Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

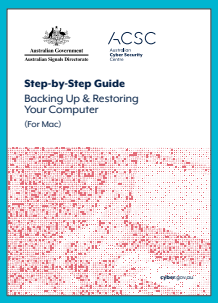
HƯỚNG DẪN VỀ AN NINH MẠNG CHO DOANH NGHIỆP NHỎ

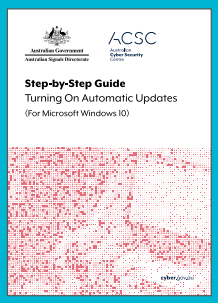
cyber.gov.au

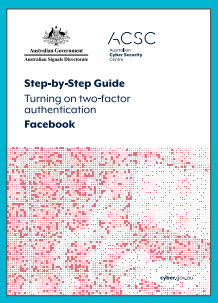
Hướng dẫn bổ sung

Muốn có thêm các biện pháp an ninh mạng để giúp doanh nghiệp giữ an toàn, quý vị hãy xem loạt bài về An ninh Mạng cho Doanh nghiệp nhỏ tại cyber.gov.au

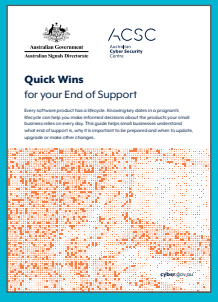
HƯỚNG DẪN TỪNG BƯỚC

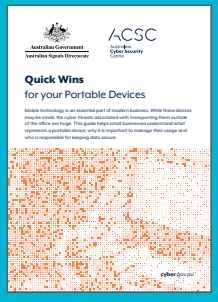


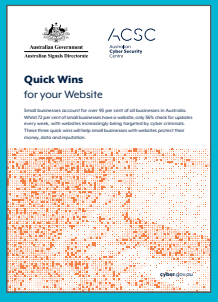




HƯỚNG DẪN THẮNG NHANH







Mục lục

Lời mở đầu

Bản hướng dẫn này được xây dựng nhằm hỗ trợ doanh nghiệp nhỏ bảo vệ cơ sở phòng ngừa các sự cố an ninh mạng phổ biến nhất.

Sự cố an ninh mạng có thể gây thảm khốc cho doanh nghiệp nhỏ.

Thật không may, tại Trung tâm An ninh Mạng Úc (Australian Cyber Security Centre - ACSC), ngày nào chúng tôi cũng chứng kiến tác động sự cố an ninh mạng gây ra cho cá nhân, doanh nghiệp nhỏ và cả các công ty lớn.

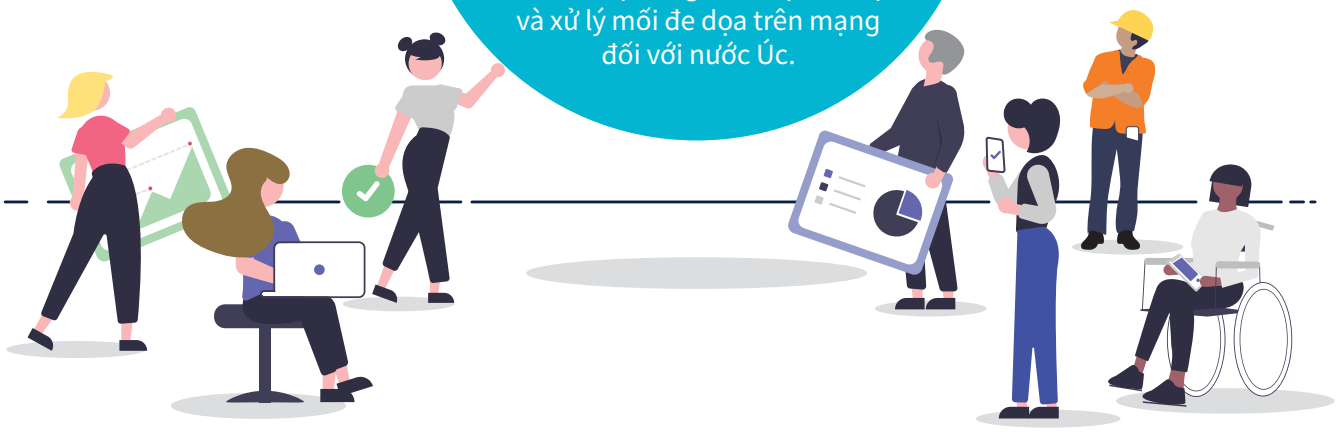
Chúng tôi nhận ra rằng rất nhiều chủ nhân và người điều hành doanh nghiệp nhỏ không có thời gian và điều kiện vật chất để chú trọng vấn đề an ninh mạng. Tuy nhiên, chỉ cần áp dụng một số các biện pháp đơn giản là có thể giúp doanh nghiệp nhỏ tránh được các sự cố an ninh mạng phổ biến.

Bản *Hướng dẫn về An ninh Mạng cho Doanh nghiệp nhỏ* của chúng tôi được soạn thảo riêng cho doanh nghiệp nhỏ để họ nắm được và thực hiện được để nâng cao khả năng bảo toàn an ninh mạng trước mối đe dọa đang biến hóa không ngừng. Hướng dẫn được soạn riêng cho doanh nghiệp nhỏ với lời văn mạch lạc chỉ dẫn việc thực hiện một cách đơn giản và dễ hiểu.

Nếu muốn nắm được một cách khái quát các căn bản về an ninh mạng, thì bản hướng dẫn này là điểm khởi đầu lý tưởng. Nếu muốn hiểu biết sâu hơn về vấn đề an ninh mạng thì quý vị có thể tìm hiểu thêm chi tiết và các lời khuyên khác nữa trên trang nhà của Trung tâm ACSC tại: **cyber.gov.au**

Công việc của Trung tâm ACSC là giúp làm cho nước Úc trở thành nơi an toàn nhất khi kết nối trên mạng.

