đang gặp vấn đề có thể biểu hiện như sau:

1. Mã độc tống tiền

Mã độc là loại virus mã hóa được Bộ Tư pháp Hoa Kỳ xem là mô hình hiện đại của tội phạm mạng với nguy cơ gây tổn thương hệ thống mạng toàn cầu cũng như ảnh hưởng đến nền kinh tế thế giới.

Khi Ransomware lây nhiễm vào máy tính, nó sẽ mã hóa và ngăn chặn người dùng truy cập vào dữ liệu bình thường trên ổ đĩa, để khôi phục hoạt động bình thường trở lại thì nạn nhân phải trả tiền cho tin tặc để đổi lấy mật khẩu để khôi phục lại dữ liệu của họ.

Cơ chế hoạt động của Ransomware là tại mỗi thời điểm khi nó hoạt động trên máy tính của nạn nhân, thì các tệp dữ liệu sẽ bị nó mã hóa thành một định dạng có đuôi khác nhau, khiến cho người dùng tốn nhiều công sức để xác định xem đang bị dính loại Ransomware nào.



Hình 10. Dữ liệu bị mã hóa khi máy tính bị nhiễm Ransomware

Người dùng thường sẽ nhận được thông báo tổng tiền của tin tặc rằng phải trả tiền chuộc cho bọn chúng thông qua bitcoin hoặc một số loại tiền ảo nào đó.



Hình 11. Thông báo tổng tiền của tin tặc trên thiết bị nhiễm Ransomware

Khi có một máy tính có thông báo dạng này thì khả năng cao là nhiều máy tính khác trong hệ thống cũng bị tình trạng tương tự. Ransomware có thể lây lan sang các máy khác hoặc mã hóa các tệp tin dùng trong mạng của tổ chức. Trong một số trường hợp, nó có thể lây lan qua các ranh giới tổ chức để lây nhiễm vào chuỗi cung ứng, khách hàng và các tổ chức khác, tạo nên chuỗi tấn công của tin tặc.

2. Tấn công phá hoại dữ liệu

Bên cạnh hình thức phổ biến là tống tiền, thì có một xu hướng khác đang tăng cao là nhắm đến việc phá hoại dữ liệu của mục tiêu.

Các tác nhân đe dọa có thể sử dụng những kỹ thuật khác nhau để kích hoạt mã độc. Ba cách phổ biến mà chúng sử dụng bao gồm nhắm đến các tệp tin hoặc dữ liệu, sao lưu hệ thống và dữ liệu, và boot hệ thống của hệ điều hành. Trong hầu hết các trường hợp, Wiper nhắm mục tiêu vào các file khôi phục hệ thống cần thiết trước tiên để đảm bảo rằng nạn nhân không có cách nào để khôi phục.

Dấu hiệu của việc bị tấn công wiper là một loạt máy tính đột ngột khởi động lại, sau đó thì nháy liên tiếp và toàn bộ màn hình chuyển sang đen. Các máy tính đã bị khóa và việc khởi động lại máy chỉ đưa về màn hình tối đen như trước. Hiện tượng này lây lan rất nhanh, mỗi phút lại có thêm hàng chục thậm chí hàng trăm máy tính bị nhiễm.

Một số ví dụ về những cuộc tấn công Wiper đã xảy ra trên thế giới như vụ tấn công của mã độc NotPetya vào tập đoàn vận chuyển A.P. Møller-Maersk năm 2017 gây ra thiệt hại khoảng 10 tỷ đô la, hay phát hiện ra mã độc HermeticWiper được sử dụng trong các cuộc tấn công nhằm vào các cơ quan chính phủ cũng như hai ngân hàng quốc doanh lớn nhất của Ukraine tháng 2 năm 2023.

4

3. Những dấu hiệu mơ hồ

Ngoài 2 trường hợp rõ ràng nêu ở trên, thì hầu hết những vụ tấn công mạng thực sự khó phát hiện. Trên thực tế, các doanh nghiệp đã chi hàng triệu đô la mỗi năm chỉ để cố gắng phát hiện sớm việc mình đã bị tấn công đã cho thấy sự khó khăn của việc này.

Dưới đây là một số dấu hiệu mà khi gặp phải bạn có thể nghĩ đến việc thiết bị đã bị dính virus hoặc mã độc (Xin lưu ý là không phải bất kỳ triệu chứng riêng lẻ nào cũng đều do bị tấn công, vì có nhiều lý do khác cũng có thể khiến thiết bị của bạn hoạt động bất thường và có những biểu hiện như chúng tôi mô tả):

- Các chương trình diệt virus bị vô hiệu hóa, bị gỡ bỏ hoặc bị thay đổi cấu hình để bỏ qua một số vấn đề nhất định.

⁴ <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

- Thiết bị bắt đầu gặp sự cố hoặc liên tục khởi động lại.
- Các thiết bị ngoại vi (máy in, máy scan,)
- bật nguồn đột ngột.
- Thiết bị hoạt động như thể có ai đó đang điều khiển nó từ xa.
- Mật khẩu đăng nhập vào thiết bị bị thay đổi.
- Trình duyệt trên thiết bị cố truy cập vào các trang web “lạ”.
- Thiết bị có vẻ chạy chậm hơn trước.
- Thiết bị vào mạng mất nhiều thời gian hơn bình thường.
- Thiết bị thường bị lag, giật khi xem các video phát trực tuyến (do virus, mã độc chiếm mất nhiều RAM và chiếm đường truyền mạng).
- Bạn bè, người thân nhận được những tin nhắn trên các ứng dụng mạng xã hội, email lạ từ phía bạn.
- Xuất hiện những ứng dụng, phần mềm mới trên thiết bị mà bạn không hề cài đặt nó.
- Pin của thiết bị dường như nhanh hết hơn trước.
- Một số phần mềm không chạy được do lỗi thiếu file.
- Trang chủ của trình duyệt web bị thay đổi.

Không thể liệt kê hết tất cả các dấu hiệu do mã độc gây ra cho thiết bị. Vì vậy, nếu bạn nghi ngờ ai đó đang tìm cách xâm nhập vào thiết bị của bạn và thiết bị của bạn có hiện tượng bất thường thì đó có thể là dấu hiệu của sự cố. Bạn cần bình tĩnh và nhanh chóng phản ứng đúng cách những hành vi cố tình xâm phạm này.

Lưu ý: Tóm tắt tổng hợp một số dấu hiệu khác cảnh báo bị tấn công mạng:

- Task Manager không chạy
- Thiết bị vào mạng chậm
- Thiết bị của bạn bắt đầu bị mất liên lạc
- Thiết bị của bạn đang gửi hoặc nhận email lạ
- Thiết bị của bạn đang gửi hoặc nhận tin nhắn văn bản lạ
- Phần mềm mới (bao gồm cả ứng dụng) được cài đặt trên thiết bị
- Pin của thiết bị của bạn dường như cạn kiệt nhanh hơn trước
- Thiết bị của bạn có vẻ chạy nóng hơn trước
- Nội dung tệp tin bị thay đổi
- Bị thiếu file trong hệ thống
- Các trang web xuất hiện hơi khác so với trước đây
- Cài đặt Internet của bạn hiển thị proxy và bạn không bao giờ thiết lập một proxy
- Một số chương trình (hoặc ứng dụng) ngừng hoạt động bình thường
- Các chương trình bảo mật đã tắt
- Tăng cường sử dụng dữ liệu hoặc tin nhắn văn bản (SMS)
- Tăng lưu lượng truy cập mạng
- Công ảo mở bất thường
- Cài đặt ngôn ngữ của thiết bị của bạn đã thay đổi
- Thấy các dấu hiệu vi phạm và/hoặc rò rỉ dữ liệu
- Thiết bị của bạn bắt đầu gặp sự cố

- Hóa đơn điện thoại di động của bạn hiển thị các khoản phí bất ngờ
- Các chương trình không xác định yêu cầu quyền truy cập
- Thiết bị bên ngoài bật nguồn đột ngột
- Thiết bị của bạn hoạt động như thể ai đó đang sử dụng nó
- Công cụ tìm kiếm trình duyệt mới mặc định
- Mật khẩu thiết bị của bạn đã thay đổi
- Cửa sổ tự bật lên yêu cầu thực hiện các lệnh
- Tiện ích trình duyệt mới xuất hiện
- Trang chủ trình duyệt mới không do bạn tạo
- Email của bạn từ thiết bị đang bị bộ lọc thư rác chặn
- Thiết bị của bạn đang cố truy cập các trang web “xấu”
- Bạn đang gặp sự cố gián đoạn dịch vụ bất thường
- Bạn được chuyển đến trang web sai
- Đèn ồ cứng của bạn dường như không bao giờ tắt
- Bạn thấy hoạt động trực tuyến không rõ nguyên nhân
- Thiết bị của bạn đột nhiên khởi động lại

VI. Ứng phó sự cố

1. Hãy bình tĩnh, suy nghĩ và hành động

Phản ứng thông thường khi biết mình bị tấn công mạng là sững sờ, khó chịu, hoảng sợ...nhưng phản ứng đúng đắn lúc này là bạn phải bình tĩnh, suy nghĩ logic, rõ ràng. Thời gian đang chống lại bạn, nên bạn cần phải hành động một cách có lý trí, trật tự.

Hãy tự thuyết phục mình là mọi thứ sẽ ổn, việc này đã được dự tính trước rồi và mình cần làm theo đúng những gì đã chuẩn bị trước đó. Bạn hãy ngăn chặn ai đó đánh cắp dữ liệu, làm hỏng dữ liệu hoặc tấn công các thiết bị bổ sung trên mạng của mình càng sớm càng tốt. Hãy nhớ thứ tự các việc cần làm ngay là:

- Tập trung tìm ra vấn đề.
- Tắt bất kỳ chương trình nào bạn đang sử dụng, lưu mọi tài liệu đang mở vào thiết bị lưu trữ mà bạn sẽ quét virus trước khi sử dụng lại.

