APAC Cybersecurity Fund
The Asia Foundation

VIETNET-ICT

CHỦ ĐỀ 3:
BẢO VỆ CÁC THIẾT BỊ SỐ

Bài 3: Phần mềm độc hại và cách phòng tránh, xử lý

với sự hỗ trợ từ Google.org

MỤC TIÊU:

- Hiểu khái niệm cơ bản về phần mềm độc hại
- Biết hậu quả nếu thiết bị nhiễm phần mềm độc hại
- Biết một số cách để phòng tránh và xử lý

Trong kỷ nguyên số hiện nay, máy tính và Internet đã trở thành những công cụ không thể thiếu trong cuộc sống hàng ngày của chúng ta. Tuy nhiên, bên cạnh những lợi ích to lớn mà chúng mang lại, chúng ta cũng phải đối mặt với không ít rủi ro, trong đó có phần mềm độc hại.

1. Phần mềm độc hại là gì ?

Hãy xem xét ví dụ sau: Chị Lan nhận được một email từ một người bạn cũ. Email có tiêu đề "Hình ảnh mới" và kèm theo một file đính kèm có tên "*hinh_moi.exe*". Chị Lan tò mò và mở file đính kèm. Ngay sau đó, máy tính của chị bắt đầu hoạt động chậm chạp, các chương trình không thể mở được, và màn hình xuất hiện những thông báo lạ. Chị Lan biết rằng máy tính của mình đã bị tấn công bởi phần mềm độc hại.

Phần mềm độc hại *là một loại chương trình máy tính được thiết kế để gây hại cho bạn hoặc thiết bị của bạn.* Nếu máy tính xách tay, máy tính để bàn hoặc thiết bị di động của bạn bị nhiễm phần mềm độc hại, nó có thể chậm lại hoặc ngừng hoạt động hoàn toàn. Phần mềm độc hại cũng có thể xóa hoặc đánh cắp dữ liệu, làm ảnh hưởng tới quyền riêng tư của bạn.

Theo báo cáo từ Viettel Cyber Security, chỉ trong nửa đầu năm 2024, lượng dữ liệu bị mã hóa trong các cuộc tấn công mạng đã lên tới 3 terabyte, gây thiệt hại ước tính hơn 10

triệu USD (gần 260 tỷ đồng) tại Việt Nam. Những sự cố nổi bật như tại VNDirect hay PVOIL cho thấy rằng ngay cả các tập đoàn lớn cũng không miễn nhiễm trước nguy cơ này. Ngoài ra, theo báo cáo của Kaspersky Security Network (KSN), từ tháng 1-5/2023, 1.120 nhân viên tại doanh nghiệp vừa và nhỏ (DNVVN) ở Việt Nam đã đối mặt với phần mềm độc hại hoặc phần mềm không mong muốn được ngụy trang dưới dạng ứng dụng doanh nghiệp. Số liệu thống kê cho thấy tổng số lần phát hiện các tệp độc hại trong quý I/2023 tại Việt Nam là 25.194. Con số này thể hiện sự tăng đột biến so với số lượng cùng kỳ năm ngoái (1.240) và cao hơn rất nhiều so với các quốc gia khác trong khu vực Đông Nam Á.

	Quý 1/2022	Quý 1/2023
Việt Nam	1.240	25.194
Malaysia	498	2.184
Phillippine	434	1.847
Singapore	112	453
Thái Lan	664	2.375
Indonesia	6.534	11.969

Hình: Số liệu về mối đe dọa phần mềm độc hại đối với DNVVN tại Việt Nam và 5 quốc gia Đông Nam Á khác. Nguồn: Kaspersky Security Network

Một số loại *phần mềm độc hại phổ biến* được biết đến như:

- **Vi-rút:** là loại phần mềm có thể lây lan nếu nó xâm nhập vào máy tính của bạn. Vi-rút đúng như tên gọi của nó sẽ làm "ốm" các dữ liệu, khiến cho các dữ liệu sẽ bị *xoá, hỏng, hoặc vô hiệu hoá*... và chúng ta không còn sử dụng được.