Trung tâm An ninh Mạng Úc (Australian Cyber Security Centre - ACSC), trực thuộc Tổng cục Tín hiệu Úc (Australian Signals Directorate - ASD), cung cấp hướng dẫn, hỗ trợ về an toàn mạng và ứng phó tức thời nhằm phòng tránh, phát hiện, và xử lý mối đe dọa trên mạng đối với nước Úc.



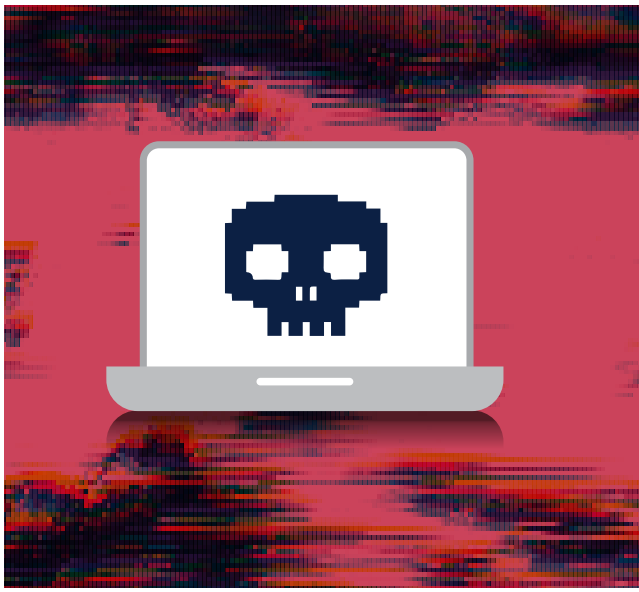
Mối đe dọa mạng: **Các lĩnh vực mấu chốt**

Đối với các doanh nghiệp nhỏ, ngay cả một sự cố an ninh mạng nhỏ nhất cũng có thể gây ra thảm khốc.

Phần này được soạn thảo nhằm giúp doanh nghiệp nhỏ nâng cao cảnh giác và chuẩn bị sẵn sàng. Phần này xác định và giải thích các loại đe dọa an ninh mạng phổ biến nhất và những biện pháp quý vị có thể thực hiện để bảo vệ doanh nghiệp.

BẢO VỆ
tiền bạc, dữ liệu & danh tiếng

Phần mềm độc hại (Malware)



Là gì? Là các phần mềm trái phép nhằm mục đích gây hại

Malware là một thuật ngữ bao trùm để chỉ các phần mềm độc hại bao gồm phần mềm tống tiền (ransomware), vi rút, phần mềm gián điệp (spyware) và phần mềm trojan.

Vì sao? Gây gián đoạn. Làm hại. Lừa đảo.

Malware cung cấp cho tội phạm cách tiếp cận thông tin quan trọng như là số trương mục ngân hàng và số thẻ tín dụng và mật khẩu.

Malware cũng có thể **kiểm soát hoặc do thám** máy tính của người dùng. Những hành động của tội phạm khi chúng xâm nhập và chiếm dữ liệu là để chúng:

- **Lừa đảo**
- **Đánh cắp danh tính**
- **Gây gián đoạn** cho doanh nghiệp
- **Đánh cắp** các dữ liệu nhạy cảm hoặc các tài sản trí tuệ
- **Chuyển đi** các dữ liệu của máy tính cho hoạt động tội phạm trên diện rộng hơn

Ai? Bất cứ ai, ở bất cứ đâu

Tội phạm sản xuất ra malware có thể trú ngụ ở bất cứ đâu trên thế giới.

Tất cả những gì chúng cần chỉ đơn giản là chiếc máy tính, kỹ năng công nghệ và ý định bất chính. Tội phạm cũng có thể dễ dàng tiếp cận các công cụ rẻ tiền để sử dụng malware chống lại quý vị.

Tội phạm có thể quăng lưới rất rộng rồi nhắm vào những nơi sơ hở để chúng dễ gây tổn thương nhất. Thông qua việc áp dụng các biện pháp an ninh mạng và nâng cao cảnh giác đối với các mối đe dọa, quý vị có thể bảo vệ doanh nghiệp tránh để cơ sở trở thành mục tiêu dễ dàng cho chúng.

BẢO VỆ CHỐNG LẠI MALWARE

- **Cập nhật tự động** hệ thống vận hành, phần mềm và các ứng dụng của quý vị
- **Thường xuyên sao lưu** các dữ liệu quan trọng
- **Huấn luyện nhân viên** để họ phát hiện ra các đường dẫn và các tài liệu đính kèm đáng ngờ

Tin nhắn lừa đảo (Phishing)

Là gì? Là các email, tin nhắn hay cuộc gọi đáng ngờ nhằm lừa người ta về tiền bạc hoặc dữ liệu

Tội phạm sẽ thường dùng email, mạng xã hội, các cuộc gọi điện thoại hoặc tin nhắn để tìm cách lừa đảo các doanh nghiệp Úc.

Những tội phạm này có thể giả làm cá nhân hoặc tổ chức mà quý vị cho là mình có biết họ hoặc nghĩ rằng mình nên tin tưởng họ.

Tin nhắn và cuộc gọi của chúng tìm cách lừa các doanh nghiệp để doanh nghiệp làm một số việc như:

- **Thanh toán hóa đơn giả mạo** hoặc thay đổi chi tiết thanh toán đối với hóa đơn hợp pháp
- **Tiết lộ chi tiết trương mục ngân hàng,** mật khẩu, và số thẻ tín dụng (đôi khi còn được gọi là lừa đảo qua mạng (phishing), tội phạm mạng có thể bắt chước các thương hiệu hoặc biểu tượng chính thức của ngân hàng và trang mạng để trông có vẻ hợp pháp)
- **Cho phép việc tiếp cận từ xa** vào máy tính hoặc máy chủ của quý vị
- **Mở tài liệu đính kèm,** trong đó thể chứa malware
- **Mua phiếu quà tặng** rồi gửi phiếu cho bọn lừa đảo

Ở đâu? Email, mạng xã hội, cuộc gọi điện thoại, tin nhắn trên điện thoại

Lừa đảo phishing không chỉ giới hạn ở email. Chúng ngày càng trở nên tinh vi hơn và khó phát hiện hơn.