2. Hãy tìm một chuyên gia

Tốt nhất, bạn nên nhờ một chuyên gia an ninh mạng giúp bạn khôi phục. Mặc dù chúng tôi cung cấp cho bạn những hướng dẫn hữu ích, nhưng khi nói đến các kỹ năng khôi phục an ninh mạng, đơn giản là không gì có thể thay thế được kinh nghiệm mà một chuyên gia giỏi có được. Tìm kiếm sự trợ giúp chuyên nghiệp khi đối mặt với một cuộc khủng hoảng dữ liệu và máy tính nghiêm trọng cũng giống như việc bạn sẽ làm nếu bất kỳ điều nào sau đây là đúng:

- Nếu ốm bạn sẽ đến bác sĩ hoặc bệnh viện.
- Nếu bạn bị bắt và bị buộc tội, bạn sẽ thuê một luật sư.

Chuyên gia ở đây có thể là một người quen có kinh nghiệm xử lý sự cố an ninh mạng hơn bạn, là người phụ trách an toàn an ninh mạng trong doanh nghiệp, hoặc có thể là bên đối tác phụ trách an toàn an ninh mạng cho công ty. Những người này với kinh nghiệm

đã có chắc chắn sẽ cho bạn những chỉ dẫn phù hợp với trường hợp hiện tại.

3. Trả tiền chuộc

Nếu bạn bị tấn công bởi mã độc tống tiền và bạn đã có bản sao lưu thích hợp, bạn có thể xóa phần mềm tống tiền giống như cách bạn xóa mã độc khác. Nếu bất kỳ dữ liệu nào bị mất trong quá trình này, bạn có thể khôi phục dữ liệu đó từ các bản sao lưu.

Tuy nhiên, nếu bạn đã bị tấn công bởi phần mềm tống tiền và không có bản sao lưu thích hợp, bạn có thể phải đối mặt với một quyết định khó khăn. Rõ ràng, việc bạn trả tiền chuộc cho tội phạm để lấy lại dữ liệu của mình không phải là điều bạn muốn, nhưng trong một số trường hợp, nếu dữ liệu của bạn quan trọng đối với bạn, thì đó có thể là con đường mà bạn cần phải đi.⁵ Trong nhiều trường hợp, bọn tội phạm thậm chí sẽ không trả lại dữ liệu của bạn nếu bạn trả tiền chuộc — vì vậy, bằng cách trả tiền chuộc, bạn không chỉ lãng phí tiền mà còn bị mất dữ liệu vĩnh viễn. Bạn sẽ cần phải quyết định nếu bạn muốn nắm lấy cơ hội đó. (Hy vọng rằng ví dụ này sẽ là động

⁵<https://www.unodc.org/roseap/uploads/documents/ransomaware/english/visual-graphics-en/should-victims-pay-when-they-are-hit-with-ransomware.html>

lực mạnh mẽ để người đọc từ nay sẽ chủ động sao lưu dữ liệu cá nhân định kỳ.)

Trước khi trả tiền chuộc, hãy tham khảo ý kiến của chuyên gia bảo mật thông tin (Tham khảo Phụ lục). Một số phần mềm tổng tiền có thể bị xóa và hoàn tác bằng các công cụ bảo mật khác nhau. Tuy nhiên, trừ khi phần mềm bảo mật của bạn cho bạn biết rằng nó có thể hoàn tác quá trình mã hóa do phần mềm tổng tiền thực hiện, đừng cố tự xóa phần mềm tổng tiền sau khi phần mềm này đã mã hóa dữ liệu của bạn. Một số phần mềm tổng tiền nâng cao sẽ xóa dữ liệu vĩnh viễn nếu phát hiện nỗ lực giải mã dữ liệu. Ngoài ra, hãy nhớ rằng một số phần mềm tổng tiền nâng cao không mã hóa dữ liệu mà xóa dữ liệu đó khỏi thiết bị của nạn nhân

Lưu ý: Ứng phó

- Bình tĩnh để xử lý sự cố một cách khôn ngoan.
- Thông báo cho nhân viên CNTT để tìm ra các vấn đề và việc cần phải làm để khắc phục mà không làm hỏng thêm hệ thống/phần mềm/công cụ
- Tìm một chuyên gia CNTT chuyên nghiệp.
- Trả tiền chuộc nhưng thông báo cho cảnh sát về vụ việc này.
- Cập nhật hệ thống bảo mật cho các mạng.
- Thay đổi hành vi sử dụng mạng xã hội;
- Liên hệ với các công ty an ninh mạng chuyên nghiệp để xác định và khắc phục sự cố.

và chỉ truyền lại dữ liệu nếu tiền chuộc được trả. Phần mềm bảo mật có thể gỡ bỏ phần mềm tống tiền như vậy, nhưng phần mềm bảo mật thường không thể khôi phục dữ liệu bị phần mềm tống tiền đánh cắp.

Cách bảo vệ tốt nhất cho người dùng trước tác động của ransomware là sao lưu và giữ cho các bản sao lưu không kết nối với bất kỳ thứ gì khác!

4. Rút kinh nghiệm cho tương lai

Điều quan trọng là phải học hỏi từ các sự cố. Nếu bạn có thể tìm ra điều gì đã xảy ra và cách tin tặc xâm nhập được vào hệ thống của bạn (trực tiếp hoặc bằng cách sử dụng mã độc), thì bạn có thể tự thiết lập các chính sách và quy trình thực tế để ngăn chặn những hành vi xâm phạm như vậy trong tương lai. Hoặc một chuyên gia an ninh mạng có thể giúp bạn làm như vậy.

VII. Khôi phục hệ thống

Dù vấn đề sự cố xảy ra trên thiết bị cá nhân, hay là xảy ra trên hệ thống thiết bị của doanh nghiệp thì việc xử lý sự cố để khôi phục lại hiện trạng được gần nhất với trước khi xảy ra sự cố tấn công mạng là điều mà ai cũng mong muốn. Nếu có một chuyên gia trợ giúp bạn hoàn toàn việc này là tốt nhất, nhưng chúng tôi cũng giới thiệu một số bước thực hiện với những trường hợp xảy ra trên thiết bị cá nhân là ví dụ để bạn hiểu quy trình xử lý việc này.

1. Khôi phục lại thiết bị khi không có trợ giúp của chuyên gia

Nếu bạn chưa thể tìm ngay được một chuyên gia, các bước sau đây là những bước bạn nên làm theo. Các bước này về cơ bản là những bước mà hầu hết các chuyên gia sẽ làm:

- Bước 1: Tìm hiểu điều gì đã xảy ra hoặc đang xảy ra.
- Bước 2: Ngăn chặn cuộc tấn công.
- Bước 3: Chấm dứt và loại bỏ cuộc tấn công.

Cụ thể các thao tác cần làm trong từng bước sẽ được trình bày chi tiết dưới đây.

1.1. Bước 1: Tìm hiểu điều gì đã hoặc đang xảy ra

Hãy thu thập càng nhiều thông tin càng tốt (nhưng đừng dành quá nhiều thời gian cho bước này) về:

- Chuyện gì đã xảy ra?
- Hệ thống thông tin và cơ sở dữ liệu nào bị tấn công?
- Tội phạm hoặc những đối tượng khác có thể làm gì với tài liệu bị đánh cắp?
- Những dữ liệu và chương trình nào đã bị ảnh hưởng?
- Ai, ngoài bạn, có thể gặp rủi ro do vi phạm (điều này bao gồm bất kỳ tác động tiềm tàng nào đối với doanh nghiệp của bạn)

1.2. Bước 2: Ngăn chặn cuộc tấn công

Chặn tin tặc bằng cách cách ly họ khỏi các thiết bị bị xâm nhập bằng cách kiểm tra theo danh sách sau:

- Cắt tất cả kết nối mạng càng sớm càng tốt: Để chấm dứt kết nối mạng cho tất cả các thiết bị trên mạng, hãy tắt bộ định tuyến của bạn bằng cách rút phích cắm. (Lưu ý: Nếu bạn đang ở trong môi trường kinh doanh, bước này thường không thực hiện được.)
- Rút bất kỳ cáp Ethernet nào: Tuy nhiên, hãy hiểu rằng một cuộc tấn công qua mạng có thể đã lan sang các thiết bị khác trên mạng. Nếu vậy, hãy ngắt kết nối mạng khỏi Mạng và ngắt kết nối từng thiết bị khỏi mạng của bạn cho đến khi thiết bị được quét để tìm các vấn đề bảo mật.
- Tắt Wi-Fi trên thiết bị bị nhiễm: Một lần nữa, cuộc tấn công từ mạng có thể đã lan sang các thiết bị khác trên mạng. Nếu vậy, hãy ngắt kết nối mạng khỏi Mạng và ngắt kết nối từng thiết bị khỏi mạng của bạn bằng cách tắt Wi-Fi tại bộ định tuyến và mọi điểm truy cập, không chỉ trên máy tính bị nhiễm.
- Tắt dữ liệu di động: Nói cách khác, hãy đặt thiết bị của bạn ở chế độ trên máy bay.
- Tắt Bluetooth và NFC: Bluetooth và NFC đều là công nghệ giao tiếp không dây hoạt động với các thiết bị ở gần nhau.

Tất cả các thông tin liên lạc như vậy sẽ bị chặn nếu có khả năng lây nhiễm hoặc tin tặc nhảy từ thiết bị này sang thiết bị khác.

- Rút ổ USB và các ổ di động khác khỏi hệ thống: Hãy lưu ý là các ổ đĩa có thể chứa mã độc, vì vậy đừng dính kèm chúng vào bất kỳ hệ thống nào khác.
- Thu hồi mọi quyền truy cập mà tin tặc đang khai thác: Nếu bạn có một thiết bị dùng chung và tin tặc đang sử dụng một tài khoản khác với tài khoản của bạn mà bằng cách nào đó chúng đã có được quyền truy cập được phép, hãy tạm thời đặt tài khoản đó thành không có quyền làm bất cứ điều gì

Nếu vì lý do nào đó, bạn cần truy cập Mạng từ thiết bị của mình để quét virus, hãy tắt tất cả các thiết bị khác trong mạng của bạn để ngăn chặn bất kỳ cuộc tấn công nào lây lan qua mạng đến thiết bị của bạn.

