



CHỦ ĐỀ 1:
TÀI SẢN SỐ CỦA BẠN VÀ CÁC RỦI RO SỐ

Bài 2:
Rủi ro số
và quản lý rủi ro số



MỤC TIÊU:

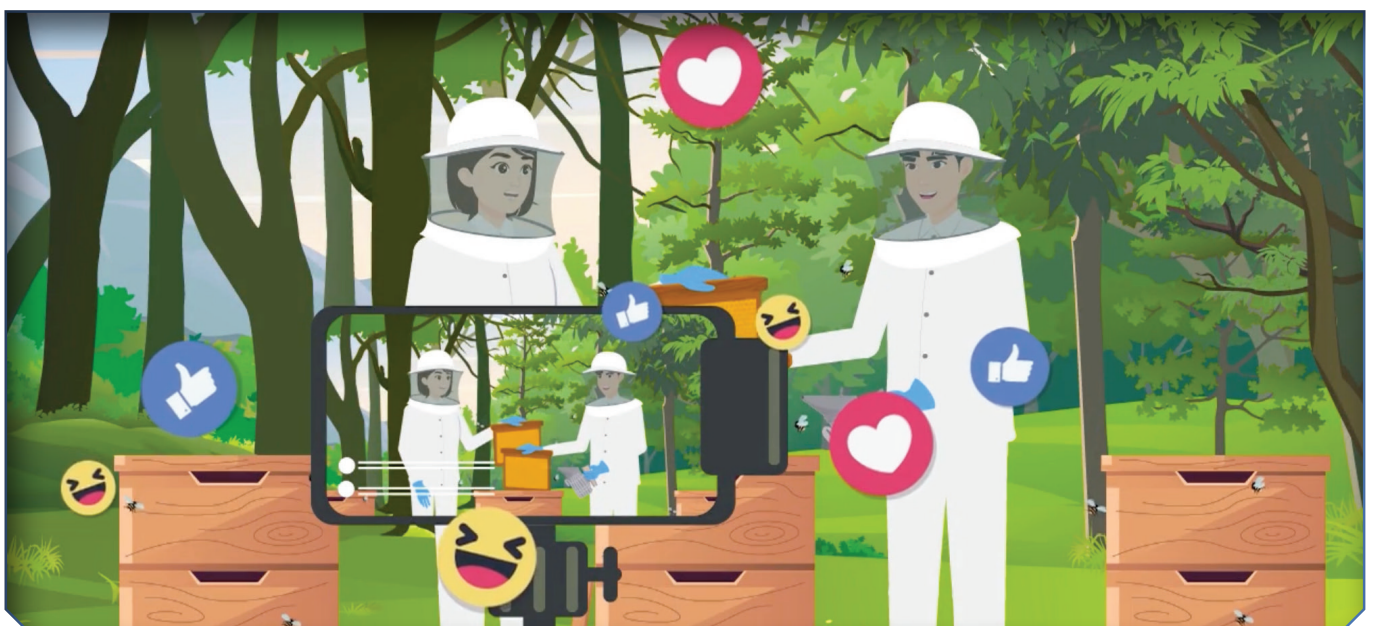


- Hiểu về khái niệm rủi ro số
- Hiểu được các tổn thất nếu các rủi ro xảy ra, từ đó ý thức được tầm quan trọng của việc kiểm soát các rủi ro số
- Biết một số thực hành cơ bản để quản lý rủi ro: thực hành bảo mật và khái niệm “vệ sinh số”

Khi cuộc sống số bắt đầu, chúng ta đã có rất nhiều tài sản số phát sinh (Bài 1, Chủ đề 1). Tuy nhiên, đi kèm với tài sản số là các rủi ro mất mát hay tổn thất. Vì vậy, hiểu và quản lý rủi ro số là bước cần thiết để giúp bạn an toàn trong thế giới số.

1. Rủi ro số là gì?

Hãy cùng xem xét tình huống sau: Chị Lan và gia đình sản xuất và buôn bán mật ong. Chị Lan tham gia mạng xã hội và quyết định mở một trang bán hàng trực tuyến trên nền tảng này. Như đã tìm hiểu trong Bài 1 (Chủ đề 1), chị Lan và gia đình có thể có những tài sản số như: các tài khoản cá nhân và tài khoản bán hàng, các thông tin và hình ảnh đăng tải về cuộc sống cũng như về việc bán hàng, các kết nối cá nhân cũng như mối quan hệ với những khách hàng trên mạng. Vậy liệu các tài sản này có luôn an toàn không?