Hãy cẩn trọng với các yêu cầu khẩn cấp về tiền bạc, thay đổi tài khoản ngân hàng, các tài liệu đính kèm bất ngờ và các yêu cầu kiểm tra hoặc khẳng định chi tiết đăng nhập.

Vào trang **scamwatch.gov.au** để trình báo lừa đảo.

Ai? Doanh nghiệp Úc

Một số tin nhắn có thể được gửi cho hàng ngàn người, hoặc nhắm vào một người cụ thể.

Tuy vậy, chúng ta đã biết rằng tội phạm hay sử dụng một số phương pháp phổ biến để tìm cách lừa đảo nhân viên quý vị. Tin nhắn có thể bao gồm:

- **Người có thẩm quyền:** Tin nhắn này có tự nhận là của người nào đó là viên chức hay nhân viên cấp cao của doanh nghiệp không?
- **Khẩn cấp:** Người ta có bảo đang có vấn đề gì đó hoặc là quý vị chỉ có ít thời gian để hồi âm hay để trả tiền không?
- **Tình cảm:** Tin nhắn có làm cho quý vị cảm thấy hoảng hốt, hi vọng hoặc tò mò không?
- **Khan hiếm:** Tin nhắn có chào mời quý vị món gì đang rất khan hiếm, hay hứa hẹn cuộc làm ăn rất hời không?
- **Sự kiện hiện tại:** Tin nhắn có liên quan đến câu chuyện thời sự đang diễn ra hay là sự kiện lớn không?

Nếu quý vị cho là tin nhắn hoặc cuộc gọi có thể thật sự là từ tổ chức quý vị tin tưởng (như là ngân hàng hoặc nhà cung cấp của quý vị), hãy tìm phương pháp liên lạc nào mà quý vị có thể tin tưởng.

Tìm trang mạng chính thức hoặc gọi số điện thoại mà họ quảng cáo. Không dùng đường dẫn hoặc chi tiết liên lạc ghi trong tin nhắn mà họ gửi cho quý vị hoặc báo cho quý vị qua điện thoại bởi vì những chi tiết đó có thể là giả mạo.

Phần mềm tống tiền (Ransomware)

Là gì? Đó là một loại phần mềm độc hại (malware) nhằm khóa máy tính hoặc hồ sơ của quý vị cho đến khi quý vị phải trả tiền chuộc cho chúng

Ransomware hoạt động bằng cách khóa lại hoặc mã hóa hồ sơ làm cho quý vị không thể sử dụng hoặc tiếp cận được. Đôi khi nó còn có thể làm cho máy ngưng hoạt động. Ransomware có thể nhiễm vào máy cũng giống như các malware khác. Ví dụ như:

- Vào các trang mạng không an toàn hoặc đáng ngờ
- Mở đường dẫn, email hoặc hồ sơ không rõ nguồn gốc
- Kém an toàn trên mạng lưới hoặc thiết bị (kể cả máy chủ) của quý vị

Vì sao? Vì tiền

Ransomware cho tội phạm mạng có thu nhập cao mà ít rủi ro. Loại phần mềm này dễ làm và dễ phân tán. Mọi người thường phải trả tiền chuộc bằng cách sử dụng tiền điện tử hoặc tiền mã hoá như Bitcoin, làm cho rất khó truy tìm dấu vết. Ngoài ra, tội phạm mạng cũng lại có lợi thế vì phần lớn các doanh nghiệp nhỏ không chuẩn bị sẵn sàng đối phó với các cuộc tấn công ransomware.

Ai? Doanh nghiệp nhỏ, trung bình và lớn

Doanh nghiệp nhỏ có thể đặc biệt dễ bị tổn thương, bởi vì họ ít khi thực hiện các biện pháp an ninh mạng để phòng tránh và khôi phục từ ransomware.

KHÔNG BAO GIỜ TRẢ TIỀN CHUỘC

Việc trả tiền chuộc không đảm bảo lấy lại được hồ sơ của nạn nhân, cũng không đảm bảo ngăn cản chúng xuất bản bất cứ dữ liệu nào bị lấy cắp hoặc rao bán dữ liệu để sử dụng vào các hành động tội phạm khác. Nó cũng làm tăng khả năng nạn nhân trở thành mục tiêu bị làm hại lần nữa.

Nếu quý vị gặp phải sự cố về ransomware và cần được hỗ trợ, hãy gọi cho Đường dây nóng 24/7 của Trung tâm ACSC qua số 1300 CYBER1 (1300 292 371).

Bất kể quyết định của nạn nhân về việc trả tiền chuộc là thế nào đi nữa thì chúng tôi vẫn khuyến khích nạn nhân hãy trình báo sự cố về ransomware cho Trung tâm ACSC tại cyber.gov.au.

PHÒNG NGỪA VÀ KHÔI PHỤC TỪ RANSOMWARE

- Thường xuyên sao lưu dữ liệu quan trọng của quý vị
- Tự động cập nhật hệ thống vận hành, phần mềm và các ứng dụng
- Khi có thể, hãy đặt chức năng xác thực đa yếu tố để tiếp cận dịch vụ (trang 12)
- Kiểm tra và giữ an toàn thiết bị của mình (kể cả máy chủ nếu có) và bất cứ các dịch vụ nào trưng bày trên mạng trên hệ thống của quý vị (Máy tính điều khiển từ xa, Chia sẻ hồ sơ, Webmail). Thảo luận vấn đề này với chuyên viên IT nếu quý vị không rõ.