1.3. Bước 3: Châm dứt và loại bỏ cuộc tấn công

Ngăn chặn một cuộc tấn công không giống như châm dứt và loại bỏ một cuộc tấn công. Ví dụ: mã độc có trên thiết bị bị nhiễm vẫn tồn tại sau khi ngắt kết nối thiết bị khỏi Mạng, cũng như bất kỳ lỗ hổng nào mà tin tặc hoặc mã độc từ xa có thể đã khai thác để chiếm quyền kiểm soát thiết bị của bạn. Vì vậy, sau khi ngăn chặn cuộc tấn công, điều quan trọng là phải làm sạch hệ thống.

Các phần sau đây mô tả một số bước cần thực hiện tại thời điểm này:

- **Khởi động máy tính**
- **Sao lưu dữ liệu**

Nếu gần đây bạn chưa sao lưu dữ liệu của mình, hãy thực hiện ngay bây giờ. Tất nhiên, việc sao lưu thiết bị bị xâm nhập không nhất thiết sẽ lưu tất cả dữ liệu của bạn (vì một số dữ liệu có thể đã bị hỏng hoặc bị thiếu), nhưng nếu bạn chưa có bản sao lưu, hãy thực hiện ngay bây giờ — lý tưởng nhất là sao chép tệp của bạn sang thiết bị khác (như ổ USB lưu trữ bên ngoài) cho đến khi nó được phần mềm bảo mật quét đúng cách.

- **Xóa rác (tùy chọn)**

Tại thời điểm này, bạn nên xóa bất kỳ tệp nào mà bạn không cần, bao gồm cả những tệp dữ liệu tạm thời mà đã lâu bạn không dùng đến.

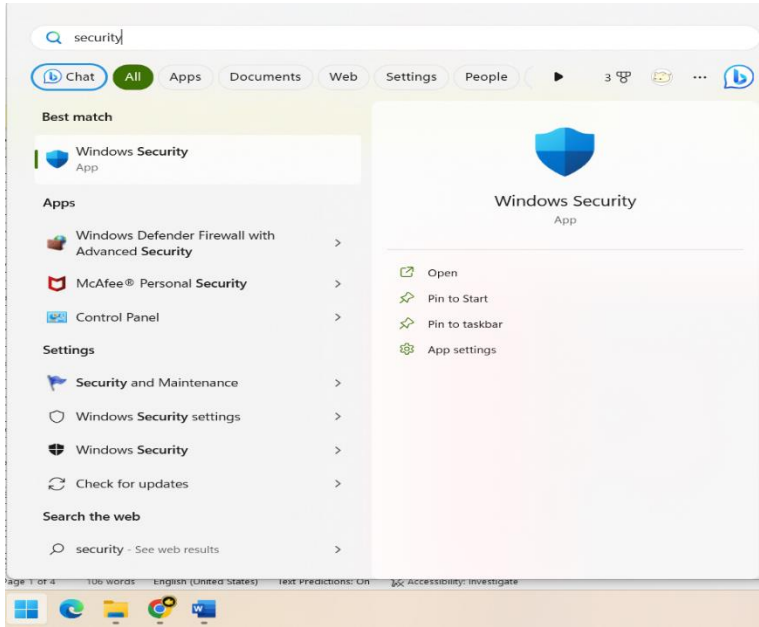
Bạn nên tiến hành bảo trì dữ liệu định kỳ, và nếu bạn đang cần dọn dẹp máy tính của mình thì bây giờ là thời điểm thích hợp. Càng ít tệp tin trong máy thì phần mềm diệt virus sẽ chạy càng nhanh. Ngoài ra, một số mã độc thường ẩn trong các tệp dữ liệu tạm thời, do đó, việc xóa các tệp đó cũng có thể trực tiếp xóa một số mã độc.

Đối với người dùng máy tính Windows, một cách dễ dàng để xóa các tệp tạm thời là sử dụng tiện ích Disk Cleanup tích hợp sẵn:

1. Trong hệ điều hành Windows 10, trong hộp thoại Search trên thanh taskbar, gõ cú pháp “disk cleanup”.
 2. Hãy chọn Disk Cleanup trong danh sách kết quả
 3. Chọn ổ đĩa bạn muốn làm sạch và chọn OK.
 4. Chọn các loại tệp tin mà bạn muốn và chọn OK.
 5. Chọn Accessories (hoặc Windows Accessories).
 6. Chọn Disk Cleanup.
- **Chạy phần mềm diệt virus**

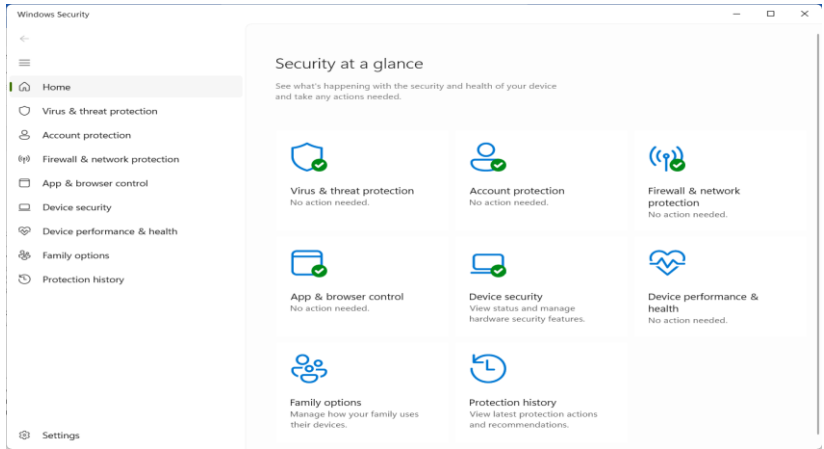
Nếu bạn đã cài phần mềm diệt virus nào đó, hãy chạy và quét toàn bộ hệ thống. Nếu bạn chưa từng cài bất kỳ phần mềm diệt virus nào, hãy sử dụng luôn **Microsoft Security** có sẵn trên máy.

Bước 1: Đầu tiên hãy click vào biểu tượng **Start** tại góc trái màn hình. Sau đó, tìm chọn công cụ **Windows Security** trong thanh tìm kiếm phía dưới của màn hình.



Hình 12.Cách khởi động ứng dụng Windows Security

Bước 2: Trên cửa sổ sẽ hiện một tab tên Security at a glance, chọn mục Virus & threat protection.



Hình 13. Giao diện của ứng dụng Windows Security

Bước 3: Tiếp theo, tiếp tục nhấp vào **Scan options** như hình bên dưới.



Hình 14. Cách để tìm lựa chọn quét virus

Bước 4: Sau đó, hãy đánh dấu vào mục thứ tư Microsoft Defender Antivirus (offline scan) rồi nhấn nút Scan now để bắt đầu tiến trình quét virus trên máy.

Quick scan
Checks folders in your system where threats are commonly found.

Full scan
Checks all files and running programs on your hard disk. This scan could take longer than one hour.

Custom scan
Choose which files and locations you want to check.

Microsoft Defender Antivirus (offline scan)
Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Antivirus (offline scan) can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

Scan now

Chờ một thời gian để phần mềm tiến hành quá trình quét. Nếu mã độc được phát hiện, Microsoft Security sẽ đề xuất các cách xử lý vấn đề. Người dùng nên làm theo các khuyến nghị để được xử lý đúng cách.

Một cảnh báo quan trọng: Bản thân phần mềm bảo mật chạy trên thiết bị bị xâm nhập có thể bị xâm phạm hoặc bất lực trước mối đe dọa liên quan (xét cho cùng, vi phạm bảo mật đã xảy ra với phần mềm bảo mật đang chạy), vì vậy, bất kể quá trình quét đó có sạch hay không, bạn nên chạy phần mềm diệt virus từ ổ đĩa khởi

động hoặc ổ đĩa cứu hộ khác, hoặc, trong trường hợp của một số sản phẩm, từ một máy tính khác trong mạng nội bộ của bạn.

Không phải tất cả các phần mềm diệt virus đều bắt được tất cả các biến thể của mã độc. Các chuyên gia bảo mật thực hiện “dọn dẹp” thiết bị thường chạy nhiều phần mềm bảo mật từ nhiều nhà cung cấp khác nhau.

- **Cài đặt lại phần mềm bị hỏng**

Bạn nên gỡ và cài đặt lại bất kỳ phần mềm nào mà bạn thấy nó bị ảnh hưởng sau khi bị tấn công, ngay cả khi phần mềm bảo mật đã sửa nó.

- **Khởi động lại hệ thống và chạy bản quét virus mới nhất**

Đối với máy tính Windows, sau khi bạn đã làm sạch hệ thống, hãy khởi động lại hệ thống ở chế độ “Safe mode with Networking” toàn bộ quy trình được mô tả ở trên (thay vì chế độ Safe Mode), chạy phần mềm diệt virus, tải xuống tất cả các bản cập nhật và chạy phần mềm bảo mật để rà quét lại.

Nếu không có bản cập nhật nào thì bạn không cần chạy lại phần mềm quét virus.

Nếu bạn đang sử dụng máy Mac, Safe Boot đã bao gồm kết nối mạng nên không cần thực hiện bước này.

Cài đặt tất cả các bản cập nhật và bản vá lỗi có liên quan. Nếu bất kỳ phần mềm nào của bạn chưa được cập nhật lên phiên bản

mới nhất và có thể chứa lỗi hỏng, hãy cập nhật phần mềm này trong quá trình dọn dẹp.

Nếu bạn có thời gian, hãy chạy lại toàn bộ phần mềm bảo mật sau khi bạn đã cài đặt tất cả các bản cập nhật.

