APAC Cybersecurity Fund
The Asia Foundation

VIETNET-ICT

CHỦ ĐỀ 3:
BẢO VỆ CÁC THIẾT BỊ SỐ

Bài 1: Rủi ro và phòng tránh rủi ro với thiết bị số

với sự hỗ trợ từ Google.org

MỤC TIÊU:

- Hiểu về các rủi ro có thể xảy ra với các thiết bị số (VD: điện thoại và máy tính)
- Biết một số cách phòng tránh rủi ro với các thiết bị số
- Nắm được một số nguyên tắc cơ bản về sao lưu dữ liệu

Ngày nay, các thiết bị số như máy tính và điện thoại thông minh không chỉ là công cụ hỗ trợ công việc và giải trí mà còn là nơi lưu trữ các thông tin cá nhân quan trọng. Tuy nhiên, chúng cũng tiềm ẩn nhiều rủi ro như bị nhiễm phần mềm độc hại, tấn công mạng, mất cắp dữ liệu, hoặc hư hỏng phần cứng. Việc hiểu rõ và có biện pháp phòng tránh sẽ giúp chúng ta bảo vệ an toàn cho thiết bị số và dữ liệu của mình.

1. Rủi ro với các thiết bị số và một số cách phòng tránh

Thiết bị số là phần cứng sử dụng máy tính hoặc vi điều khiển, xuất hiện mọi nơi trong kỷ nguyên số hiện nay. Có rất nhiều loại thiết bị số, từ các máy tính với cấu hình mạnh mẽ xử lý các nhiệm vụ phức tạp như phân tích thống kê và xử lý dữ liệu lớn, đến các bộ vi xử lý được sử dụng để điều khiển máy giặt, TV và các thiết bị gia dụng khác. Trong số các thiết bị số này, **điện thoại thông minh** và **các loại máy tính** (bao gồm máy tính để bàn, máy tính xách tay, máy tính bảng) là các thiết bị số quan trọng nhất về khía cạnh bảo mật và an toàn dữ liệu do chúng lưu trữ lượng lớn thông tin cá nhân, công việc và tài chính. Điện thoại thông minh chứa các ứng dụng ngân hàng, mạng xã hội và tin nhắn cá nhân, trong khi máy tính thường được sử dụng để làm việc, lưu trữ tài liệu và giao dịch trực tuyến. Bởi vậy trong khuôn khổ bài học này, chúng ta sẽ đề cập chủ yếu tới các rủi ro và thực hành bảo mật đối với 2 loại thiết bị này.

1.1. Rủi ro về bảo mật dữ liệu

Hãy xem xét ví dụ sau: Chị Hoa đang mở máy tính làm việc tại một quán cà phê. Chị Hoa cần tạm rời khỏi máy tính để ra ngoài, máy tính chị Hoa vẫn đang mở và không có mật khẩu. Vậy có thể có những rủi ro gì có thể xảy ra với máy tính của chị Hoa?

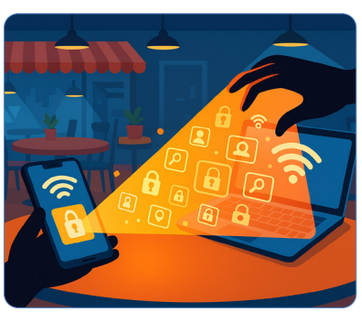
Một số rủi ro tiềm ẩn có thể kể đến như sau: Kẻ xấu có thể xem và tìm kiếm các thông tin có giá trị trong máy của chị Hoa, sao lưu các dữ liệu có giá trị như các hình ảnh, nội dung trò chuyện mà chị Hoa không muốn tiết lộ, danh sách khách hàng hay bí mật của công ty. Kẻ xấu cũng có thể lợi dụng để cài các phần mềm độc hại vào máy tính, sau đó có thể theo dõi và lấy các thông tin của chị Hoa. Thậm chí, kẻ xấu có thể lấy trộm máy tính của chị Hoa và biến mất.