Cân nhắc về phần mềm: **Các lĩnh vực mấu chốt**

Quản lý phần mềm, dữ liệu và các tài khoản trên mạng có thể gia tăng sự bảo vệ lên rất nhiều cho doanh nghiệp đối với các loại đe dọa mạng phổ biến nhất.

Ví dụ như, hệ thống vận hành là mảnh phần mềm quan trọng nhất trong máy tính của quý vị. Hệ thống quản lý phần cứng và tất cả các chương trình nằm trong phần cứng, vì thế cần phải được cập nhật thường xuyên để đảm bảo quý vị luôn sử dụng phiên bản an toàn nhất.

Tăng cường sự vững chắc, cập nhật và giữ an toàn với các cân nhắc về phần mềm này cho doanh nghiệp nhỏ.

Cập nhật tự động

Là gì? Cập nhật phần mềm

Cập nhật là phiên bản phần mềm được nâng cấp (chương trình, ứng dụng và hệ thống vận hành) quý vị đã cài đặt trong máy chủ, máy tính và thiết bị di động. **Cập nhật tự động** là được đặt mặc định hoặc được **'đặt sẵn để không cần nhớ'** để cập nhật phần mềm của quý vị ngay khi có phiên bản mới.

Vì sao? Vì an toàn

- Giữ hệ thống vận hành và các ứng dụng được cập nhật là **một trong những cách tốt nhất bảo vệ quý vị** tránh sự cố an ninh mạng
- Thường xuyên cập nhật phần mềm sẽ **giảm cơ hội cho tin tặc khai thác điểm yếu đã biết** để chúng chạy malware hoặc xâm nhập vào thiết bị của quý vị
- **Tiết kệm thời gian và cũng không phải lo lắng,** cập nhật tự động là việc quan trọng nhằm giữ an toàn cho thiết bị và dữ liệu của quý vị.

Khi nào? Hôm nay & mỗi ngày

- **Bật cập nhật tự động,** nhất là đối với hệ thống vận hành
- **Thường xuyên kiểm tra cập nhật trong** trường hợp không có cập nhật tự động
- Nếu nhận được lời nhắc cập nhật hệ thống vận hành hoặc các phần mềm khác, quý vị nên **cài đặt cập nhật càng sớm càng tốt**
- **Đặt giờ thuận tiện cho cập nhật tự động** để tránh công việc kinh doanh thường ngày bị gián đoạn
- Nếu quý vị sử dụng **phần mềm chống vi rút, hãy đảm bảo có bật cập nhật tự động**

LƯU Ý:

Nếu phần cứng hoặc phần mềm của quý vị đã quá cũ thì có khả năng là không cập nhật được và có thể làm cho doanh nghiệp của quý vị dễ bị tổn thương về các vấn đề an toàn.

Trung tâm ACSC khuyến nghị cập nhật thiết bị hay phần mềm càng sớm càng tốt.

Đến năm 2020, hệ thống Windows 7, Microsoft Office 2010 và Windows Server 2008 đã hết hạn được hỗ trợ và không còn an toàn.

Muốn biết thêm chi tiết, hãy đọc bản hướng dẫn tiêu đề Thắng Nhanh của Trung tâm ACSC về Hết hạn Hỗ trợ tại trang cyber.gov.au

Sao lưu Tự động

Là gì? Sao lưu dữ liệu

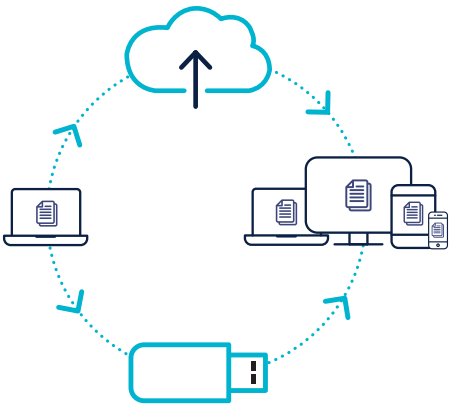
Sao lưu là một bản lưu điện tử cho các dữ liệu quan trọng nhất của doanh nghiệp, ví dụ như chi tiết khách hàng và sổ sách tài chính. Bản sao lưu có thể được lưu ở một thiết bị lưu trữ bên ngoài hoặc trên đám mây.

Sao lưu tự động là hệ thống mặc định hoặc được 'đặt sẵn để không phải nhớ' nhằm tự động sao lưu dữ liệu mà không cần con người can thiệp.

Khi ngưng kết nối và tháo thiết bị trữ sao lưu ra một cách an toàn sau mỗi lần sao lưu sẽ đảm bảo là thiết bị được an toàn nếu xảy ra sự cố an ninh mạng.