– **Xóa tất cả các điểm System Restore có thể có vấn đề**

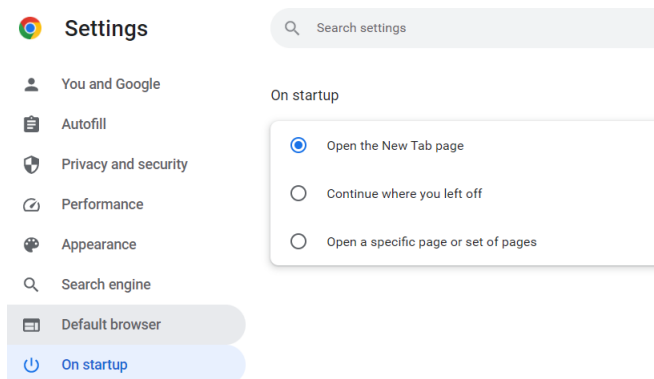
System Restore là một công cụ hữu ích, nhưng nó cũng có thể nguy hiểm. Ví dụ: nếu một hệ thống tạo điểm khôi phục khi mã độc đang chạy trên thiết bị, việc khôi phục điểm đó có thể sẽ khôi phục mã độc! Do đó, sau khi dọn dẹp hệ thống, hãy nhớ xóa tất cả các điểm khôi phục hệ thống có thể đã được tạo khi hệ thống của bạn bị xâm phạm. Nếu bạn không chắc liệu điểm khôi phục có thể có vấn đề hay không, hãy xóa nó. Đối với hầu hết người dùng, điều này có nghĩa là có thể tốt để xóa tất cả các điểm System Restore.

Các bước để thực hiện:

1. Nhấp vào menu Start.
2. Nhấp vào Control Panel.
3. Nhấp vào All Control Panel Items.
4. Chọn Recovery.
5. Chọn Configure System Restore.
6. Thực hiện theo hướng dẫn để xóa những điểm system restore đã có.

– Khôi phục cài đặt đã sửa đổi

Một số tin tặc và mã độc có thể sửa đổi các cài đặt khác nhau trên thiết bị của bạn. Một trong những phần hay bị thay đổi nhất là phần Homepage của trình duyệt vì phần Startup của trình duyệt khi bị thay đổi sẽ có thể mở đến phần cài đặt lại mã độc hoặc thực hiện một số tác vụ bất chính khác. Vì thế bạn nên vào trình duyệt và thay đổi lại thành địa chỉ an toàn.



Hình 15.Cách thiết lập lại trang nhà trên trình duyệt Chrome

Khi sử dụng các phiên bản trình duyệt khác nhau, quy trình sẽ hơi khác một chút nhưng có thể dễ dàng thực hiện khi bạn tìm kiếm hướng dẫn trên Google.

– Cài đặt lại toàn bộ thiết bị

Đôi khi, thay vì tuân theo các quy trình đã nói ở trên, cài đặt lại toàn bộ thiết bị từ đầu sẽ dễ dàng hơn. Trên thực tế, do nguy cơ phần mềm bảo mật thiếu một số vấn đề hoặc lỗi của người dùng khi thực hiện dọn dẹp bảo mật, nhiều chuyên gia khuyên rằng bất cứ khi nào có thể, người dùng nên cài đặt lại toàn bộ thiết bị sau khi bị tấn công. Tuy nhiên, ngay cả khi bạn định cài đặt lại hết tất cả, trước hết bạn vẫn nên quét virus toàn bộ thiết bị vì có một số dạng mã độc hiếm gặp có thể tồn tại ngay cả sau khi khôi phục (chẳng hạn như mã độc lập trình lại BIOS, một số virus nằm ở phần boot hệ thống, v.v.) và nên rà quét tất cả các thiết bị trên cùng một mạng với thiết bị bị xâm nhập tại thời điểm xâm nhập hoặc sau đó, để đảm bảo rằng virus không lây lan trên thiết bị mới được cài lại.

2. Cách xử lý thông tin bị đánh cắp

Nếu máy tính, điện thoại hoặc máy tính bảng của bạn bị xâm phạm, có thể thông tin nhạy cảm trên đó đã bị đánh cắp và bị tội phạm sử dụng sai mục đích.

Bạn nên thay đổi lại tất cả các mật khẩu được lưu trữ trên thiết bị và kiểm tra lại tất cả các tài khoản có thể truy cập từ thiết bị mà không cần đăng nhập (do đã cài đặt trước đó trên thiết bị thành “Remember Me” sau khi đăng nhập thành công) để đảm bảo rằng không hề sai sót. Vì nếu mật khẩu của bạn được lưu trữ ở định dạng

được mã hóa mạnh thì nhu cầu thay đổi mật khẩu sẽ ít cấp bách hơn là nếu được lưu trữ ở dạng văn bản rõ ràng hoặc mã hóa yếu, nhưng lý tưởng nhất là trừ khi bạn chắc chắn rằng mã hóa sẽ tồn tại lâu dài. Nếu đã không đảm bảo chắc chắn thì bạn nên thay đổi mật khẩu.

Nếu bạn nghi ngờ rằng thông tin có thể đã bị đánh cắp và có thể được sử dụng để mạo danh bạn, bạn nên báo cáo với cơ quan công an và giữ lại các giấy tờ liên quan. Ví dụ, nếu bạn bị cảnh sát chặn lại và thông báo rằng có lệnh bắt giữ bạn ở một nơi nào đó mà bạn chưa từng đến, thì bạn sẽ có bằng chứng rằng bạn đã báo cáo về việc thông tin của bạn bị đánh cắp.

Nếu bạn tin rằng thông tin thẻ tín dụng hoặc thẻ ghi nợ của mình đã bị đánh cắp, hãy liên hệ với Ngân hàng nơi bạn mở thẻ để yêu cầu khóa thẻ cũ và cấp thẻ mới. Ngoài ra, hãy kiểm tra tài khoản xem có giao dịch đáng ngờ nào không.

Ghi nhật ký mọi cuộc gọi bạn thực hiện, thời điểm bạn thực hiện, bạn đã nói chuyện với ai và những gì diễn ra trong cuộc gọi.

Thông tin đó càng nhạy cảm thì việc hành động và xử lý nhanh chóng càng quan trọng.

Dưới đây là lời khuyên về xử lý thông tin bị lấy cắp:

Loại 1: Thông tin không riêng tư, nhưng có thể giúp bạn tội phạm đánh cắp danh tính:

- Tên, địa chỉ và số điện thoại nhà riêng: Loại thông tin này thực sự có sẵn cho bất kỳ ai muốn nó, thậm chí không cần hack bạn. Nhưng loại thông tin này có thể được sử dụng kết hợp với các thông tin khác để thực hiện mọi loại tội phạm, đặc biệt là nếu người khác không nghi ngờ gì mắc lỗi (ví dụ: bằng cách cho phép ai đó có thông tin này mở thẻ thư viện mà không cần xuất trình giấy tờ tùy thân).
- Thông tin hồ sơ công khai khác: Giá mà bạn đã trả cho ngôi nhà của mình, tên của các con bạn, v.v. Mặc dù thông tin này là hồ sơ công khai, nhưng tội phạm liên hệ thông tin đó với thông tin khác có thể lấy được từ máy tính của bạn có thể gây ra sự cố cho bạn.

Loại 2: Thông tin nhạy cảm như địa chỉ email, số điện thoại di động, số tài khoản thẻ tín dụng không có mã CVC, số tài khoản thẻ ghi nợ yêu cầu mã PIN để sử dụng hoặc không có mã CVC, số thẻ ATM, số thẻ sinh viên, số hộ chiếu, ngày sinh đầy đủ bao gồm cả năm, và như thế. Những mục này tạo ra rủi ro bảo mật khi bị xâm phạm — ví dụ: địa chỉ email bị đánh cắp có thể dẫn đến các cuộc tấn công lừa đảo tinh vi sử dụng thông tin khác thu thập được từ máy tính của bạn, cố gắng xâm nhập vào tài khoản, gửi thư rác, v.v. Ngoài ra, loại thông tin bị đánh cắp này có thể được tội phạm sử dụng như một phần của hành vi trộm cắp danh tính và tội phạm gian lận tài chính, nhưng có thể yêu cầu kết hợp nhiều phần thông tin để tạo ra rủi ro nghiêm trọng.

Loại 3: Thông tin rất nhạy cảm như mật khẩu của tài khoản trực tuyến, số tài khoản ngân hàng, mã PIN, thẻ tín dụng và thẻ ghi nợ, câu trả lời cho các câu hỏi thử thách mà bạn đã sử dụng để bảo mật tài khoản, v.v. Những loại thông tin này thường có thể bị lạm dụng ngay khi chúng sở hữu nó.

VIII. Tổng kết

Trong cuốn sổ tay này, chúng tôi đã trình bày những kiến thức cơ bản mà mọi người cần biết về an toàn thông tin. Những kiến thức này có mức độ từ dễ đến khó, yêu cầu từ thấp lên cao:



1. Vấn đề đầu tiên và quan trọng nhất là **nhận thức**, xác định được các nguy cơ, rủi ro.
2. Trên cơ sở đó, phải xây dựng các biện pháp **phòng vệ**.
3. Luôn luôn cảnh giác cao độ để kịp thời **phát hiện** các vấn đề phát sinh.
4. Có sự phối hợp chặt chẽ giữa các bên, các bộ phận để có thể **ứng phó** với những sự cố xảy ra
5. Có đủ năng lực để **khôi phục** lại hệ thống và sớm trở lại hoạt động bình thường.

Hi vọng những kiến thức mà chúng tôi đã cung cấp trong cuốn sổ tay này sẽ là hành trang đồng hành cùng các bạn trong quá trình sống và làm việc trên môi trường số.

Cuối cùng, dù bạn đã hiểu và hoàn toàn làm được tất cả mọi điều được trình bày trong cuốn sổ tay này, chúng tôi mong rằng bạn sẽ duy trì thói quen theo dõi các tin tức về hướng dẫn an toàn thông tin trên những kênh truyền thông chính thống (đài truyền hình, các trang thông tin của chính phủ, bộ, ban ngành). Công nghệ thông tin luôn thay đổi và việc thường xuyên cập nhật những kiến thức này sẽ giúp bạn có thêm nhiều hiểu biết, kinh nghiệm và luôn tự tin trên môi trường Mạng.

Chúc bạn và tổ chức của bạn luôn tham gia không gian mạng một cách an toàn!

IX. Phụ lục

1. Pháp luật của Việt Nam về an toàn thông tin, an ninh mạng

Luật An toàn thông tin mạng được Quốc hội thông qua vào tháng 11 năm 2015 và chính thức có hiệu lực từ ngày 01/7/2016 và Luật An ninh mạng được Quốc hội thông qua vào tháng 6 năm 2018 và chính thức có hiệu lực từ ngày 01/01/2019. Đây là các cơ sở pháp lý quan trọng cho việc quản lý các hoạt động liên quan đến an toàn, an ninh thông tin ở Việt Nam. Ngoài Luật An toàn thông tin mạng và Luật An ninh mạng, đã có nhiều văn bản có liên quan đến công nghệ thông tin và an toàn thông tin được Quốc hội, Chính phủ và các cơ quan nhà nước ban hành như:

- Luật công nghệ thông tin số 67/2006/QH11 của Quốc hội, ngày 12/07/2006.
- Nghị định số 90/2008/NĐ-CP của Chính phủ “Về chống thư rác”, ngày 13/08/2008.
- Quyết định số 59/2008/QĐ-BTTTT của Bộ Thông tin và Truyền thông “Ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số”, ngày 31/12/2008.
- Quyết định 63/QĐ-TTg của Thủ tướng Chính phủ “Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020”, ngày 13/01/2010.

- Chỉ thị số 897/CT-TTg của Thủ tướng Chính phủ “V/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số”, 10/06/2011.
- Thông tư số 23/2011/TT-BTTTT của Bộ TT&TT “Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước”, ngày 11/08/2011.
- Nghị định số 77/2012/NĐ-CP của Chính phủ “Sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 của Chính phủ về chống thư rác”, ngày 05/10/2012.
- Nghị định 72/2013/NĐ-CP của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ Mạng và thông tin trên mạng; quy định về việc chia sẻ thông tin trên các trang mạng xã hội.

1.1. Luật An toàn thông tin mạng

Luật An toàn thông tin mạng là bộ luật đầy đủ đầu tiên của Việt Nam về an toàn thông tin được Quốc hội khóa XIII thông qua tại Phiên họp thứ 10 vào ngày 19/12/2015 và chính thức có hiệu lực từ ngày 01/7/2016. Luật quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin

mạng; quản lý nhà nước về an toàn thông tin mạng. Đối tượng áp dụng của luật là các cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin mạng tại Việt Nam.

Luật An toàn thông tin mạng gồm 8 chương và 54 điều với nội dung chính như sau:

- Chương I – Những quy định chung gồm 8 điều quy định phạm vi điều chỉnh, đối tượng áp dụng của luật; giải thích các từ ngữ, thuật ngữ; nêu nguyên tắc bảo đảm an toàn thông tin mạng, chính sách của Nhà nước và vấn đề hợp tác quốc tế về an toàn thông tin mạng.
- Chương II – Bảo đảm an toàn thông tin mạng gồm 21 điều quy định về các vấn đề bảo vệ thông tin mạng, bảo vệ thông tin cá nhân, bảo vệ hệ thống thông tin và ngăn chặn xung đột thông tin trên mạng.
- Chương III – Mật mã dân sự gồm 7 điều quy định về các vấn đề có liên quan đến mật mã dân sự, bao gồm kinh doanh, xin cấp giấy phép kinh doanh, xuất khẩu nhập khẩu, sử dụng sản phẩm, dịch vụ mật mã dân sự.
- Chương IV – Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng gồm 3 điều quy định quản lý tiêu chuẩn, quy chuẩn kỹ thuật, đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng.

- Chương V – Kinh doanh trong lực vực an toàn thông tin mạng gồm 7 điều quy định về việc cấp giấy phép kinh doanh sản phẩm dịch vụ và quản lý nhập khẩu sản phẩm an toàn thông tin mạng.
- Chương VI – Phát triển nguồn nhân lực an toàn thông tin mạng gồm 2 điều quy định về đào tạo, bồi dưỡng nghiệp vụ và văn bằng, chứng chỉ đạo tạo về an toàn thông tin mạng.
- Chương VII – Quản lý nhà nước về an toàn thông tin mạng gồm 2 điều quy định các nội dung và trách nhiệm quản lý nhà nước về an toàn thông tin mạng.
- Chương VIII – Điều khoản thi hành gồm 2 điều quy định ngày bắt đầu có hiệu lực của luật và giao chính phủ và các cơ quan nhà nước ban hành các văn bản hướng dẫn chi tiết việc thực hiện.

1.2. Luật An ninh mạng

Tiếp theo Luật An toàn thông tin mạng, Luật An ninh mạng được Quốc hội khóa XIV thông qua tại Phiên họp thứ 5 vào ngày 12/6/2018 và chính thức có hiệu lực từ ngày 01/01/2019 [18]. Luật gồm 7 chương, 43 điều quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Nội dung tóm tắt của luật như sau:

- Chương I – Những quy định chung gồm 9 điều quy định phạm vi điều chỉnh, đối tượng áp dụng của luật; giải thích các từ ngữ, thuật ngữ; nêu nguyên tắc, biện pháp bảo vệ an ninh mạng, chính sách của Nhà nước và vấn đề hợp tác quốc tế về an ninh mạng; quy định các hành vi bị nghiêm cấm và xử lý vi phạm pháp luật về an ninh mạng.¹⁵⁴
- Chương II – Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia gồm 6 điều quy định về các vấn đề thẩm định, đánh giá điều kiện, kiểm tra, giám sát và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.
- Chương III – Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng gồm 7 điều quy định các vấn đề phòng ngừa và xử lý các hành vi xâm phạm an ninh mạng, bao gồm phòng ngừa và xử lý các hành vi tuyên truyền chống nhà nước, kích động bạo loạn, gây rối,...; phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, quyền riêng tư của cá nhân; phòng, chống tấn công, khủng bố và các tình huống nguy hiểm trên mạng; và vấn đề đấu tranh bảo vệ an ninh mạng.
- Chương IV – Hoạt động bảo vệ an ninh mạng gồm 7 điều quy định về vấn đề bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, hệ thống thông tin của các cơ quan tổ chức; bảo đảm an ninh thông tin trên không gian mạng; vấn đề nghiên cứu, phát triển và nâng cao năng lực tự

chủ về an ninh mạng; và vấn đề bảo vệ trẻ em trên không gian mạng.

- Chương V – Bảo đảm hoạt động bảo vệ an ninh mạng gồm 6 điều quy định về lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng, tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; vấn đề giáo dục, bồi dưỡng kiến thức, nghiệp vụ và phổ biến kiến thức an ninh mạng; và vấn đề kinh phí bảo vệ an ninh mạng.
- Chương VI – Trách nhiệm của cơ quan, tổ chức, cá nhân quy định trách nhiệm của các chủ thể trong đảm bảo an ninh mạng, bao gồm trách nhiệm của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, chính quyền các tỉnh, thành phố, các tổ chức và cá nhân.
- Chương VII – Điều khoản thi hành gồm 1 điều quy định ngày bắt đầu có hiệu lực của luật và yêu cầu về điều kiện an ninh mạng đối với hệ thống thông tin đang vận hành, sử dụng được đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

2. Những địa chỉ đào tạo và cung cấp nguồn nhân lực về an ninh mạng

Hiện tại ở Việt Nam có 8 đơn vị uy tín đào tạo bậc đại học có ngành An toàn thông tin, đó là:

- Đại học Bách khoa Hà Nội (BKHN) – ngành Kỹ thuật máy tính
- Đại học Công nghệ – Đại học Quốc gia Hà Nội (UET) – ngành Mạng máy tính và truyền thông dữ liệu
- Học viện Công nghệ Bưu chính Viễn thông (PTIT) – ngành An toàn thông tin
- Học viện Kỹ thuật mật mã (KMA) – ngành An toàn thông tin
- Học viện Kỹ thuật Quân sự (MTA) – ngành An toàn thông tin
- Học viện An ninh nhân dân (ANND) – ngành An toàn thông tin
- Đại học Bách khoa Đà Nẵng (DUT) – ngành An toàn thông tin
- Đại học CNTT – ĐHQG TP HCM (UIT) – ngành An toàn thông tin

Đây là những nguồn cung cấp nhân lực có chất lượng cao, được đào tạo bài bản và có trình độ cao.

Ngoài ra, các doanh nghiệp có thể lựa chọn tổ chức các khoá đào tạo nâng cao nhận thức và trình độ cho cán bộ công nhân viên trong cơ quan, hoặc cá nhân có nhu cầu nâng cao trình độ chuyên sâu về ATTT có thể đăng kí các khoá đào tạo chuyên sâu về An ninh mạng tại một số công ty, tổ chức sau:

ST T	Tên tổ chức	Website	Đánh giá
1	Công ty BKAV	bkav.com.vn	Ngoài các bộ phần mềm diệt virus nổi tiếng thương hiệu BKAV, công ty BKAV còn cung cấp các giải pháp, dịch vụ an ninh mạng, đào tạo và xây dựng hệ thống mô phỏng cho học viên.
2	Công ty Cổ phần An ninh mạng Việt Nam VSEC	vsec.com.vn	Đây là một trong những đơn vị cung cấp dịch vụ ATTT uy tín tại Việt Nam. Công ty có tổ chức các chương trình đào tạo có lý thuyết và thực hành trên hệ thống giả lập để tăng cường khả năng phản ứng và xử lý sự cố ATTT cho học viên, tổ chức.
3	VNPT-IT	https://vnptit.vn/dich-vu-ao-tao-an-toan-thong-tin	Công ty Công nghệ thông tin VNPT cung cấp nhiều giải pháp, dịch vụ đánh giá, tư vấn, đảm bảo An toàn thông tin và đào tạo An toàn thông tin cho các đơn vị tổ chức.
4	Công Ty TNHH Tư Vấn và Đào Tạo Netpro	netpro.com.vn	Các khoá đào tạo Security gồm có EC-Council, CompTIA Security+, SCP
5	Hiệp hội ATTT Việt	www.vnisa.org.vn	Đây là nơi tập hợp các cá nhân, tổ chức làm công tác nghiên cứu giảng dạy, ứng dụng và phát triển

	Nam VNISA		ATTT nhằm hướng dẫn thực hiện các chủ trương đường lối của nhà nước trong việc ứng dụng và phát triển kỹ thuật, công nghệ, ATTT, đưa ra đề xuất, khuyến nghị với cơ quan quản lý nhà nước trong việc xây dựng cơ chế chính sách phát triển ngành. Hiệp hội còn tổ chức một số khoá đào tạo cấp chứng chỉ CISSP cho các chuyên gia bảo mật.
6	Công ty Cổ phần Qnet	qnet.edu.vn	Cung cấp 1 số khoá học về An toàn an ninh.