Cũng giống như tài sản trong thế giới thực, chúng ta có những nguy cơ bị lấy cắp, mất trộm, hư hại, thất lạc... Các tài sản số cũng đối mặt với các rủi ro tương tự. Ví dụ, tài khoản cá nhân và tài khoản bán hàng của chị Lan và gia đình cũng có thể bị lấy cắp và chiếm đoạt quyền sử dụng; từ đó kẻ xấu có thể sử dụng cho nhiều mục đích xấu như lấy cắp các thông tin và dữ liệu riêng tư, lừa đảo, tung thông tin sai lệch.... Nguy cơ bị lấy cắp tài khoản trực tuyến được coi là một trong rất nhiều các rủi ro số mà chị Lan và gia đình cần chú ý.

Rủi ro số là các mối đe dọa và lỗ hổng tiềm ẩn phát sinh khi sử dụng các công cụ, nền tảng và công nghệ kỹ thuật số. Chúng là một phần tất yếu trong quá trình chúng ta tham gia và kinh doanh trên môi trường số. Trong cuộc sống hiện đại, chuyển đổi số ngày càng trở nên quan trọng, đặc biệt trong kinh doanh, nơi nó đóng vai trò thiết yếu để mở rộng quy mô và tăng hiệu quả. Tuy nhiên, việc dựa nhiều hơn vào các giải pháp kỹ thuật số cũng đồng nghĩa với việc đối mặt với những rủi ro số không thể tránh khỏi. Đây là hệ quả tự nhiên của sự phát triển công nghệ, đòi hỏi mỗi cá nhân và tổ chức phải chủ động nhận diện và giải quyết những lỗ hổng có thể gây ảnh hưởng đến mục tiêu trong cuộc sống cá nhân hay công việc.



2. Chúng ta phải đối mặt với những rủi ro số nào?

Rủi ro số phát sinh từ việc tài sản số của chúng ta trở thành mục tiêu tấn công. Đối với mỗi loại tài sản số, chúng ta có thể sẽ phải đối mặt với các rủi ro số khác nhau. Vì vậy, khi xác định các rủi ro số, chúng ta cần đặt câu hỏi: *Có những mối đe dọa nào liên quan đến các loại tài sản số mà chúng ta đang sở hữu?* Dưới đây là bảng tham khảo về các mối đe dọa phổ biến gắn liền với từng loại tài sản số:

Loại tài sản	Các rủi ro/mối đe dọa phổ biến có thể xảy ra
Thiết bị 	- Xâm nhập trái phép thiết bị, hệ thống - Đánh cắp dữ liệu thông tin
Phần mềm 	- Phần mềm độc hại (phần mềm gián điệp, mã độc tống tiền...) - Đánh cắp dữ liệu thông qua các phần mềm cài đặt trên máy
Thông tin 	- Đánh cắp thông tin cá nhân - Quấy rối trực tuyến, tống tiền - Tin giả, tin sai sự thật
Danh tính và mối quan hệ 	- Phát ngôn tiêu cực - Bắt nạt qua mạng - Giả mạo danh tính - Lừa đảo hẹn hò và kết bạn qua mạng
Tiền 	- Lừa đảo tài chính qua mạng

SUY NGÃM

Từ những tài sản số mà bạn đã liệt kê ở Bài 1 (Chủ đề 1), hãy nêu những rủi ro số liên quan?

Tại Việt Nam, các rủi ro số phổ biến nhất phải kể đến như *lộ thông tin cá nhân và các tài khoản trực tuyến, lừa đảo/gian lận trực tuyến*. Theo một báo cáo của Google năm 2021, 4/5 người dùng internet tại Việt Nam từng bị tổn hại dữ liệu cá nhân và đây là mức cao nhất trong khu vực Đông Nam Á¹. Theo thống kê của Viettel Threat Intelligence, 6 tháng đầu năm 2024, các vụ lộ lọt thông tin cá nhân tại Việt Nam tăng 50% so với cùng kỳ năm 2023, với 16 triệu bản ghi các dữ liệu nhạy cảm bị lộ lọt và rao bán².