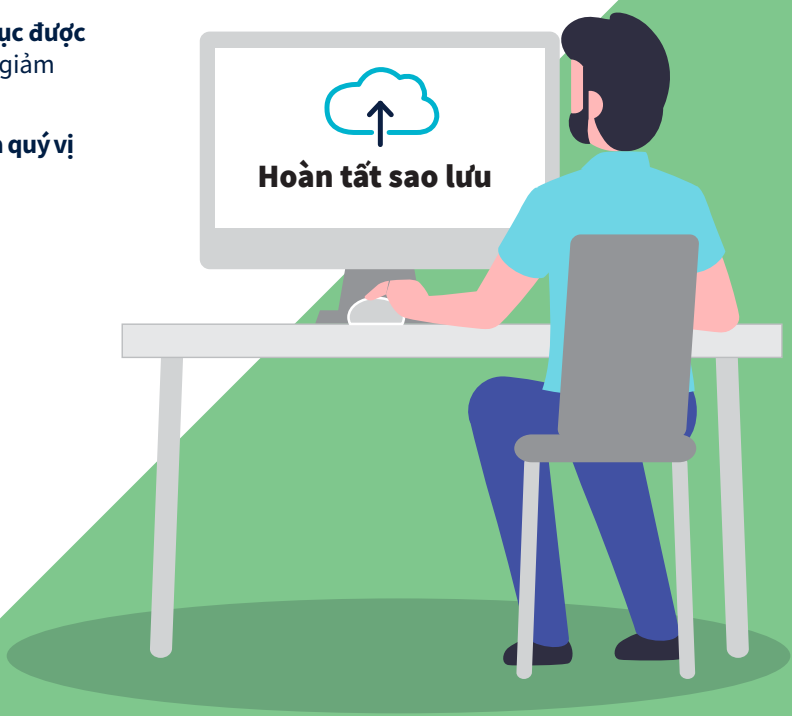
Vì sao? Khôi phục đơn giản

- **Sao lưu là biện pháp cần trọng,** để cho quý vị vẫn tiếp cận được dữ liệu trong trường hợp dữ liệu bị mất, bị đánh cắp hoặc bị hư hại
- **Cho phép doanh nghiệp của quý vị khôi phục được** sau sự cố mạng (chẳng hạn ransomware) và giảm thiểu thời gian ngừng hoạt động
- **Bảo vệ sự đáng tin cậy của doanh nghiệp của quý vị** và giúp đáp ứng các trách nhiệm pháp lý^



Khi nào? Hôm nay & mỗi ngày

- **Lựa chọn hệ thống sao lưu phù hợp với doanh nghiệp của mình.** Hãy cân nhắc những gì quý vị có đủ khả năng bị mất trong tình huống xấu nhất để giúp hướng dẫn cho quý vị chọn các yêu cầu đặt ra chẳng hạn như bao lâu thì quý vị phải sao lưu dữ liệu một lần.
- **Thường xuyên kiểm tra hệ thống sao lưu** bằng cách thử khôi phục dữ liệu
- **Luôn luôn giữ ít nhất một bản sao lưu không kết nối với thiết bị của quý vị,** tốt hơn là cất ở ngoài doanh nghiệp đề phòng tình huống bị thiên tai hoặc trộm cắp
- **Không kết nối sao lưu của quý vị với thiết bị bị nhiễm** ransomware hoặc bị nhiễm vi rút.



^Một số ngành cụ thể có nghĩa vụ phải giữ hồ sơ trong một khoảng thời gian nhất định. Hãy đảm bảo quý vị nắm được yêu cầu về việc lưu dữ liệu.

Xác thực đa yếu tố

Là gì? Là biện pháp an toàn đòi hỏi có từ hai bằng chứng trở lên về danh tính trước khi cho phép quý vị tiếp cận

Xác thực đa yếu tố (Multi-factor authentication – MFA) thường yêu cầu phải có sự kết hợp giữa:

- **điều gì đó quý vị biết** (mật khẩu/cụm mật khẩu, PIN, câu hỏi bí mật)
- **điều gì đó quý vị có** (thẻ smartcard, thiết bị xác thực, ứng dụng xác thực)
- **điều gì đó là của riêng quý vị** (vân tay hay là đặc điểm sinh trắc học nào khác)

Vì sao? Sự an toàn mạnh hơn nhiều

MFA là một trong những cách bảo vệ hiệu quả nhất chống lại sự tiếp cận trái phép thông tin và tài khoản rất giá trị của quý vị.

Có nhiều lớp xác thực làm cho việc tin tặc tấn công doanh nghiệp quý vị bị khó hơn rất nhiều. Chúng có thể xoay xở đánh cắp được một bằng chứng về danh tính như mật khẩu của quý vị, nhưng chúng vẫn cần phải lấy được và sử dụng các bằng chứng danh tính khác nữa thì mới tiếp cận được tài khoản của quý vị.

Ở đâu? Tiếp cận vào các tài khoản quan trọng

Doanh nghiệp nhỏ nên thực hiện MFA cho các tài khoản quan trọng bất kỳ khi nào có thể, ưu tiên các tài khoản tài chính và email. Một số phương án MFA bao gồm, nhưng không giới hạn bởi:

- Thiết bị xác thực
- Pin bất kỳ
- Đặc điểm sinh trắc học/vân tay
- Ứng dụng xác thực
- Email
- SMS

Con người và Thủ tục: **Các Lĩnh vực mấu chốt**

Doanh nghiệp, dù nhỏ tới mức nào, vẫn cần phải cảnh giác và chủ động áp dụng các biện pháp an ninh mạng ở tất cả mọi tầng lớp.

Quy trình nội bộ và lực lượng lao động là tuyến phòng thủ cuối cùng, và là một trong những tuyến phòng thủ quan trọng nhất để bảo vệ doanh nghiệp trước mối đe dọa an ninh mạng.

Do doanh nghiệp nhỏ thường thiếu điều kiện để có nhân viên chuyên về IT, phần này đề cập cách quý vị có thể quản lý việc tiếp cận thông tin ở doanh nghiệp, giữ an toàn các tài khoản kinh doanh, và huấn luyện nhân viên về cách phòng ngừa, phát hiện và trình báo sự cố an ninh mạng.

Kiểm soát tiếp cận

Là gì? Là kiểm soát những ai được tiếp cận nội dung nào trong môi trường máy tính của doanh nghiệp

Kiểm soát tiếp cận là một cách giới hạn việc tiếp cận hệ thống máy tính. Việc này giúp bảo vệ doanh nghiệp giới hạn việc tiếp cận:

- Hồ sơ và thư mục văn bản
- Các ứng dụng
- Cơ sở dữ liệu
- Hộp thư
- Tài khoản trên mạng
- Mạng lưới

Vì sao? Để giảm thiểu nguy cơ xảy ra việc tiếp cận trái phép thông tin quan trọng

Thông thường, khi nhân viên thực thi vai trò của mình, họ không cần phải được tiếp cận hoàn toàn tất cả dữ liệu, tài khoản và hệ thống của doanh nghiệp.