- **Phần mềm gián điệp (Spyware):** khi phần mềm này xâm nhập vào thiết bị, nó sẽ âm thầm hoạt động *theo dõi các hành vi và dữ liệu trên thiết bị* của bạn, nhưng nguy hiểm là nó sẽ không để cho bạn biết tới sự tồn tại của nó, trong khi bạn sẽ bị lộ lọt thông tin và theo dõi mọi hoạt động trên thiết bị.

- **Phần mềm quảng cáo (Adware):** là phần mềm *hiển thị quảng cáo* trên màn hình máy tính hoặc thiết bị di động, chuyển hướng kết quả tìm kiếm đến các trang web quảng cáo và thu thập dữ liệu người dùng.

- **Phần mềm tống tiền (Ransomware):** là một loại phần mềm độc hại *mã hóa dữ liệu* của người dùng và *yêu cầu họ trả tiền chuộc* để lấy lại quyền truy cập vào dữ liệu. Đây là một trong những loại phần mềm độc hại nguy hiểm nhất hiện nay, thường nhắm tới các ngành có giá trị cao như y tế, cơ sở hạ tầng quan trọng và dịch vụ tài chính.

2. Phần mềm độc hại xâm nhập bằng cách nào?

Phần mềm độc hại có thể xâm nhập vào thiết bị của bạn qua nhiều cách khác nhau, thường lợi dụng *sự bất cẩn của người dùng* hoặc *khai thác lỗ hổng bảo mật* trong hệ thống. Một số phương thức phổ biến bao gồm:

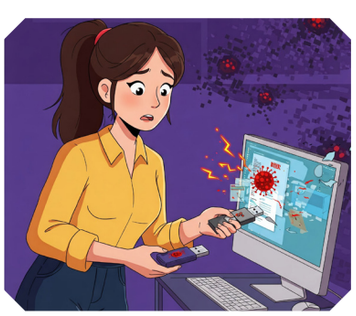
- **Ứng dụng giả mạo và phần mềm không rõ nguồn gốc:** Một số phần mềm miễn phí và không rõ nguồn gốc có thể chứa phần mềm độc hại. Người dùng tải và cài đặt những ứng dụng này mà không kiểm tra nguồn gốc, vô tình cho phép mã độc xâm nhập vào hệ thống.

Ví dụ: Anh Khoa thấy một bài viết quảng cáo về một phần mềm chỉnh sửa ảnh miễn phí trên một trang web lạ. Anh Khoa đã nhấn tải về máy. Sau khi cài đặt, máy tính bắt đầu chạy chậm, xuất hiện quảng cáo liên tục và dữ liệu cá nhân bị đánh cắp.

- **Email lừa đảo:** Nhiều phần mềm độc hại được phát tán qua các email giả mạo. Khi bạn nhấp vào liên kết hoặc tải xuống tệp đính kèm từ email không rõ nguồn gốc, bạn có thể vô tình cài đặt phần mềm độc hại vào thiết bị của mình.

Ví dụ: Chị Hoa nhận được một email trông giống như từ ngân hàng, yêu cầu tải xuống một tệp PDF chứa "sao kê tháng". Khi mở tệp, phần mềm gián điệp được cài đặt, đánh cắp thông tin đăng nhập ngân hàng của bạn.

- **Thiết bị ngoại vi (USB, ổ cứng ngoài, thẻ nhớ...):** Nếu kết nối USB hoặc ổ cứng bị nhiễm phần mềm độc hại vào máy tính, phần mềm độc hại có thể tự động lây lan mà không cần người dùng thực hiện thao tác nào. Một số loại vi-rút, như Autorun, có thể tự động chạy ngay khi thiết bị được cắm vào.