3. Mạng lưới nhà cung cấp dịch vụ an ninh mạng / cung cấp dịch vụ phòng vệ và bảo mật hệ thống mạng tại Việt Nam

ST T	Tên tổ chức	Website	Giải pháp/Dịch vụ ATTT
1	Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam	https://vncert.vn/	Là cơ quan điều phối quốc gia về ứng cứu sự cố, thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông. Có chức năng điều phối, ứng cứu các sự cố an toàn thông tin mạng trên toàn quốc.
2	Trung tâm Giám sát an toàn không gian mạng quốc gia	https://soc.gov.vn/	NCSC là đơn vị trung tâm thúc đẩy liên minh phòng chống mã độc & xử lý tấn công mạng. Cùng nhau bảo vệ tài sản của cơ quan, tổ chức và người dân Việt

			Nam trước các nguy cơ tấn công mạng với mục tiêu "Giảm tỉ lệ lây nhiễm mã độc tại Việt Nam, góp phần đưa Việt Nam trở thành quốc gia có môi trường mạng an toàn, tin cậy".
3	Công ty Cổ phần phát triển phần mềm và hỗ trợ công nghệ Misoft	misoft.com.vn	<p>Là một trong những công ty hàng đầu trong lĩnh vực ATTT tại Việt Nam, MISOFT không chỉ cung cấp nhiều dịch vụ ATTT (tư vấn, đánh giá ATTT, triển khai và hỗ trợ kỹ thuật ATTT và đào tạo ATTT), mà còn là đối tác chính và nhà phân phối được uỷ quyền của nhiều công ty an ninh mạng hàng đầu thế giới như Check Point, Forcepoint, Trend Micro,</p> <p>Cung cấp các giải pháp an toàn CNTT toàn diện cho hệ thống CNTT của tổ chức từ máy trạm máy chủ, hệ thống mạng, CSDL, web cho tới giám sát an ninh tập trung.</p>
4	Công ty TNHH an ninh an toàn thông tin CMC - CMC Cyber Security	cmccybersecurity.com	<p>Giải pháp phòng chống mã độc và quản trị tập trung</p> <p>Phần mềm diệt virus (CMC IS) – Miễn phí</p> <p>Giải pháp tường lửa bảo vệ website</p> <p>Giải pháp phòng chống mã độc mã hoá dữ liệu</p>

			Gói dịch vụ và giải pháp
5	Công ty TNHH Hệ thống thông tin FPT	fis.com.vn	Kiểm tra đánh giá bảo mật FPT EagleEye.MSOC FPT EagleEye.MDR Tuân thủ tiêu chuẩn thanh toán PCI DSS
6	Công ty 4Netnam	netnam.vn	Dịch vụ giám sát và ứng cứu sự cố ATTT Dịch vụ quản trị thiết bị, hệ thống ATTT Dịch vụ giám sát hạ tầng mạng và ứng dụng Dịch vụ bảo vệ hệ thống Dịch vụ đánh giá ATTT
7	Công ty Cổ phần An ninh mạng Việt Nam VSEC	vsec.com.vn	Đánh giá bảo mật Trung tâm giám sát ATTT – SOC Tư vấn ATTT
8	Công ty Cổ phần tin học Mi Mi (Mi2 Jsc.)	mi2.com.vn	Tư vấn xây dựng Hệ thống Quản lý ATTT theo tiêu chuẩn ISO/IEC 27001 Tư vấn Phân loại dữ liệu Hỗ trợ Quản trị Hệ thống thông tin Kiểm tra đánh giá an toàn hệ thống

9	Công ty CP Công nghệ an ninh không gian mạng Việt Nam	vncs.vn	<p>là đơn vị cung cấp nhiều sản phẩm/dịch vụ an ninh mạng của riêng mình, đồng thời là nhà phân phối uỷ quyền của các hãng bảo mật nổi tiếng như Splunk, BeyondTrust, Invicti, ...</p> <p>Cung cấp các giải pháp bảo vệ doanh nghiệp trước các nguy cơ tấn công mạng như:</p> <p>Giám sát ATTT VNCS SOC</p> <p>Kiểm tra, đánh giá an toàn thông tin – Penetration Testing</p> <p>Phản ứng và xử lý sự cố ATTT - Incident Response</p> <p>Dịch vụ đánh giá xâm nhập hệ thống – Compromise Assesment</p>
10	Công ty TNHH Máy tính Nét	netcom.vn	<p>Cung cấp các giải pháp hạ tầng mạng</p> <p>Cung cấp các giải pháp ứng dụng mạng</p>
11	Công ty Cổ phần công nghệ Savis	savis.vn	<p>Giải pháp giám sát an ninh mạng – Savis SOC</p> <p>Savis Cyber Security</p>
12	Công ty Cổ phần Cystack Việt Nam	cystack.net	<p>Cung cấp các giải pháp Penetration Testing, Web Secutiy, Endpoint Security</p>

13	Công ty Cổ phần An toàn thông tin CyRadar	cyradar.com	Pentesst, Next-Gen SOC, CyRadar Cloud SOC for AWS
14	Công ty TNHH truyền thông và tin học Pama	pama.com.vn	Các giải pháp bảo mật Fidelis, Flowmon, Novicom, Runecast, OKSystems là công cụ hữu hiệu đảm bảo an toàn thông tin cho cá nhân, tổ chức.
15	Công ty An ninh mạng Viettel	https://viettelcybersecurity.com/	Dịch vụ an ninh mạng (Cloudrity) (Giám sát ATTT mạng, Săn tìm mối nguy ATTT< Kiểm tra đánh giá ATTT) Giải pháp điều phối, tự động hoá và phản ứng an ninh mạng
16	Công ty TNHH MTV 129	https://129infosec.com.vn	Giải pháp phòng chống mã độc BCY Endpoint Security Giải pháp bảo mật, an toàn mạng VIPNet
17	Công ty Công nghệ thông tin VNPT	https://vnptit.vn/	Giải pháp VNPT Smart IR: cho phép truy vấn, điều tra nguyên nhân khi có sự cố về mã độc, giám sát cài đặt phần mềm trái phép và giám sát tuân thủ chính sách bảo mật trên hệ thống CNTT của các tổ chức, doanh nghiệp Giải pháp VNPT DNS Protection: là giải pháp thực


			<p>hiện lọc/chặn các yêu cầu đến các tên miền của các máy chủ độc hại dựa trên danh sách các tên miền được cập nhật và phát hành bởi các tổ chức bảo mật trên thế giới. DNS Protection cung cấp khả năng phát hiện và ngăn chặn kết nối đến các máy chủ độc hại, không mong muốn và đảm bảo an toàn an ninh cho người dùng trong khi sử dụng Mạng</p> <p>Dịch vụ Giám sát An toàn thông tin</p> <p>Dịch vụ Đánh giá An toàn thông tin</p> <p>Các dịch vụ Đánh giá An toàn thông tin</p> <p>Dịch vụ Đào tạo An toàn thông tin</p> <p>Dịch vụ Tư vấn, thiết kế An toàn thông tin</p>
18	Công ty Cổ phần Sensecures	https://sensecures.vn/	<p>Dịch vụ Đào tạo nhận thức an toàn thông tin - Security Awareness Training</p> <p>Dịch vụ Tư vấn An toàn thông tin</p> <p>Dịch vụ An ninh mạng uỷ thác quản trị</p>

19	Công ty TNHH TMGS Việt Nam	https://tmgs.vn/	Dịch vụ đánh giá ATTT Dịch vụ ứng cứu sự cố ATTT
20	Công ty Cổ phần Phân phối Việt Nét	https://vietnetco.vn/	Network Security – Bảo mật hạ tầng mạng Giải pháp SOC & NOC Endpoint Security Giải pháp bảo mật ứng dụng
21	Công ty TNHH Vina Aspire	https://vinaaspire.com	là đơn vị cung cấp nhiều sản phẩm/dịch vụ an ninh mạng của riêng mình, đồng thời là nhà phân phối ủy quyền của các hãng bảo mật nổi tiếng như Splunk, BeyondTrust, Invicti, ...
22	Công ty Công nghệ An ninh mạng Quốc gia Việt Nam	https://www.ncsgroup.vn	Dịch vụ đánh giá ATTT: Dịch vụ đánh giá xâm nhập hệ thống, Dịch vụ kiểm thử xâm nhập hệ thống/ứng dụng, Dịch vụ rà soát, phân tích, gỡ bỏ mã độc, Dịch vụ điều tra và ứng phó sự cố an ninh mạng, Dịch vụ triển khai tích hợp giải pháp ATTT, Dịch vụ thông tin tình báo an ninh mạng Dịch vụ giám sát ATTT: SOC, OT/ICS security

23	Công ty Cổ phần Thiết bị và Truyền thông NGS	http://ngs.com.vn	Giải pháp bảo mật toàn diện cho các tổ chức/doanh nghiệp Giám sát và quản lý các sự kiện bảo mật SIEM Phản ứng sự cố Incident Response
24	Công ty Cổ phần Dịch vụ Công nghệ tin học HPT	https://hpt.vn	Giải pháp tự động hoá quy trình ứng phó sự cố SOAR Bộ giải pháp quản lý AT ANTT Giải pháp và dịch vụ bảo mật
25	Công ty HANEL		

4. Hướng dẫn sử dụng phần mềm Windows Security


Phần mềm Windows Security có sẵn trong hệ điều hành Windows, được mặc định khởi động cùng Windows. Phần mềm Windows luôn thiết lập ở chế độ tự động, liên tục quét virus, malware và các mã độc. Ngoài tính năng bảo vệ trong thời gian thực, các bản cập nhật (update) còn được tự động tải xuống để giúp giữ cho thiết bị của bạn luôn an toàn và bảo vệ khỏi các mối đe dọa.

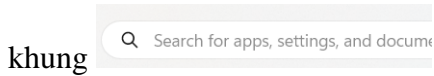
Phần mềm Windows Security có biểu tượng hình cái khiên màu xanh  luôn nằm ở góc dưới bên phải của màn hình cùng các ứng dụng được đặt chế độ khởi động cùng Windows khác (như bộ gõ Unikey). Nếu như máy tính của bạn có cài đặt và bật 1 phần mềm antivirus khác, thì tính năng Bật tự động của phần mềm Windows

Security sẽ tự động tắt, nếu gỡ cài đặt ứng dụng khác đi thì tính năng này của Windows Security sẽ tự động bật lại.

4.1. Khởi động chương trình


Để bật chế độ chạy của phần mềm Windows Security, ta thực hiện như sau:

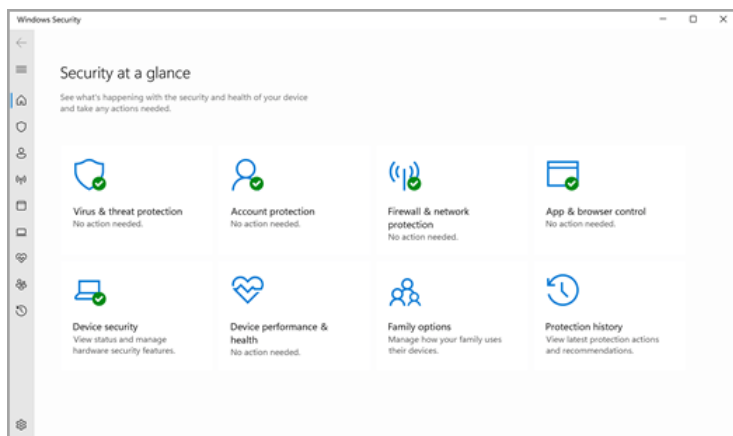
- Chọn biểu tượng Windows  nằm ngoài cùng ở góc dưới bên trái màn hình, sau đó gõ Windows Security trong



- Nếu bạn gõ đúng thì phía bên phải của thực đơn sẽ hiện ra hình dưới:



- Lúc này bạn có thể đưa chuột đến biểu tượng  của chương trình, hoặc chọn lệnh Open để khởi động chương trình. Bạn sẽ thấy có cửa sổ giao diện của chương trình mở ra như hình dưới đây.



Hình 16.Cửa sổ giao diện Windows Security

4.2. Các tính năng của Windows Security

Windows Security giúp bạn quản lý các công cụ bảo vệ thiết bị và dữ liệu của bạn gồm có:

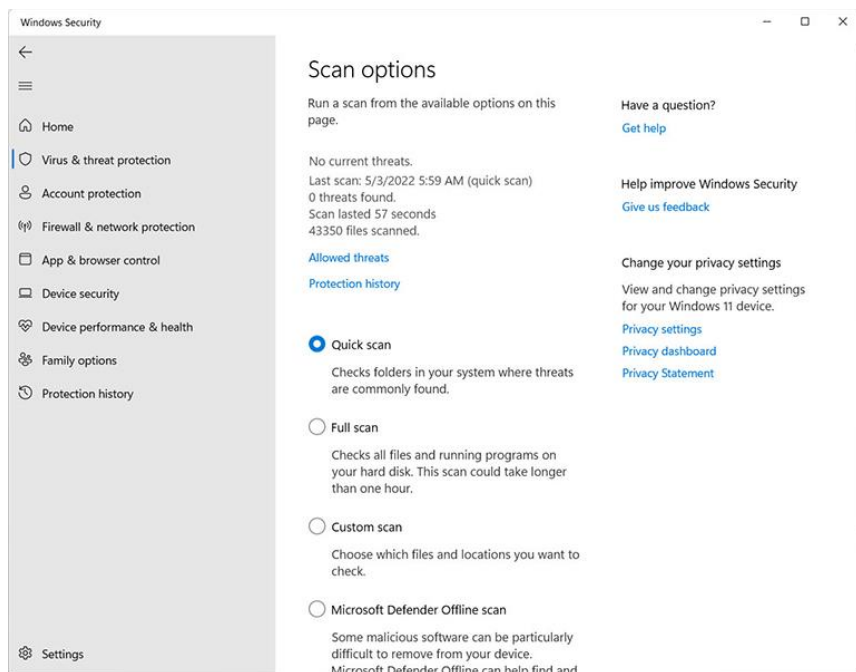
- Virus & threat protection (Chống virus và mối đe dọa): Phần này chứa các tùy chọn để quét virus thiết bị, theo dõi các mối đe dọa, nhận các bản cập nhật dữ liệu bảo mật, chạy quét offline và thiết lập các tính năng chống ransomware nâng cao.
- Account protection (Bảo vệ tài khoản): Cung cấp các tính năng giúp người dùng bảo vệ danh tính Windows của mình với các tùy chọn đăng nhập Windows Hello, cài đặt tài khoản, khóa động,...

- Firewall & network protection (Tường lửa & bảo vệ mạng): Quản lý cài đặt cho tường lửa và theo dõi những hoạt động đang diễn ra với mạng và kết nối với Mạng của bạn.
- App & browser control (Kiểm soát ứng dụng & trình duyệt): Cập nhật cài đặt cho thiết SmartScreen của Windows Security giúp bảo vệ thiết bị của bạn chống lại các ứng dụng, tệp, trang web và nội dung tải xuống tiềm ẩn nguy hiểm. Bạn sẽ có tính năng bảo vệ khai thác và bạn có thể tùy chỉnh cài đặt bảo vệ cho các thiết bị của mình.
- Device security (Bảo mật thiết bị): Xem lại các tùy chọn bảo mật được tích hợp sẵn như Bộ xử lý bảo mật (TPM) và Secure Boot được tích hợp trong phần cứng của thiết bị để giúp bảo vệ thiết bị của bạn khỏi bị các mối đe dọa và tấn công.
- Device performance & health (Hiệu suất và tình trạng hoạt động của thiết bị): Windows Security thường xuyên quét máy tính và hiển thị các báo cáo về tình trạng và hiệu suất của thiết bị ở phần này.
- Family options (Tùy chọn gia đình): Phần này giúp bạn theo dõi các thiết bị trong gia đình của bạn và các hoạt động trực tuyến của trẻ bằng tài khoản Microsoft.
- Protection history (Lịch sử bảo vệ): Phần này cho bạn xem và quản lý các hoạt động và đề xuất bảo vệ mới nhất.

Các biểu tượng trạng thái cho biết mức độ an toàn của bạn:

- **Màu xanh** lá cây có nghĩa là hiện không có bất kỳ hành động nào được đề xuất.
- **Màu vàng** có nghĩa là có một đề xuất an toàn cho bạn.
- **Màu đỏ** cảnh báo rằng có điều gì đó cần bạn chú ý ngay lập tức.

4.3. Thiết lập các tính năng chống virus và các mối đe dọa



Hình 17. Giao diện phần Virus & threat protection

a. Có 4 tùy chọn:

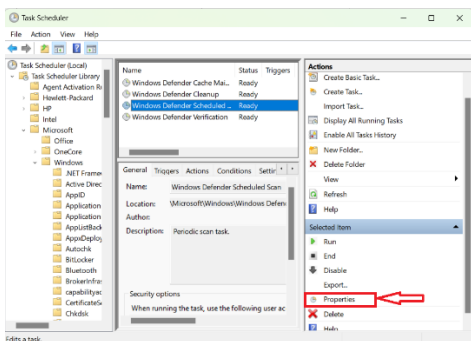
- **Quick scan:** quá trình này sẽ chỉ kiểm tra các thư mục khởi động và registry để đảm bảo rằng không có gì độc hại ẩn náu bên trong chúng. Quá trình này thực hiện rất nhanh, nhưng có thể không quá hiệu quả nếu người dùng muốn dọn dẹp virus ẩn náu khắp mọi nơi.
- **Full scan:** sẽ quét mọi tập tin và thư mục trên máy tính, registry, tất cả các mục khởi động và cũng có thể được định cấu hình để quét các ổ đĩa gắn mạng. Quá trình Full scan có thể mất hàng giờ tùy thuộc vào dung lượng lưu trữ người dùng có và tốc độ máy tính. Người dùng có thể đợi và chạy quá trình quét toàn bộ khi không cần đến máy tính của mình trong vài giờ.
- **Custom scan:** có thể được đặt để nhắm mục tiêu bất kỳ thư mục nào mà người dùng muốn quét.
- **Microsoft Defender Offline scan:** được sử dụng khi mã độc khó loại bỏ trong khi Windows 11 đang hoạt động. Chạy chế độ này sẽ quét máy tính để tìm mã độc trước khi hệ điều hành tải, giúp loại bỏ virus khi nó không thể tự bảo vệ. Lựa chọn này hữu ích khi mã độc có thể đã tự ghi vào một nơi mà phần mềm chống virus không thể xóa nó hoặc nó có thể chủ động chặn phần mềm chống virus xóa nó trong các trường hợp sử dụng bình thường.

Sau khi đã chọn được kiểu quét mong muốn, người dùng hãy nhấp vào nút Scan Now. Chờ một thời gian để phần mềm tiến hành quá trình quét. Nếu mã độc được phát hiện, Microsoft Defender sẽ đề xuất các cách xử lý vấn đề. Người dùng nên làm theo các khuyến nghị để được xử lý đúng cách.

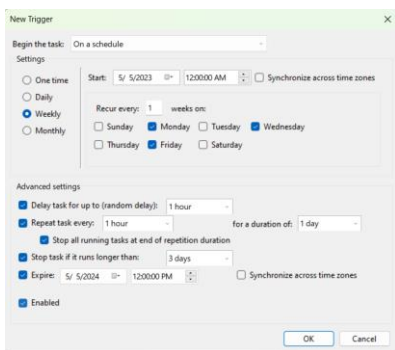
b. Lập lịch quét riêng

Ngay cả khi Windows Security thường xuyên quét thiết bị để giữ cho thiết bị an toàn, người dùng vẫn có thể đặt thời gian và tần suất quét bằng cách sau:

- Chọn nút Start, nhập Schedule tasks trong hộp Search và trong danh sách kết quả, chọn Task Scheduler.
- Trong ngăn bên trái, hãy chọn mũi tên (>) bên cạnh Task Scheduler Library để mở rộng, thực hiện thao tác tương tự với Microsoft > Windows, rồi sau đó cuộn xuống và chọn thư mục Windows Defender.
- Trong ngăn trên cùng ở giữa, hãy Windows Defender Scheduled Scan.
- Trong ngăn Actions bên phải, cuộn xuống và chọn Properties.