Tiếp cận như vậy nên được giới hạn khi có thể, để nhân viên và các nhà cung cấp bên ngoài không gây nguy hiểm cho doanh nghiệp của quý vị một cách bất cẩn hoặc ác ý.

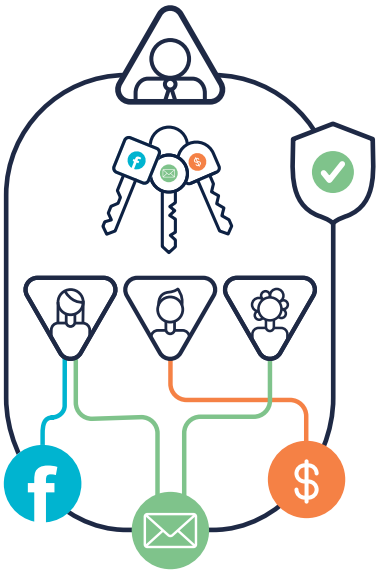
Hệ thống kiểm soát và thủ tục tiếp cận cho phép chủ doanh nghiệp hoặc người điều hành:

- **Quyết định cho ai được tiếp cận** các hồ sơ, cơ sở dữ liệu và hộp thư cụ thể
- **Kiểm soát bất cứ tiếp cận được phép nào cho nhà cung cấp bên ngoài** chẳng hạn như nhân viên kế toán, nhà cung cấp nơi lưu trữ trang mạng
- **Giới hạn cho ai được tiếp cận vào tài khoản** như trang mạng nhà cung cấp và mạng xã hội
- **Giảm thiểu khả năng bị tổn hại** trong tình huống bất cứ tài khoản, thiết bị hay hệ thống nào bị xâm phạm
- **Rút quyền tiếp cận hệ thống và dữ liệu** khi nhân viên thay đổi vị trí làm việc hoặc rời doanh nghiệp

Ai? Nguyên tắc đặc quyền tối thiểu

Tùy thuộc vào tính chất của doanh nghiệp, nguyên tắc đặc quyền tối thiểu là cách an toàn nhất cho phần lớn các doanh nghiệp nhỏ.

Nguyên tắc này chỉ cho phép người dùng ở mức tối thiểu cần thiết để thực thi nhiệm vụ. Điều này cũng sẽ giảm thiểu nguy cơ người trong 'nội bộ' bất cẩn hoặc cố ý gây nguy hiểm cho doanh nghiệp.



NGUYÊN TẮC KIỂM SOÁT TIẾP CẬN

- Chuyển nhân viên của quý vị từ tài khoản 'quản trị viên' sang tài khoản tiêu chuẩn trên thiết bị của doanh nghiệp.
- Xét duyệt lại việc cho phép tiếp cận hồ sơ và thư mục điện tử
- Không được chia sẻ tài khoản hay cụm mật khẩu/mật khẩu giữa nhân viên với nhau
- Cần nhớ phải rút quyền tiếp cận, xóa tài khoản và/hoặc thay đổi cụm mật khẩu/mật khẩu khi nhân viên rời doanh nghiệp, hoặc khi quý vị thay đổi nhà cung cấp

Cụm mật khẩu

Là gì? Là phiên bản an toàn hơn của mật khẩu

Xác thực đa yếu tố (Multi-factor authentication - MFA, xem trang 12) là một trong những cách hiệu quả nhất để bảo vệ tài khoản của quý vị chống lại tin tặc. Tuy nhiên nếu không có MFA, thì quý vị nên sử dụng cụm mật khẩu để bảo vệ tài khoản của mình.

Cụm mật khẩu sử dụng bốn từ bất kỳ trở lên làm mật khẩu. Chẳng hạn như 'pha lê củ hành đất sét bánh xoắn'.

Vì sao? Vì an toàn và dễ nhớ

Cụm mật khẩu rất khó cho tin tặc luận ra, nhưng lại dễ nhớ đối với quý vị.

Tạo cụm mật khẩu sao cho:

- **Dài.** Cụm mật khẩu của quý vị càng dài bao nhiêu càng tốt bấy nhiêu. Hãy làm cụm mật khẩu có độ dài tối thiểu là 14 chữ.
- **Khó đoán.** Hãy sử dụng một hỗn hợp các từ bất kỳ không liên quan gì với nhau. Không dùng các cụm từ, câu trích dẫn hoặc lời hát nổi tiếng.
- **Độc nhất.** Không tái sử dụng cụm mật khẩu cho nhiều tài khoản.

Nếu trang mạng hoặc dịch vụ yêu cầu phải có mật khẩu phức hợp bao gồm dấu hiệu, chữ hoa hoặc con số, quý vị có thể cho cả những cái đó vào cụm mật khẩu của mình. Cụm mật khẩu vẫn nên dài, khó đoán và độc nhất để có sự an toàn cao nhất.

Ở đâu? Tài khoản và thiết bị của quý vị

Nếu quý vị không sử dụng được MFA cho tài khoản hoặc thiết bị của mình, điều quan trọng là dùng cụm mật khẩu để giữ an toàn. Trong hoàn cảnh này, một cụm mật khẩu an toàn có thể là vật cản duy nhất ngăn chặn kẻ xấu vào thông tin giá trị của quý vị.

Nhớ làm cụm mật khẩu độc nhất, bởi vì việc tái sử dụng mật khẩu cũng làm cho tin tặc dễ xâm nhập vào nhiều tài khoản.