Ví dụ: Chị Hoa mang USB từ máy tính công ty về nhà để làm việc. Khi cắm vào máy tính cá nhân, vi-rút trong USB lây lan, khiến hệ thống bị lỗi và mất dữ liệu quan trọng.

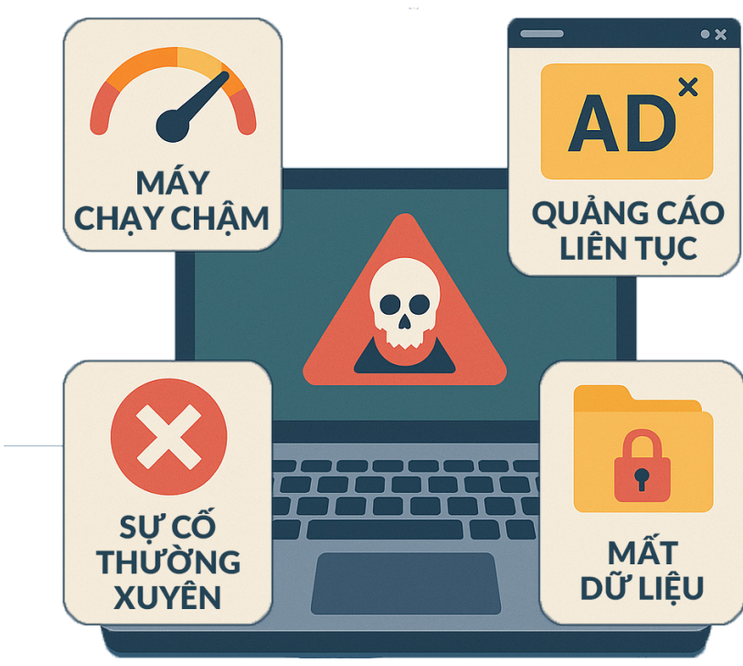
- **Trang web độc hại:** Truy cập vào các trang web không tin cậy hoặc bị tấn công có thể khiến phần mềm độc hại được tải xuống và triển khai mà không biết.

Ví dụ: Anh Khoa vào một trang web cung cấp phim miễn phí. Anh Khoa nhấp vào một liên kết tải phim nhưng thực chất lại tải về một phần mềm độc hại, làm máy bị nhiễm mã độc tống tiền (ransomware), khóa toàn bộ dữ liệu và yêu cầu trả tiền để mở khóa.

3. Một số dấu hiệu nhận biết thiết bị nhiễm phần mềm độc hại

Việc phát hiện máy tính bị nhiễm phần mềm độc hại đôi khi không hề dễ dàng, bởi không phải lúc nào cũng có những dấu hiệu rõ ràng. Tuy nhiên, bạn có thể dựa vào một số triệu chứng nhất định để nhận biết. Bạn cần lưu ý là không phải bất kỳ triệu chứng riêng lẻ nào cũng đồng nghĩa với việc máy tính bị nhiễm phần mềm độc hại. Có nhiều nguyên nhân khác có thể khiến thiết bị của bạn hoạt động bất thường.