Trên đây là một ví dụ nhỏ về rủi ro bảo mật dữ liệu mà bạn có thể gặp phải. Ngoài ra, còn có vô vàn các rủi ro về bảo mật dữ liệu khác có thể dẫn tới hậu quả bị xâm phạm quyền riêng tư của bạn. Có thể kể tới một số rủi ro phổ biến như:

- **Đánh cắp dữ liệu cá nhân:**

- Khi máy tính/điện thoại bị xem trộm, nguy cơ bị rò rỉ thông tin cá nhân và tài liệu nhạy cảm như tài khoản ngân hàng, thông tin đăng nhập, hoặc tài liệu công việc quan trọng là rất cao, dẫn đến hậu quả nghiêm trọng như mất danh tính, mất tiền, thiệt hại công việc...

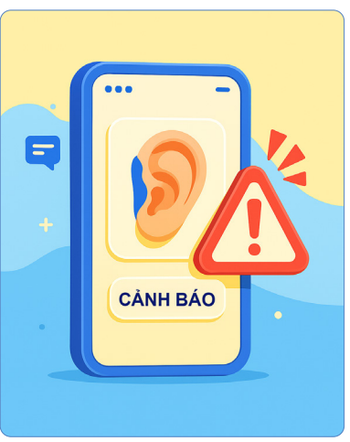
- Thông tin nhạy cảm như tin nhắn, hình ảnh, email, hoặc tài liệu lưu trữ trên điện thoại có thể bị truy cập và sử dụng trái phép bằng một vài cách khác. Ví dụ, một ứng dụng độc hại có thể sao chép tin nhắn SMS hoặc đọc email để thu thập thông tin cá nhân hoặc mã OTP.



- Các kết nối không an toàn[1], như khi dùng Wi-Fi miễn phí ở quán cà phê hoặc nơi công cộng, có thể khiến thông tin cá nhân của bạn bị đánh cắp. Tin tặc có thể "nghe trộm" dữ liệu bạn gửi và nhận, như mật khẩu, tài khoản ngân hàng hoặc tin nhắn. Chúng còn có thể tạo ra các điểm Wi-Fi giả với tên giống mạng thật để lừa bạn kết nối, từ đó lấy cắp thông tin. Nếu truy cập vào các trang web không có bảo mật (không có "https" ở đầu), dữ liệu của bạn cũng dễ bị đọc trộm. Ngoài ra, bật Bluetooth hoặc NFC (tính năng kết nối không dây) khi không dùng cũng có thể khiến hacker kết nối vào điện thoại mà bạn không hay biết.

1 Tham khảo thêm Chủ đề 2, bài 3 – Kết nối an toàn

- **Theo dõi vị trí hoặc hoạt động của bạn:** Kẻ xấu có thể sử dụng dữ liệu định vị GPS hoặc các quyền truy cập vị trí trên điện thoại để theo dõi hành trình hoặc nơi bạn đến. Một số ứng dụng còn có thể theo dõi thói quen sử dụng điện thoại, bao gồm các trang web truy cập, ứng dụng mở, và thậm chí thao tác nhập liệu.



- **Nghe lén, quay lén hay ghi âm lén:** Nguyên nhân chính là do ứng dụng độc hại, phần mềm gián điệp (spyware) hoặc các thiết bị vật lý bị gắn thêm như micro và camera ẩn. Một số trợ lý ảo cũng có thể bị lợi dụng để nghe lén mà không cần sự đồng ý. Hậu quả của việc này là rò rỉ thông tin nhạy cảm, bị giám sát, tống tiền hoặc bị phát tán hình ảnh riêng tư lên mạng xã hội.

Một số cách **phòng chống** rủi ro này mà bạn có áp dụng bao gồm:

Đặt mật khẩu cho thiết bị: Đặt mật khẩu đăng nhập cho máy tính[2] và cài đặt khóa màn hình điện thoại khi không sử dụng.