Muốn có thêm hướng dẫn về cách tạo cụm mật khẩu, hãy xem bản hướng dẫn của ACSC về Tạo Cụm mật khẩu mạnh có tại **cyber.gov.au**

CÂN NHẮC SỬ DỤNG CHỨC NĂNG QUẢN LÝ MẬT KHẨU

Chức năng quản lý mật khẩu (cũng có thể dùng để cất giữ cụm mật khẩu) tạo điều kiện để có thói quen tốt về an ninh mạng. Có một cụm mật khẩu độc nhất cho từng tài khoản giá trị có thể nghe như là quá khó; tuy nhiên, việc sử dụng chức năng quản lý mật khẩu để lưu cụm mật khẩu sẽ giải phóng quý vị khỏi gánh nặng phải nhớ cụm mật khẩu nào dùng ở đâu.
Đảm bảo là bất cứ chức năng quản lý mật khẩu nào quý vị dùng đều có nguồn gốc đáng tin cậy và có uy tín và được bảo vệ bởi cụm mật khẩu mạnh và dễ nhớ riêng.

Huấn luyện nhân viên

Là gì? Là việc giáo dục để bảo vệ nhân viên và doanh nghiệp chống lại mối đe dọa mạng

Quý vị hãy tự học để biết và dạy cho nhân viên cách phòng ngừa, phát hiện và trình báo tội phạm mạng.

Huấn luyện nhân viên về các kiến thức căn bản về an ninh mạng, kể cả việc phải cập nhật thiết bị và giữ an toàn cho tài khoản của họ, và nhận ra các tin nhắn lừa đảo.

Quý vị cũng nên cân nhắc thực hiện kế hoạch **ứng phó với sự cố an ninh mạng** để hướng dẫn cho doanh nghiệp và nhân viên trong tình huống xảy ra sự cố trên mạng.

Việc này sẽ giúp quý vị nắm được các thiết bị và quy trình quan trọng, cũng như các liên lạc chủ chốt mà quý vị có thể cần dùng để ứng phó và khôi phục.

Vì sao? Nhân viên có thể là tuyến phòng thủ đầu tiên và cuối cùng chống lại mối đe dọa an ninh mạng

Việc huấn luyện có thể làm thay đổi thói quen và hành vi của nhân viên và tạo nên trách nhiệm chung để giữ cho doanh nghiệp được an toàn.

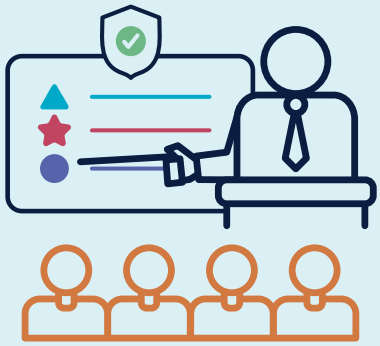
An ninh mạng là trách nhiệm của mỗi người.

Khi nào? Thường xuyên nâng cao nhận thức và huấn luyện về an ninh mạng

An ninh mạng liên tục biến hóa.

Giữ cho tất cả mọi người được cập nhật về mối đe dọa an ninh mạng có thể là sự khác biệt giữa việc tin tặc có xâm nhập được vào tiền bạc, tài khoản hoặc dữ liệu của quý vị hay là không.

"Quý vị hãy tự học để biết và dạy cho nhân viên cách phòng ngừa, phát hiện và trình báo tội phạm mạng."



CHỈ DẪN VỀ NHẬN THỨC AN NINH MẠNG

- Huấn luyện nhân viên phát hiện các đường dẫn và tài liệu đính kèm đáng ngờ
- Định kỳ tổ chức huấn luyện cập nhật về an ninh mạng
- Lập kế hoạch ứng phó sự cố an ninh mạng
- Khuyến khích văn hóa an ninh mạng mạnh mẽ
- Chia sẻ các ví dụ về tin nhắn lừa đảo để giúp nhân viên phát hiện mối đe dọa an ninh mạng

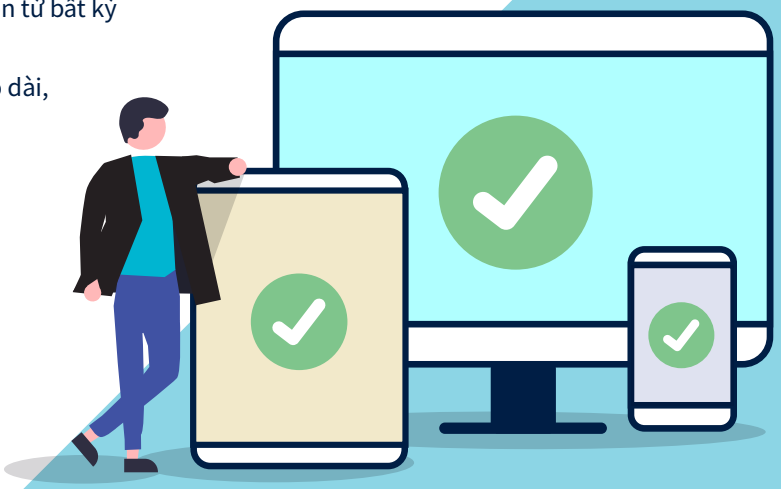
Bảng kiểm tra tóm lược

Cân nhắc về phần mềm

- **Tự động cập nhật hệ thống vận hành, phần mềm và các ứng dụng**
  - Nếu nhận được nhắc nhở cập nhật hệ thống vận hành hoặc các phần mềm khác, quý vị nên cài đặt cập nhật càng sớm càng tốt
  - Đặt thời gian thuận tiện để cập nhật tự động nhằm tránh gián đoạn cho hoạt động bình thường của doanh nghiệp
- **Thường xuyên sao lưu dữ liệu quan trọng**
  - hường xuyên kiểm tra bản sao lưu bằng cách thử khôi phục dữ liệu
  - Luôn luôn giữ ít nhất một bản sao lưu không kết nối vào thiết bị của mình
- **Thực hiện chức năng MFA cho các tài khoản quan trọng khi có thể**
  - MFA là một trong những cách hiệu quả nhất để bảo vệ thông tin và tài khoản giá trị của quý vị
  - Ưu tiên các tài khoản tài chính và email để bảo đảm công hiệu tối đa