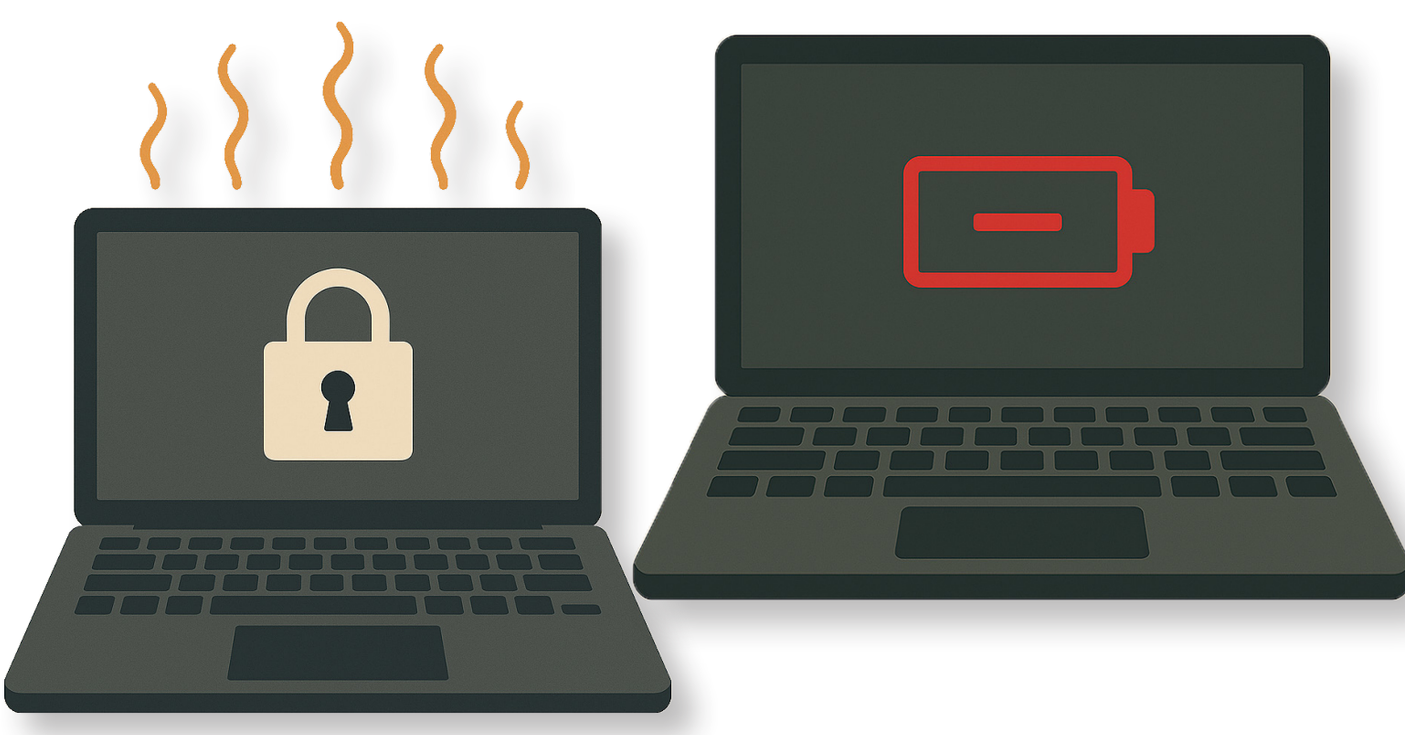
Mặc dù vậy, nếu thiết bị của bạn đột nhiên xuất hiện những **dấu hiệu đáng ngờ** hoặc gặp phải **các sự cố** *ngay sau khi bạn nhấp vào một liên kết trong email hoặc tin nhắn, tải xuống và chạy một phần mềm nào đó, hoặc mở một tệp đính kèm đáng ngờ*, thì rất có thể máy tính của bạn đã bị nhiễm phần mềm độc hại. Trong trường hợp này, bạn cần ngay lập tức thực hiện các biện pháp khắc phục để bảo vệ dữ liệu và hệ thống.



Một số dấu hiệu nhận biết có thể bao gồm:

- Thiết bị có vẻ chạy chậm hơn so với trước, trục trặc hoặc đóng băng
- Thiết bị quá nóng
- Pin của thiết bị dường như cạn kiệt nhanh hơn trước
- Ứng dụng được mở hoặc đóng tự động
- Cửa sổ bật lên và quảng cáo không mong muốn, xuất hiện nhiều quá mức
- Email hoặc tin nhắn trò chuyện trái phép được gửi dưới tên của bạn
- Webcam tự bật
- Đã cài đặt phần mềm diệt vi-rút trước đó, nhưng bây giờ không cài đặt nữa
- Các chương trình hoặc ứng dụng mới đột nhiên xuất hiện trên thiết bị của bạn và bạn không cài đặt nó

Không thể liệt kê tất cả các dấu hiệu do phần mềm độc hại 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 có cách ứng phó đúng cách với hành vi vi phạm nếu chúng xảy ra.