Đối với rủi ro lừa đảo và gian lận tài chính, theo Liên minh Chống Lừa đảo Toàn cầu (GASA), trong năm 2023, hơn 1/4 dân số toàn cầu đã trở thành nạn nhân của lừa đảo trực tuyến. Riêng tại Việt Nam, khoảng 400.000 tỷ đồng, tương đương 3,6% GDP, đã rơi vào tay kẻ lừa đảo³. Việt Nam có tỷ lệ thiệt hại do lừa đảo trực tuyến trên GDP cao thứ 2 trên thế giới. Các vụ lừa đảo trực tuyến được thực hiện với các hình thức rất đa dạng, phổ biến là các hình thức tấn công qua phần mềm độc hại và giả mạo (phishing). Theo Viettel Threat Intelligence, có tới 2364 tên miền gian lận được phát hiện và 496 trang web giả mạo tại Việt Nam năm 2024, tăng 4 lần so với cùng kỳ năm 2023⁴.



1 Báo cáo Trách nhiệm số, Google, 2021.

2 Báo cáo “Tình hình nguy cơ mất ATTT tại Việt Nam”, Viettel Threat Intelligence, 2024.

3 Báo cáo của Liên minh chống lừa đảo toàn cầu GASA, 2023.

4 Báo cáo “Tình hình nguy cơ mất ATTT tại Việt Nam”, Viettel Threat Intelligence, 2024.

3. Hậu quả khi xảy ra các rủi ro số

Một khi đã tham gia thế giới số và môi trường mạng thì chúng ta vẫn luôn phải đối mặt với các mối đe dọa và rủi ro nhằm trực tiếp tới các tài sản số chúng ta có. Việc kiểm soát các rủi ro số không tốt sẽ có thể dẫn tới các hậu quả nghiêm trọng đối với các tài sản số và từ đó tác động trực tiếp tới cá nhân và tổ chức. Có thể phân chia thành 4 loại hậu quả sau:



HẬU QUẢ KINH TẾ: liên quan đến các thiệt hại về tài chính hoặc chi phí để phục hồi (VD: thu nhập bị mất hoặc bị gián đoạn, chi phí để trả tiền chuộc, chi phí để phục hồi hệ thống...). Cụ thể, nếu một cá nhân hay một doanh nghiệp đang bán hàng trên trang

Facebook với một nguồn thu nhập ổn định từ các khách hàng trực tuyến thì việc bị mất tài khoản đó sẽ khiến cho việc bán hàng trên nền tảng đó bị gián đoạn và do đó nguồn thu nhập bị ảnh hưởng. Ngoài ra, cá nhân hay tổ chức đó có thể phải trả tiền chuộc để lấy lại tài khoản hoặc mất chi phí thuê người để hỗ trợ lấy lại tài khoản đó.

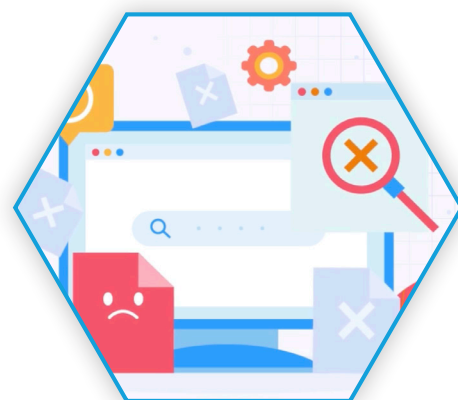
HẬU QUẢ XÃ HỘI: là các tác động tiêu cực đối với các mối quan hệ và tương tác xã hội cũng như các thiệt hại ảnh hưởng tới danh tiếng của cá nhân hoặc tổ chức. Các hậu quả xã hội cụ thể mà cá nhân hoặc tổ chức có thể trải qua bao gồm: ảnh hưởng tới các mối quan hệ, mất lòng tin từ đối tác, khách hàng và thậm chí là khiến họ buộc phải rút lui khỏi cộng đồng mà họ tham gia. Một ví dụ khác là trường hợp tài khoản mạng xã hội của cá nhân hoặc tổ chức bị giả mạo, hoặc xuất hiện các tài khoản mạo danh đăng tải nội dung sai lệch, gây nhầm lẫn và độc hại. Hành vi này không chỉ làm mất uy tín của cá nhân mà còn gây tổn hại nghiêm trọng đến danh tiếng của tổ chức.





HẬU QUẢ TÂM LÝ: bao gồm trải nghiệm tiêu cực, cảm giác mất an toàn và những vấn đề liên quan đến sức khỏe tâm thần. Ví dụ như một cá nhân có thể bị rơi vào trạng thái bất an, xuống tinh thần hoặc nản lòng do bị hăm dọa và quấy rối trực tuyến do tài khoản của họ bị tấn công và mất các thông tin nhạy cảm hoặc quan trọng.

HẬU QUẢ KỸ THUẬT: như mất hoặc hỏng dữ liệu hoặc mất quyền truy cập vào thông tin, tài khoản hay hệ thống. Ví dụ khi chúng ta nhấp vào đường dẫn độc hại có chứa vi-rút hoặc mã độc, máy tính của chúng ta sẽ bị nhiễm vi-rút hoặc mã độc đó khiến các dữ liệu của chúng ta có thể bị mã hóa và không thể mở ra đọc được theo cách thông thường.



Hãy tham khảo một số ví dụ sau đây về rủi ro số phổ biến và hậu quả cụ thể của các rủi ro này:



RỦI RO SỐ: Lừa đảo trực tuyến; Xâm phạm dữ liệu; Chiếm đoạt thông tin cá nhân...



HẬU QUẢ KINH TẾ: Mất việc làm; Mất tiền và tài sản; Bị tống tiền; Giảm thu nhập; Công việc bị gián đoạn; Bị phạt; Bị phải bồi thường; Mất thời gian; Mất chi phí để phục hồi

RỦI RO SỐ: Quấy rối, xâm hại trực tuyến; Tin giả; Trộm cắp danh tính...



HẬU QUẢ XÃ HỘI: Xung đột; Quan hệ cá nhân bị phá vỡ; Bị cô lập; Trạng thái cực đoan cá nhân lan ra tập thể; Trạng thái sợ mạng, hoặc không tham gia nhiệt tình; Bị bôi nhọ; Mất quan điểm; Luôn bị để ý, theo dõi; Giảm các cơ hội mở rộng quan hệ



RỦI RO SỐ: Bắt nạt trên mạng; Tin giả; Quấy rối, xâm hại trực tuyến; Giả mạo danh tính...

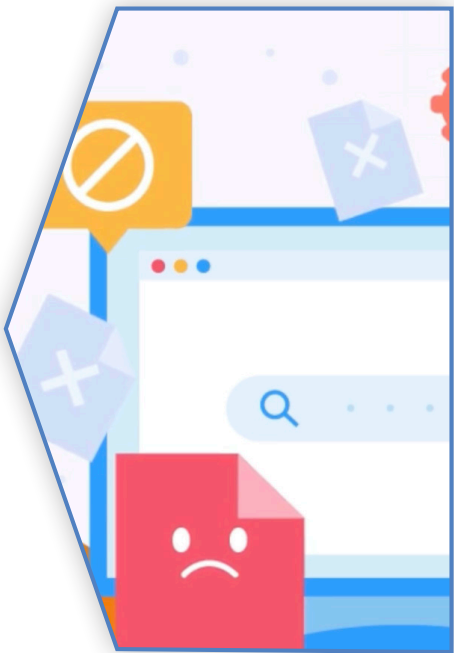


HẬU QUẢ TÂM LÝ: Bị nghiện mạng; Cảm giác tiêu cực; Mất tập trung; Thất vọng; Mất tự tin; Chán nản; Lo lắng; Đánh mất bản thân; Bối rối; Xấu hổ

RỦI RO SỐ: Phần mềm độc hại; Phần mềm gián điệp; Xâm nhập trái phép...



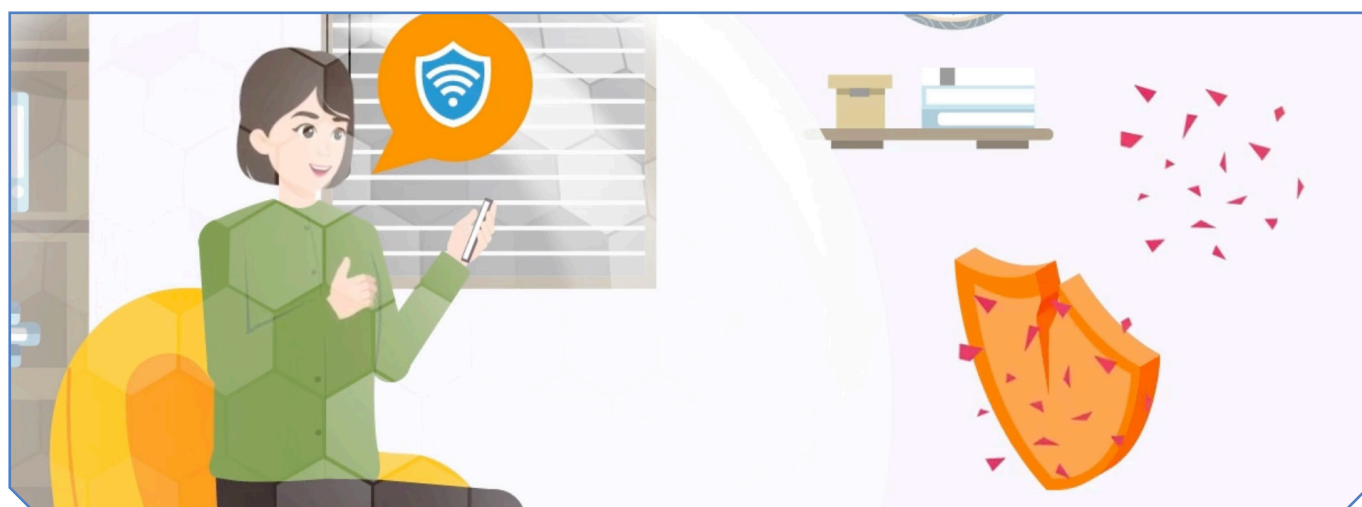
HẬU QUẢ KỸ THUẬT: Kỹ thuật, thiết bị/hệ thống bị hư hỏng; Thiết bị/hệ thống bị phá hủy; Thiết bị nhiễm vi-rút; Mất khả năng truy cập vào tài khoản/hệ thống; Máy chạy chậm



4. Một số thực hành cơ bản để quản lý rủi ro số (Vệ sinh số)

Trong bối cảnh các hệ thống và thiết bị của chúng ta ngày càng kết nối chặt chẽ hơn, đồng thời tội phạm mạng ngày càng gia tăng cả về số lượng lẫn mức độ tinh vi, các rủi ro số đối với cá nhân và tổ chức sẽ trở nên đáng nghiêm trọng hơn.

May mắn thay, các cá nhân và tổ chức vẫn có thể chủ động bảo vệ mình trước rủi ro bằng việc áp dụng thực hành một bộ các biện pháp bảo mật an ninh mạng toàn diện, được ví như “**vệ sinh số**”. Cũng giống như việc rửa tay, đeo khẩu trang và giãn cách xã hội có thể giảm thiểu rủi ro sức khỏe cho bạn, các biện pháp vệ sinh số cơ bản có thể giảm thiểu tiếp xúc và nguy cơ bị tấn công khi tham gia thế giới số. Hãy hình dung việc này như việc bảo vệ sức khỏe của bản thân, gia đình mình, hoặc tập thể và doanh nghiệp.



Thực hiện các biện pháp vệ sinh số cơ bản nhất có thể ngăn chặn đến 86% các cuộc tấn công mạng cơ bản nhất⁵. Bạn hãy lưu ý rằng bất kể bạn đang sử dụng loại thiết bị nào (điện thoại di động, máy tính bảng, máy tính xách tay hay máy tính để bàn), các bước vệ sinh số cơ bản này đều có thể áp dụng. Một số kiến thức cơ bản về vệ sinh số bạn có thể áp dụng để quản lý các rủi ro số bao gồm:

5 Theo Center for Internet Security (CIS): <https://www.cisecurity.org/about-us/media/press-release/center-for-internet-security-cis-releases-community-defense-model-v2-0-for-cybersecurity>



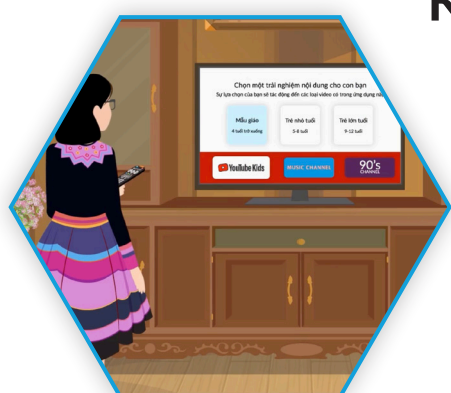
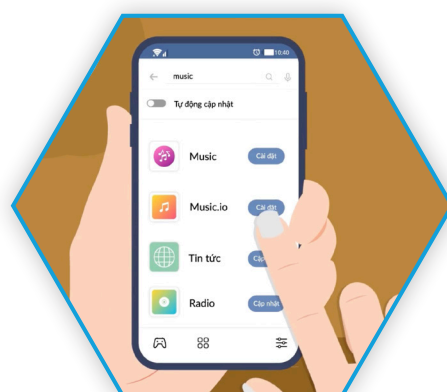
Biết những gì bạn có: Kiểm kê những tài sản số mà bạn có. Hủy kích hoạt các thiết bị (thiết bị di động, máy tính bảng, máy tính xách tay, máy tính để bàn, điểm truy cập, v.v.) hoặc tài khoản bạn không còn sử dụng nữa.

Sao lưu: Thường xuyên sao lưu dữ liệu của bạn, hãy lưu trên cả thiết bị và các nền tảng điện toán đám mây (bản lưu ngoại tuyến và trực tuyến).



Mật khẩu và công cụ để bảo vệ chúng: Sử dụng mật khẩu mạnh, duy nhất. Bật xác thực hai yếu tố và sử dụng ứng dụng quản lý mật khẩu.

Cài đặt phần mềm uy tín và cập nhật thường xuyên: Sử dụng các phần mềm đáng tin cậy, có bản quyền. Cập nhật phần mềm thường xuyên và để chế độ cập nhật tự động.



Kiểm soát truy cập: Không phải ai cũng cần quyền truy cập vào thiết bị hoặc có các quyền giống nhau (đăng/xem/chỉnh sửa). Giới hạn người dùng và quyền chỉ ở những gì họ cần. Điều này bao gồm khả năng tải xuống phần mềm hoặc ứng dụng mới.

Lãnh đạo: Dẫn dắt bằng cách làm gương và đào tạo nhân viên, tình nguyện viên, hoặc thành viên gia đình của bạn, những người cũng có thể chia sẻ thiết bị của bạn về những thực hành bảo mật cơ bản.



Ngoài cách thực hành cơ bản về “vệ sinh số” kể trên, có nhiều các thức hành để quản lý rủi ro số và an toàn hơn trong thế giới số với các nội dung chi tiết trong những bài học tiếp theo.



Quản lý rủi ro số là trách nhiệm của tất cả các đối tượng tham gia thế giới số. Do đó, nó bao gồm vai trò của tất cả các cấp độ từ cá nhân tới các tổ chức/doanh nghiệp. Cụ thể như sau:

ĐỐI VỚI CÁ NHÂN

Các cá nhân đóng vai trò nền tảng trong việc giảm thiểu rủi ro số vì họ là những người sử dụng trực tiếp các thiết bị và dịch vụ kỹ thuật số. Các vai trò này có thể thực hiện bằng các hành động cụ thể bao gồm:

- Nâng cao nhận thức, hiểu biết và kỹ năng về an toàn số.
- Thực hành an toàn số (bao gồm các thực hành “vệ sinh số”) thường xuyên.

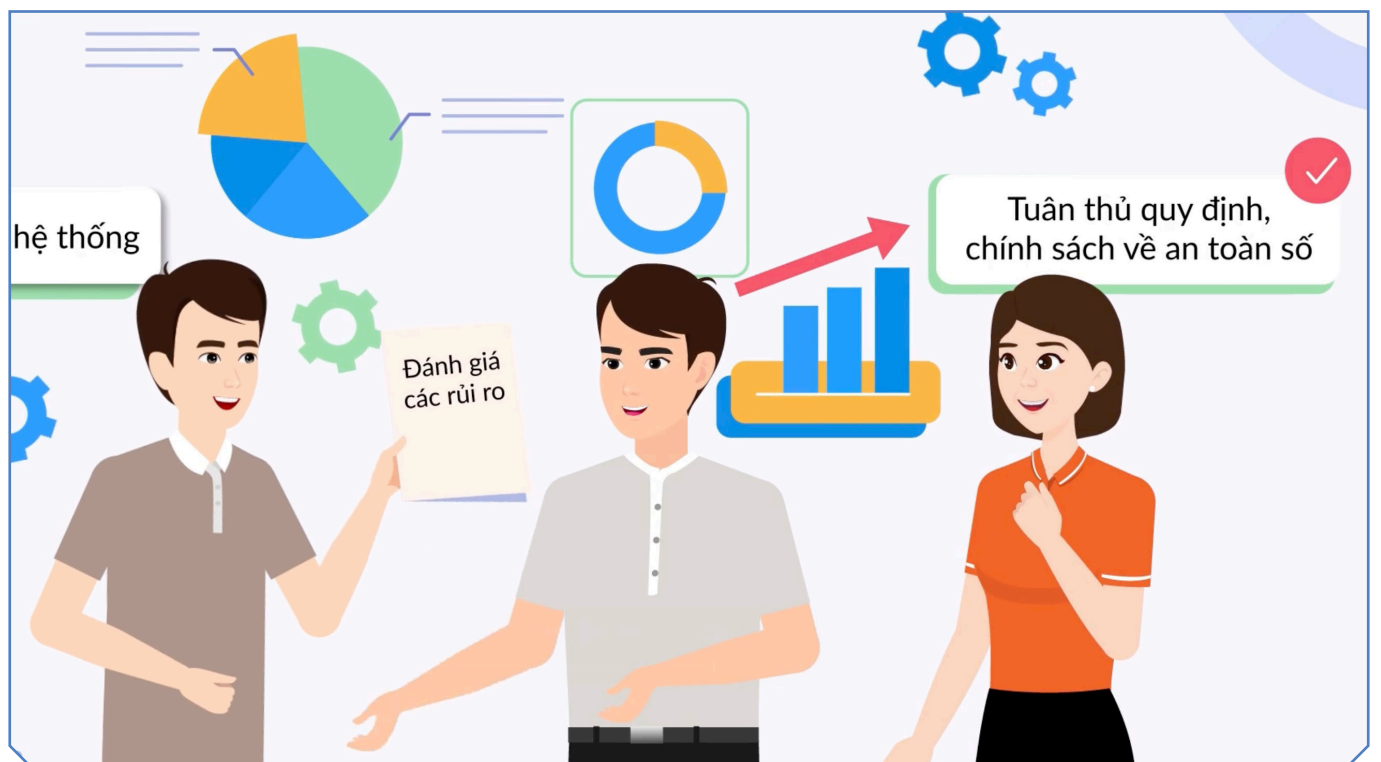


ĐỐI VỚI TỔ CHỨC/DOANH NGHIỆP

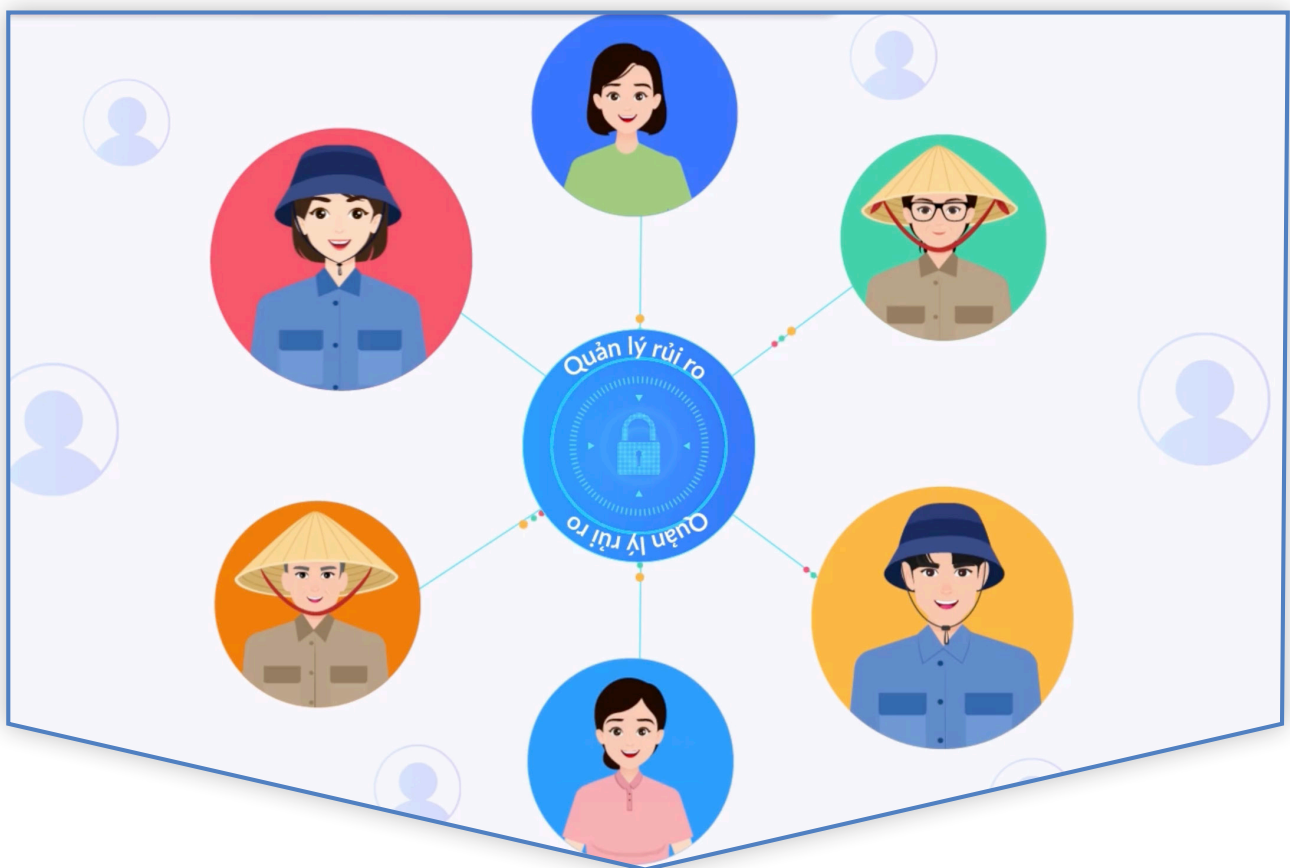
Doanh nghiệp chịu trách nhiệm quản lý rủi ro cho toàn bộ hệ thống kỹ thuật số và bảo vệ thông tin của tổ chức cũng như khách hàng. Các vai trò này có thể thực hiện bằng các hành động cụ thể bao gồm:



- Xây dựng chính sách quản lý rủi ro
- Đào tạo nhân viên
- Đầu tư và sử dụng các công nghệ, phần mềm nâng cao bảo mật
- Đánh giá rủi ro thường xuyên
- Tuân thủ các tiêu chuẩn và quy định về an toàn số và bảo vệ dữ liệu có liên quan



Nội dung chính cần ghi nhớ



1. Rủi ro số là các mối đe dọa và lỗ hổng tiềm ẩn phát sinh khi sử dụng các công cụ, nền tảng và công nghệ kỹ thuật số.
2. Rủi ro số phát sinh từ việc tài sản số của chúng ta trở thành mục tiêu tấn công. Vì vậy, khi xác định các rủi ro số, chúng ta cần đặt câu hỏi: có những mối đe dọa nào liên quan đến các loại tài sản số mà chúng ta đang sở hữu?
3. Các mối đe dọa và rủi ro vẫn luôn tồn tại trên mạng và ngày càng nhiều hơn, tinh vi hơn, đe dọa trực tiếp tới các tài sản số chúng ta có. Việc kiểm soát các rủi ro số không tốt sẽ có thể dẫn tới các hậu quả nghiêm trọng đối với các tài sản số và từ đó tác động trực tiếp tới cá nhân và tổ chức. Có thể phân chia thành 4 loại hậu quả sau:
 - **Hậu quả kinh tế:** liên quan đến việc đánh cắp hoặc mất nguồn lực tài chính hoặc chi phí để phục hồi.
 - **Hậu quả xã hội:** là tổn hại liên quan đến các tác động

tiêu cực đối với các mối quan hệ và tương tác xã hội cũng như các thiệt hại về danh tiếng.

- **Hậu quả tâm lý:** Trải nghiệm đau khổ, mất an toàn và những vấn đề liên quan đến sức khỏe tâm thần.
- **Hậu quả kỹ thuật:** Mất hoặc hỏng dữ liệu hoặc mất quyền truy cập vào thông tin hay hệ thống.

4. Việc áp dụng thực hành một bộ các biện pháp bảo mật an ninh mạng toàn diện, được ví như “vệ sinh số” là một cách thức hiệu quả giúp bạn quản lý rủi ro số tốt hơn.

5. Việc quản lý rủi ro số là trách nhiệm của tất cả các đối tượng tham gia thế giới số. Ở cấp độ cá nhân, người dùng cần nâng cao nhận thức, hiểu biết và thực hành thường xuyên các biện pháp an toàn số. Ở cấp độ tổ chức và doanh nghiệp, các nhiệm vụ tập trung vào xây dựng chính sách, đào tạo nhân viên, cải thiện hệ thống, đánh giá các rủi ro, cũng như tuân thủ các quy định và chính sách về an toàn số.