Đối với thiết bị máy tính: lưu ý Đăng xuất/ Khóa máy tính khi rời khỏi hoặc không sử dụng và cài đặt thêm tính năng Khóa màn hình khi hết thời gian chờ.[3]

2 Tham khảo: https://support.microsoft.com/vi-vn/windows/sign-in-ch%E1%BB%8Dn-trong-windows-8ae09c04-c5da-41c9-972f-b126a13d18a8

3 Tham khảo: https://support.microsoft.com/vi-vn/windows/c%C3%A1ch-%C4%91i%E1%BB%81u-ch%E1%BB%89nh-c%C3%A0i-%C4%91%E1%BA%B7t-ngu%E1%BB%93n-v%C3%A0-ch%E1%BA%BF-%C4%91%E1%BB%99-ng%E1%BB%A7-trong-windows-26f623b5-4fcc-4194-863d-b824e5ea7679 (bạn có thể tìm kiếm trên youtube và google các hướng dẫn phù hợp với hệ điều hành máy tính bạn đang dùng)

Chỉ cài đặt các ứng dụng uy tín, có nguồn gốc và chỉ cấp các quyền cần thiết cho các ứng dụng[4].

Sử dụng các kết nối Internet an toàn[5]: Khuyến khích sử dụng VPN[6] khi kết nối các mạng Wifi bên ngoài.

1.2. Rủi ro về lỗ hổng bảo mật và phần mềm độc hại

Các thiết bị số như điện thoại hoặc máy tính muốn vận hành được đều cần các hệ điều hành và các phần mềm hỗ trợ. Ngoài ra, trong quá trình sử dụng, tùy theo các nhu cầu cá nhân và công việc khác nhau, chúng ta lại cài đặt thêm các phần mềm, ứng dụng vào thiết bị. Việc sử dụng các hệ điều hành và phần mềm sẽ khiến cho thiết bị phát sinh các nguy cơ lỗ hổng bảo mật. **Lỗ hổng bảo mật** là *những điểm yếu hoặc thiếu sót trong hệ thống, phần mềm hoặc mạng*. Lỗ hổng bảo mật có thể được ví như một cánh cửa sổ bị quên đóng trong ngôi nhà của bạn. Dù bạn đã khóa cửa chính rất cẩn thận, kẻ trộm vẫn có thể lẻn vào qua cánh cửa sổ đó để đánh cắp tài sản hoặc gây hại. Tương tự, trong hệ thống máy tính hoặc điện thoại, một lỗ hổng bảo mật nhỏ cũng có thể tạo điều kiện cho hacker xâm nhập và thực hiện các hành vi trái phép.

Một rủi ro nữa mà thiết bị có thể gặp phải là nhiễm **các phần mềm độc hại** như *vi-rút, phần mềm gián điệp, mã độc tống tiền*... Rủi ro này xảy ra khi phần mềm có hại bị cài đặt hoặc xâm nhập vào thiết bị mà không được người dùng cho phép.

---

4 Tham khảo thêm các thực hành an toàn ứng dụng khác trong Chủ đề 3 – Bài 2 – Sử dụng ứng dụng an toàn

5 Tham khảo thêm Chủ đề 2 – Bài 3 – Kết nối an toàn

6 VPN hay Mạng riêng ảo tạo ra kết nối mạng riêng tư giữa các thiết bị thông qua Internet. VPN được sử dụng để truyền dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng

Những phần mềm này có thể *đánh cắp dữ liệu, theo dõi hoạt động, chiếm quyền điều khiển thiết bị, hoặc phá hoại hệ thống.* Ví dụ, một phần mềm gián điệp (spyware) có thể bí mật ghi lại mật khẩu và thông tin ngân hàng, hoặc mã độc tống tiền (ransomware) có thể khóa dữ liệu và yêu cầu tiền chuộc để mở lại.