4. Một số cách phòng tránh và xử lý phần mềm độc hại

Để **phòng tránh** các phần mềm độc hại này, bạn có thể áp dụng một số biện pháp sau:

Một trong những biện pháp hiệu quả để bảo vệ thiết bị của bạn khỏi phần mềm độc hại là **sử dụng phần mềm diệt vi-rút.** Cài đặt phần mềm diệt vi-rút giúp bảo vệ thiết bị của bạn khỏi phần mềm độc hại bằng cách phát hiện và loại bỏ các mối đe dọa. Nó bảo vệ thiết bị của bạn liên tục và cập nhật thường xuyên để chống lại các mối đe dọa mới. Ngoài ra, phần mềm diệt vi-rút còn bảo vệ dữ liệu cá nhân và ngăn chặn truy cập vào các trang web không an toàn.

Suy nghĩ kỹ trước khi nhấp vào bất kỳ các liên kết, tải phần mềm hay thận trọng khi mở email có chứa các tệp tin hoặc hình ảnh đính kèm. Các liên kết hoặc tệp đính kèm có thể chứa mã độc, vi-rút hoặc phần mềm gián điệp, có thể đánh cắp dữ liệu cá nhân, tài khoản hoặc làm hỏng hệ thống của bạn. Hacker thường sử dụng kỹ thuật lừa đảo (phishing) để dụ người dùng tải xuống phần mềm độc hại hoặc cung cấp thông tin nhạy cảm. Ngoài ra, các phần mềm không rõ nguồn gốc có thể chứa mã độc chạy ngầm, làm chậm máy tính hoặc chiếm quyền điều khiển thiết bị.

Chỉ tải xuống hoặc cài đặt phần mềm từ các nguồn đáng tin cậy và hết sức cẩn trọng khi tải xuống các file thực thi/ file cài đặt (là những file có đuôi .exe, .pkg, .sh, .dll hoặc .dmg). File thực thi là các tệp tin đặc biệt chứa mã lệnh mà máy tính có thể thực hiện. Đôi khi, các file này có thể thực hiện các hành động không hợp lệ. Ví dụ: một người có thể viết một file thực thi để xóa ổ cứng của ai đó hoặc cài đặt một trình duyệt giả mạo.

Luôn **cập nhật các phiên bản mới** nhất của phần mềm và hệ điều hành của máy tính: Các bản cập nhật thường vá lỗi, cải thiện hiệu suất, giúp hệ thống hoạt động ổn định và mượt mà hơn. Ngoài ra, chúng còn bổ sung các tính năng mới, nâng cao trải nghiệm người dùng và đảm bảo phần mềm tương thích với công nghệ hiện đại. Nếu không cập nhật, máy tính có thể trở nên dễ bị tấn công, gặp lỗi hoặc hoạt động kém hiệu quả.

Sao lưu dữ liệu cũng có ý nghĩa rất quan trọng trong việc đối phó với phần mềm độc hại. Khi máy tính bị nhiễm phần mềm độc hại, dữ liệu có thể bị xóa, mã hóa hoặc hỏng hóc, gây ra mất mát thông tin quan trọng. Việc sao lưu dữ liệu thường xuyên giúp bạn có một bản sao an toàn để khôi phục lại khi cần thiết, giảm thiểu thiệt hại và thời gian gián đoạn *(Tham khảo thêm phần hướng dẫn sao lưu ở Bài 1 - Chủ đề 3).*

Khi thiết bị nhiễm phần mềm độc hại, bạn có thể tham khảo một số cách xử lý sau:

- **Ngắt kết nối Internet:** Tắt Wi-Fi hoặc rút cáp mạng để ngăn chặn phần mềm độc hại lây lan hoặc đánh cắp dữ liệu, đồng thời điều đó cũng sẽ giúp ngăn kẻ xấu điều khiển máy tính của bạn từ xa.

- **Chạy phần mềm diệt vi-rút:** Sử dụng phần mềm bảo mật uy tín để quét và loại bỏ phần mềm độc hại.

- **Gỡ bỏ các chương trình đáng ngờ:** Kiểm tra danh sách ứng dụng đã cài đặt và xóa các phần mềm lạ hoặc không rõ nguồn gốc.

- **Đổi mật khẩu quan trọng:** Nếu có dấu hiệu bị xâm nhập tài khoản, hãy đổi mật khẩu ngay để bảo vệ dữ liệu cá nhân.

- **Khôi phục hệ thống (nếu cần):** Nếu thiết bị vẫn bị ảnh hưởng, hãy sử dụng chế độ khôi phục về trạng thái trước đó hoặc cài đặt lại hệ điều hành.

Nội dung chính cần ghi nhớ

1. **Phần mềm độc hại là một loại chương trình máy tính được thiết kế để gây hại cho bạn hoặc thiết bị của bạn.** Nếu máy tính xách tay, máy tính để bàn hoặc thiết bị di động của bạn bị nhiễm phần mềm độc hại, nó có thể chậm lại hoặc ngừng hoạt động hoàn toàn. Phần mềm độc hại cũng có thể xóa hoặc đánh cắp dữ liệu, gây nguy hiểm cho quyền riêng tư của bạn.
2. Phần mềm độc hại **có thể xâm nhập vào máy tính của bạn qua nhiều cách khác nhau** thường lợi dụng sự bất cẩn của người dùng hoặc khai thác lỗ hổng bảo mật trong hệ thống. Một số phương thức phổ biến bao gồm:

- Ứng dụng giả mạo và phần mềm không rõ nguồn gốc
- Email lừa đảo
- Thiết bị ngoại vi (USB, ổ cứng ngoài, thẻ nhớ...)
- Trang web độc hại

3. Việc phát hiện máy tính bị nhiễm phần mềm độc hại đôi khi không hề dễ dàng nhưng bạn có thể dựa vào **một số dấu hiệu** nhất định để nhận biết như thiết bị chạy chậm, trục trặc hoặc quá nóng, ứng dụng tự đóng hoặc mở, email hoặc tin nhắn trò chuyện trái phép... Tuy nhiên, không thể liệt kê tất cả các dấu hiệu do phần mềm độc hại 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.

4. Để phòng tránh các phần mềm độc hại này, bạn có thể áp dụng một số **biện pháp** sau:
   - Chỉ tải xuống hoặc cài đặt phần mềm từ các nguồn đáng tin cậy và hết sức cẩn trọng khi tải xuống các file thực thi (là những file có đuôi .exe, .pkg, .sh, .dll hoặc .dmg).
   - Sử dụng phần mềm diệt vi-rút
   - Suy nghĩ kỹ trước khi nhấp vào bất kỳ các liên kết, tải phần mềm hay thận trọng khi mở email có chứa các tệp tin hoặc hình ảnh đính kèm
   - Luôn cập nhật các phiên bản mới nhất của phần mềm và hệ điều hành của máy tính để vá các lỗ hổng bảo mật
   - Sao lưu dữ liệu
5. Để xử lý khi thiết bị nhiễm phần mềm độc hại, bạn có thể tham khảo một số thực hành sau:
   - Ngắt kết nối Internet
   - Chạy phần mềm diệt vi-rút
   - Gỡ bỏ các chương trình đáng ngờ
   - Đổi mật khẩu quan trọng
   - Khôi phục hệ thống (nếu cần)