- Trong cửa sổ mở ra, hãy chọn tab Triggers, rồi chọn New.
- Đặt thời gian và tần suất ưu tiên của bạn, sau đó chọn OK.
- Xem lại lịch và chọn OK.



c. Bật/tắt tính năng Microsoft Defender Antivirus để bảo vệ trong thời gian thực

Đôi khi, bạn có thể phải ngừng chạy tính năng bảo vệ trong thời gian thực một lát. Trong khi tính năng bảo vệ trong thời gian thực bị tắt, các tệp bạn mở hoặc tải xuống sẽ không được quét tìm các mối đe dọa. Tuy nhiên, tính năng bảo vệ trong thời gian thực sẽ

sớm tự động bật lại sau một thời gian ngắn để bảo vệ thiết bị của bạn.

Để tắt tạm thời tính năng bảo vệ trong thời gian thực:

- Chọn Virus & threat protection settings > Manage settings. (Trong các phiên bản đầu tiên của Windows 10, hãy chọn Virus & threat protection > Virus & threat protection settings.)

Virus & threat protection settings

No action needed.

[Manage settings](#)

- Chuyển cài đặt Real-time protection thành Off và chọn Yes để xác nhận.

d. Bật/tắt tính năng cập nhật dữ liệu

- Chọn Virus & threat protection updates > Protection updates.

Virus & threat protection updates

Security intelligence is up to date.

Last update: 5/5/2023 10:34 AM

[Protection updates](#)

- Trên trang tiếp theo, chọn Check for updates để tải xuống và cài đặt các bản cập nhật.

e. Bật/tắt tính năng Ransomware Protection

Ransomware Protection là một tính năng hữu ích đi kèm với Windows 11 để giúp bảo mật thiết bị của người dùng trước các cuộc tấn công Ransomware. Tuy nhiên, theo mặc định, tính năng bảo vệ chống ransomware này bị tắt trên tất cả các thiết bị của Microsoft. Để kích hoạt và sử dụng tính năng này, hãy thực hiện các bước sau:

- Chọn Virus & threat protection updates > Manage ransomware protection.

Ransomware protection

No action needed.

[Manage ransomware protection](#)

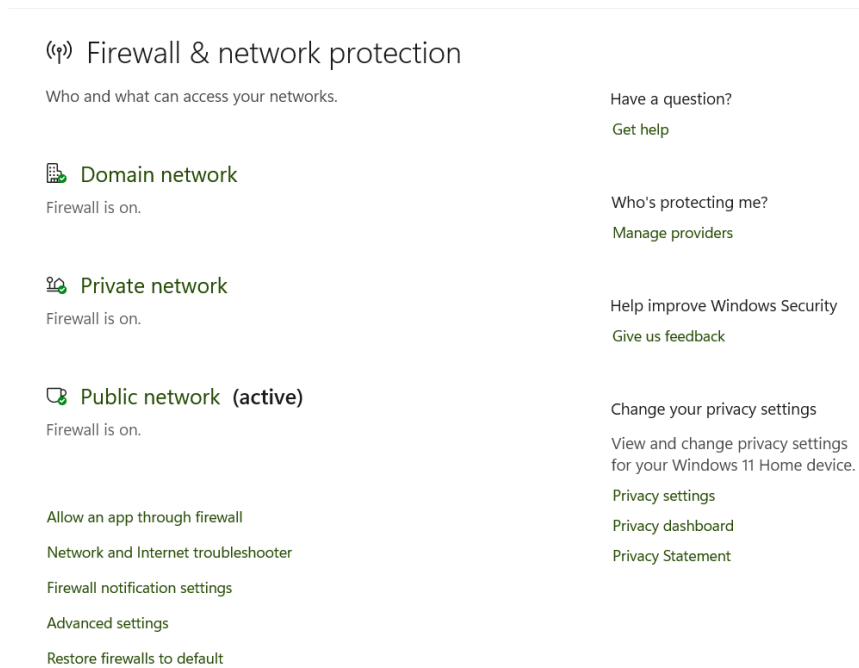
- Trong tùy chọn Controlled folder access, đổi lựa chọn Off sang On để kích hoạt.

Khi kích hoạt xong, bạn sẽ phải đưa một số chương trình yêu thích của mình vào danh sách trắng để chúng có quyền truy cập vào thư mục được kiểm soát. Bước này sẽ giúp bạn tránh việc xác thực sai và cho phép cài đặt các chương trình mới:

- Trong tùy chọn Controlled folder access, nhấp vào Allow an app through Controlled folder access.
- Tiếp đó, chọn nút Add an allowed app, sau đó chọn Browse all apps hoặc Recently blocked apps:

- Browse all apps cho phép bạn chọn bất kỳ ứng dụng nào từ máy tính của mình.
 - Recently blocked apps sẽ hiển thị cho bạn danh sách các ứng dụng đã bị chặn gần đây bởi tùy chọn Controlled folder access, từ đó bạn có thể xem xét và bỏ chặn một ứng dụng đã có trong danh sách này.
- Để tránh gắn cờ nhầm phần mềm hoặc ứng dụng hữu ích là ransomware, hãy thêm chúng vào phần Protected Folders.

4.4. Quản lý tường lửa và bảo mật mạng



Hình 18. Giao diện phần Firewall & network protection

Có 3 tùy chọn loại mạng:

- Domain network (mạng miền)
- Private network (mạng riêng)
- Public network (mạng công cộng)

Cấu hình mạng hiện đang được sử dụng sẽ được đánh dấu là “active”

a. Bật / Tắt Microsoft Defender Firewall

Tường lửa bảo vệ hệ thống và dữ liệu khỏi bị truy cập trái phép và các mối đe dọa, tuy nhiên, đôi khi, bạn có thể cần phải tắt tường lửa. Ví dụ: khi tải xuống file từ các nguồn không đáng tin cậy hoặc truy cập vào một ứng dụng đang bị chặn.

Nếu bạn đã quyết định vô hiệu hóa tường lửa của Microsoft Defender, bạn có thể vào từng cấu hình mạng và bật hoặc tắt chúng theo yêu cầu của mình. Nhấp vào loại mạng để xem cài đặt tường lửa của nó.

 Private network

Firewall is on.



Sau đó, trong phần Microsoft Defender Firewall, hãy nhấp vào nút “On” để tắt “Off”.

Microsoft Defender Firewall


Helps protect your device while on a domain network.



Nếu bạn muốn bật lại tường lửa cho tất cả các mạng cùng nhau, bạn có thể chỉ cần nhấp vào nút ‘Restore settings’ để khôi phục cài đặt mặc định.

Firewall & network protection

Who and what can access your networks.

 Microsoft Defender Firewall is using settings that may make your device unsafe.

Restoring default settings will remove all Windows Defender Firewall settings that you have configured for all network locations. This might cause some apps to stop working.

Restore settings



Domain network

Firewall is off.

Turn on

Mỗi cấu hình mạng cũng có một cài đặt khác – ‘Block all incoming connections, including those in the list of allowed programs’ trong Incoming connections. Cài đặt này giúp tăng thêm mức độ bảo mật khi bạn bị tấn công.

Incoming connections

Prevents incoming connections when on a public network.

Blocks all incoming connections, including those in the list of allowed apps.

Theo mặc định, Windows Defender Firewall chặn tất cả các kết nối đến trừ khi có một quy tắc ngoại lệ do bạn hoặc một ứng dụng được phép tạo. Bất tùy chọn này sẽ ghi đè tất cả các ngoại lệ đó và chặn tất cả lưu lượng đến không được yêu cầu bao gồm cả những lưu lượng dành cho các chương trình được phép. Khi bạn chặn tất cả các kết nối đến với máy tính của mình, các thiết bị khác trong cùng một mạng cũng không thể kết nối với máy tính. Tuy nhiên, bạn vẫn có thể duyệt Mạng, gửi và nhận thư, v.v.

b. Một số cài đặt khác

Một số cài đặt khác trong phần Firewall & network protection cho phép người dùng để tùy chỉnh và quản lý các trường lựa của Windows.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

- Allow an app through firewall – Thao tác này sẽ đưa bạn đến applet bảng điều khiển, nơi bạn có thể thêm, thay đổi và xóa các ứng dụng được phép giao tiếp thông qua Windows Defender Firewall
- Network and Mạng troubleshooter – Liên kết này cho phép bạn chạy trình gỡ rối để khắc phục các sự cố mạng và Mạng.

- Firewall notification settings – Tùy chọn này cho phép bạn quản lý các nhà cung cấp bảo mật và thông báo từ Windows Security.
- Advanced settings – Nó mở ra bảng điều khiển Windows Defender Firewall, nơi bạn có thể theo dõi và quản lý các quy tắc bảo mật kết nối đến, đi và kết nối.
- Restore firewalls to default – Tùy chọn này cho phép khôi phục cài đặt mặc định của tường lửa.

X. Danh mục tài liệu tham khảo

- [1].VN action brief WPS cybersecurity VTE, 2022
- [2].Luật An toàn thông tin mạng 2015.
- [3].Luật An ninh mạng 2018.
- [4].Network Security Assessment, 2nd Edition, Chris McNab, O'Reilly Media, Inc.
- [5].Network security essentials: Applications an Standards 4th edition, William Stallings - Copyright © 2011 Pearson Education.
- [6].Bao cao Thuong nien an ninh mang 2022 du bao 2023_Vina Aspire
- [7].VNITA – Cyber security report 2017, Viện Công nghệ Thông tin, Đại học Quốc gia Hà Nội
- [8].Giáo trình Cơ sở an toàn thông tin, Hoàng Xuân Dâu, Học viện CN BCVT, Bộ TT&TT.
- [9].Cyber-Security-for-Dummies 2019, Joseph Steinberg
- [10]. Holger Schulze, Insider Threat Report 2020, Cybersecurity Insider, 2020.

Mọi đóng góp ý kiến xin gửi qua biểu sau:
<https://forms.office.com/r/7u9aYQ6Ut5> . Xin cảm ơn!