Để phòng tránh rủi ro này, chúng ta có thể thực hiện một số thực hành bảo mật sau:

- **Chỉ dùng những phần mềm có bản quyền:** Việc sử dụng phần mềm bản quyền giúp đảm bảo bạn nhận được các bản cập nhật và hỗ trợ kỹ thuật từ nhà sản xuất, bảo vệ thiết bị khỏi lỗ hổng bảo mật và phần mềm độc hại. Ngoài ra, việc này còn tuân thủ pháp luật và tôn trọng quyền sở hữu trí tuệ của các nhà phát triển phần mềm.
- **Cập nhật hệ điều hành và phần mềm thường xuyên** sẽ giúp vá các lỗ hổng bảo mật, sửa lỗi và cải thiện hiệu suất. Điều này bảo vệ thiết bị khỏi các mối đe dọa như hacker hoặc phần mềm độc hại khai thác lỗ hổng để tấn công.
- **Cài đặt các phần mềm diệt vi-rút** giúp bảo vệ thiết bị khỏi các mối đe dọa như vi-rút, phần mềm độc hại, và các cuộc tấn công mạng. Tuy nhiên, bạn cần lưu ý chỉ nên sử dụng những phần mềm diệt vi-rút uy tín và có bản quyền như Avast, AVG, McAfee...

- **Kiểm tra kỹ các liên kết và tệp đính kèm trước khi mở:** việc này sẽ tránh việc nhấp vào các đường link độc hại dẫn đến việc cài đặt các phần mềm độc hại xuống điện thoại của bạn.
- **Cẩn trọng khi cài đặt các ứng dụng** (nguồn gốc, quyền truy cập…) (tham khảo thêm các thực hành an toàn ứng dụng khác trong *Chủ đề 3 – Bài 2 – Sử dụng ứng dụng an toàn).*

SUY NGẪM

Để bảo vệ thiết bị khỏi phần mềm độc hại và lỗ hổng bảo mật, bạn không nên làm gì?

A. Chỉ dùng những phần mềm có bản quyền

B. Cập nhật hệ điều hành và phần mềm thường xuyên

C. Cài đặt các phần mềm diệt vi-rút uy tín và có bản quyền

D. Tải và cài đặt phần mềm từ các nguồn không rõ nguồn gốc

(Đáp án đúng: D)

1.3. Rủi ro do mất, hỏng, hoặc cháy nổ

Rủi ro mất thiết bị và các tác nhân vật lý có thể gây tổn thất nghiêm trọng về dữ liệu và tài sản. Khi máy tính hoặc điện thoại bị mất hoặc đánh cắp, kẻ xấu có thể truy cập vào thông tin cá nhân, tài khoản hoặc tài liệu quan trọng của bạn nếu không được bảo vệ kỹ. Ngoài ra, các yếu tố vật lý như rơi vỡ, nước vào máy, hoặc cháy nổ có thể làm hỏng thiết bị và gây mất dữ liệu nếu không có bản sao lưu. Cả hai loại rủi ro này đều đòi hỏi người dùng phải chủ động bảo vệ thiết bị và dữ liệu của mình.

Để giảm thiểu rủi ro này, bạn có thể tham khảo một số phương pháp bảo mật:

Sao lưu dữ liệu: Sao lưu dữ liệu là một biện pháp quan trọng giúp giảm thiểu rủi ro mất mát dữ liệu trên máy tính hoặc điện thoại. Khi gặp sự cố như thiết bị bị hỏng, vi-rút tấn công, bị đánh cắp, hoặc lỗi phần cứng, các bản sao lưu sẽ giúp bạn vẫn có thể khôi phục lại các thông tin quan trọng.

(Đối với điện thoại) **Kích hoạt tính năng "Tìm thiết bị"** (Find My iPhone - Find My Device): sử dụng các công cụ như "Find My iPhone" (iOS) hoặc "Find My Device" (Android) để định vị, khóa hoặc xóa dữ liệu từ xa nếu thiết bị bị mất.

2. Sao lưu dữ liệu

Trong các phương thức phòng tránh rủi ro đối với thiết bị, việc sao lưu dữ liệu là phương pháp hiệu quả nhất để giảm thiểu thiệt hại do việc mất dữ liệu gây ra. Việc sao lưu nên áp dụng cho tất cả các thiết bị bất kể đó là điện thoại di động, máy tính bảng, máy tính xách tay hay máy tính để bàn.

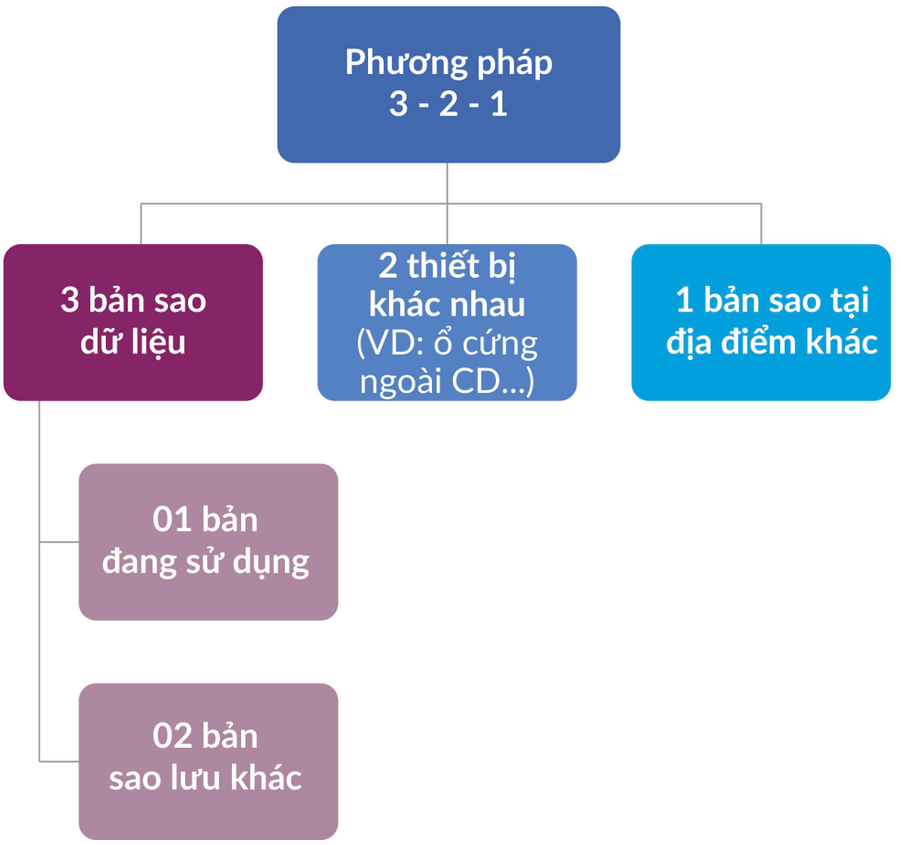
Phương pháp sao lưu 3-2-1 giúp bảo vệ dữ liệu hiệu quả trước các rủi ro mất mát. Nguyên tắc này đề xuất:

Lưu trữ ba **(03)** bản sao dữ liệu.

Trong đó, hai **(02)** bản sao được lưu trên hai loại phương tiện khác nhau để giảm nguy cơ mất dữ liệu nếu một phương tiện bị hỏng. Ví dụ, một bản có thể lưu trên ổ cứng ngoài, bản khác trên đĩa CD, hoặc một bản sao khác lưu trữ trên nền tảng đám mây (lưu trữ trực tuyến).

Một **(01)** bản sao nên được lưu ở địa điểm khác để bảo vệ dữ liệu khỏi các sự cố như trộm cắp, hỏa hoạn hoặc thiên tai.

Cách tiếp cận này giúp đảm bảo dữ liệu luôn an toàn, ngay cả khi xảy ra sự cố bất ngờ.



Ví dụ: Hãy tưởng tượng bạn có một bản báo cáo quan trọng. Để bảo vệ báo cáo này, bạn nên:

- Lưu 1 bản trên máy tính của bạn.
- Lưu 1 bản trên ổ cứng ngoài.
- Gửi 1 bản cho người thân ở xa và nhờ họ giữ hộ.

Như vậy, ngay cả khi máy tính của bạn bị hỏng hoặc nhà bạn gặp sự cố, bạn vẫn có thể lấy lại được báo cáo từ ổ cứng ngoài hoặc từ người thân.

Việc sao lưu dữ liệu không chỉ đơn thuần là lưu trữ, mà để thực sự hiệu quả, bạn cần cân nhắc một số lưu ý quan trọng sau:

- **Đối với bản sao lưu ngoại tuyến** (được lưu trên các thiết bị không kết nối Internet), bạn cần:
  - Lưu trữ dữ liệu cục bộ trên các thiết bị bên ngoài: Sử dụng ổ cứng, USB và thẻ nhớ hoặc thiết bị khác để lưu trữ các bản sao lưu của bạn.
  - Ngắt kết nối với Internet và lưu trữ thiết bị một cách an toàn.
  - Bảo quản các thiết bị này ở vị trí an toàn và bảo mật: Xem xét các yếu tố môi trường, ví dụ, cất giữ ở các tầng

cao hơn ở những khu vực dễ bị lũ lụt.

- **Đối với bản sao lưu trực tuyến hoặc trên đám mây** (được lưu trên các nền tảng điện toán đám mây như Google Drive, hoặc iCloud), bạn cần:
  - Lưu trữ đám mây cho phép sao lưu tự động, bảo mật có thể truy cập từ mọi nơi.
  - Sao lưu tự động định kỳ: Sao lưu đám mây nên được thiết lập tự động và chạy thường xuyên để giảm thiểu nguy cơ mất dữ liệu và giúp bạn dễ dàng khôi phục dữ liệu khi cần thiết.
  - Đảm bảo các biện pháp bảo mật chặt chẽ: lựa chọn nhà cung cấp đám mây có uy tín, đặt mật khẩu mạnh cho tài khoản, bật xác thực 2 lớp.
- **Kiểm tra các bản sao lưu:** cần kiểm tra các bản sao lưu để đảm bảo rằng chúng hoạt động và dữ liệu được sao lưu có thể truy cập được.

Nội dung chính cần ghi nhớ

1. Các **rủi ro thường gặp** đối với thiết bị (điện thoại và máy tính) và các thực hành bảo mật có thể thực hành để có thể giảm thiểu rủi ro bao gồm:

- **Rủi ro về bảo mật dữ liệu**
  - → Đặt mật khẩu cho thiết bị
  - → Chỉ cài đặt các ứng dụng uy tín, có nguồn gốc và chỉ cấp các quyền cần thiết cho các ứng dụng.
  - → Sử dụng các kết nối Internet an toàn. Khuyến khích sử dụng VPN khi kết nối các mạng wifi bên ngoài.
- **Rủi ro do lỗ hổng bảo mật, phần mềm độc hại**
  - → Chỉ dùng những phần mềm có bản quyền
  - → Cập nhật hệ điều hành và phần mềm thường xuyên sẽ giúp vá các lỗ hổng bảo mật, sửa lỗi và cải thiện hiệu suất.
  - → Cài đặt các phần mềm diệt vi-rút uy tín
- **Rủi ro do mất, hỏng hoặc cháy nổ**
  - → Sao lưu dữ liệu
  - → (Đối với điện thoại) Kích hoạt tính năng "Tìm thiết bị" (Find My iPhone - Find My Device)

2. Trong các phương thức phòng tránh rủi ro đối với thiết bị, việc sao lưu dữ liệu là phương pháp hiệu quả nhất để giảm thiểu thiệt hại do việc mất dữ liệu gây ra. **Phương pháp sao lưu 3-2-1** là phương pháp khuyến khích thực hiện và có thể thực hiện với nguyên tắc:
   - → Lưu trữ ba (03) bản sao dữ liệu.
   - → Trong đó, hai (02) bản sao được lưu trên hai loại phương tiện khác nhau.
   - → Một (01) bản sao nên được lưu ở địa điểm khác.