Con người và Thủ tục

- **Kiểm soát việc cho ai được tiếp cận những gì trong nội bộ doanh nghiệp quý vị**
  - Áp dụng nguyên tắc đặc quyền tối thiểu đối việc việc cho phép tiếp cận
  - Nhớ xóa các tài khoản và/hoặc đổi cụm mật khẩu/mật khẩu khi một nhân viên thôi việc
- **Khi không làm được chức năng MFA, hãy dùng cụm mật khẩu để bảo vệ tài khoản và thiết bị**
  - Hãy dùng cụm mật khẩu gồm có bốn từ bất kỳ trở lên làm mật khẩu
  - Cụm mật khẩu hữu hiệu nhất khi nó dài, khó đoán và độc nhất
- **Hãy huấn luyện nhân viên của quý vị các kiến thức căn bản về an ninh mạng**
  - Huấn luyện có thể bao gồm cập nhật thiết bị, giữ an toàn cho các tài khoản và phát hiện tin nhắn lừa đảo
  - Định kỳ tổ chức huấn luyện cập nhật cho nhân viên về an ninh mạng



Từ điển thuật ngữ

Phầm mềm chống vi rút
Chương trình phần mềm nhằm mục đích bảo vệ máy tính hoặc mạng lưới của quý vị chống lại vi rút.

Ứng dụng
Cũng còn được gọi là ứng dụng di động, ứng dụng là một thuật ngữ chỉ phần mềm thường được dùng cho điện thoại thông minh hay máy tính bảng.

Tài liệu Đính kèm
Hồ sơ được gửi kèm theo email.

Ứng dụng xác thực
Ứng dụng được dùng để khẳng định danh tính của người sử dụng máy tính để cho phép tiếp cận thông qua chức năng xác thực đa yếu tố (MFA).

Sinh trắc học
Nhận dạng một người bằng số đo các đặc điểm sinh học như vân tay hoặc giọng nói.

Bitcoin
Tiền điện tử (tiền mã hóa) được dùng trên Internet cho các dịch vụ khác nhau.

Brute Force Attack (Tấn công bẻ khoá mật khẩu)
Một loại tấn công phát ra hàng triệu tổ hợp chữ cái trong một giây. Tấn công này hiệu quả chống lại các mật khẩu ngắn hoặc mật khẩu chỉ có một từ.

Đám mây
Mạng lưới các máy chủ từ xa cung cấp khả năng lưu trữ phân phối và sức mạnh xử lý cực lớn.

Tội phạm mạng
Bất cứ cá nhân nào xâm nhập trái phép vào một hệ thống máy tính để làm tổn hại hoặc đánh cắp thông tin.

Dữ liệu
Dữ liệu là các thông tin bao gồm hồ sơ, văn bản, con số, hình ảnh, âm thanh hoặc video.

Cài đặt mặc định
Điều gì đó mà máy tính, hệ thống vận hành hoặc chương trình đã được xác định từ trước cho người sử dụng.

Tấn công từ điển
Một loại tấn công phát ra hàng triệu lần tấn công dựa trên các quy tắc và cơ sở dữ liệu. Kiểu tấn công này đạt hiệu quả đối với các cụm mật khẩu ít phức tạp và sử dụng phổ biến hơn.

Mã hóa
Quá trình làm cho người khác không đọc được dữ liệu nhằm mục đích ngăn ngừa người khác xâm nhập vào nội dung của dữ liệu.

Mạng lưới
Tập hợp các máy tính, máy chủ, máy tính lớn, thiết bị mạng lưới, phần ngoại vi hoặc các thiết bị khác kết nối với nhau để cho phép chia sẻ dữ liệu.

Hệ thống vận hành
Phần mềm được cài đặt trong ổ cứng của máy tính để giúp cho phần cứng của máy tính giao tiếp được với và chạy các chương trình máy tính. Chẳng hạn như: Microsoft Windows, Apple macOS, iOS, Android.

Phần mềm
Thường được gọi là chương trình, tập hợp các chỉ dẫn để tạo điều kiện cho người sử dụng giao diện với máy tính, với phần cứng của máy tính hay là để thực thi công việc.

Phần mềm gián điệp (spyware)
Một chương trình được soạn ra để bí mật thu thập thông tin về hoạt động của người dùng trên thiết bị của họ.

Thiết bị xác thực (token)
Mã an toàn được phát ra bởi một thiết bị cụ thể hoặc một ứng dụng xác thực để dùng cho chức năng xác thực đa yếu tố. Thiết bị xác thực cũng có thể để chỉ việc thiết bị phát ra mã an toàn đủ nhỏ để vừa móc chìa khóa (keychain) hoặc có hình thù giống như thẻ tín dụng.

Trojans
Một dạng phần mềm độc hại thường giả dạng làm phần mềm hợp pháp, nhưng có chứa mã độc được tin tặc sử dụng để tiếp cận vào hệ thống của người dùng.

Vi rút
Chương trình được soạn ra để gây tổn hại, lấy cắp thông tin cá nhân, chỉnh sửa dữ liệu, gửi email, hiển thị tin nhắn hoặc kết hợp các hành động này.

Miễn trách nhiệm.
Bản hướng dẫn này gồm các nội dung mang tính tổng quát và không nên được coi là các hướng dẫn pháp lý hoặc dựa vào đó để được giúp đỡ trong bất cứ hoàn cảnh cụ thể hoặc tình huống khẩn cấp nào. Trong bất cứ vấn đề quan trọng nào, quý vị nên tìm sự hướng dẫn chuyên nghiệp, độc lập, phù hợp, liên quan tới hoàn cảnh riêng của quý vị.

Chính phủ Liên bang không chịu bất cứ trách nhiệm hoặc nghĩa vụ nào đối với tổn hại, tổn thất hoặc chi phí phát sinh do hậu quả của việc dựa vào thông tin trong hướng dẫn này.

Muốn biết thêm thông tin hoặc trình báo sự cố an ninh mạng, hãy liên lạc với chúng tôi tại: cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre