SỞ THÔNG TIN VÀ TRUYỀN THÔNG

TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TỰ BẢO VỆ MÌNH TRÊN KHÔNG GIAN MẠNG

Nội dung trình bày:

1. Tầm quan trọng an toàn trên không gian mạng
2. Các hình thức tấn công mạng phổ biến
3. Các kỹ năng cơ bản để phòng tránh

Á

Ő, Ï ÄÁÕÄÁÎ ÄÓÑ, Î ÉÆÄÁÎ Ä ÓĹÄÁÎ ÄÓÑÇÎ ÄĢĘJÎ ÉÄ ÉÕÄÁÎ Ä ´ Î É

Trong thời đại công nghệ số ngày nay, an toàn trên không gian mạng đóng vai trò vô cùng quan trọng đối với mỗi cá nhân và tổ chức.

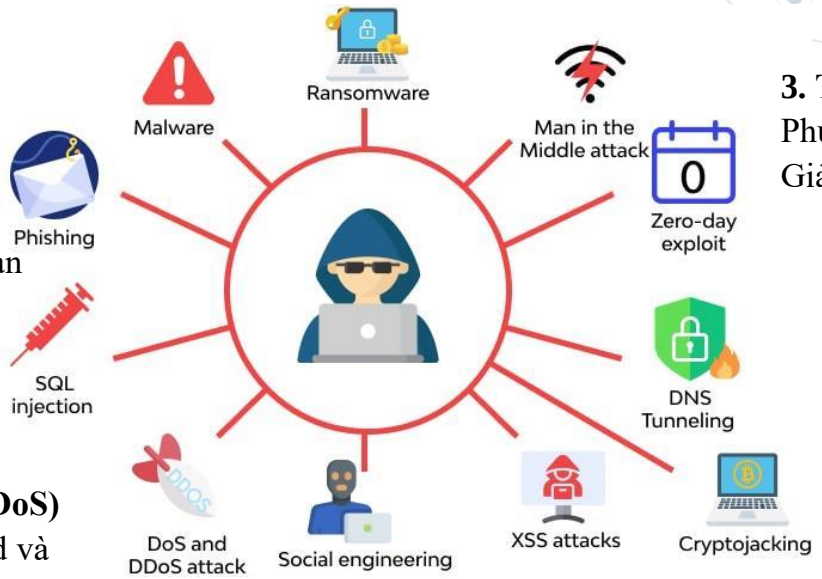
Báo cáo thường niên WeAreSocial Digital 2024 vừa được phát hành cho thấy:

- Thời gian trung bình mà người dùng dành để sử dụng Internet là 6 giờ 18 phút, xem TV là 2 giờ 21 phút và truy cập mạng xã hội là 2 giờ 25 phút.
- Hơn một nửa người dùng internet tại Việt Nam sử dụng trên thiết bị di động với tỷ lệ 55,7% so với 44,3% dùng trên máy tính.
- 73,3% dân số Việt Nam đang dùng mạng xã hội. Mức dân số Việt Nam theo ghi nhận hiện là hơn 99 triệu dân. Trong đó, thời gian trung bình người dùng tại Việt Nam lướt mạng xã hội mỗi ngày là 2 giờ 25 phút, thuộc Top 20 trên thế giới.

Á

1. Tấn công bằng phần mềm độc hại (Malware)

- Spyware (phần mềm gián điệp).
- Ransomware (mã độc tống tiền).
- Virus; Worm (phần mềm độc hại lây lan với tốc độ nhanh).



3. Tấn công giả mạo (Phishing)

Phương thức: Giả mạo Email.

Giả mạo Website. Deep voice, Deepfake

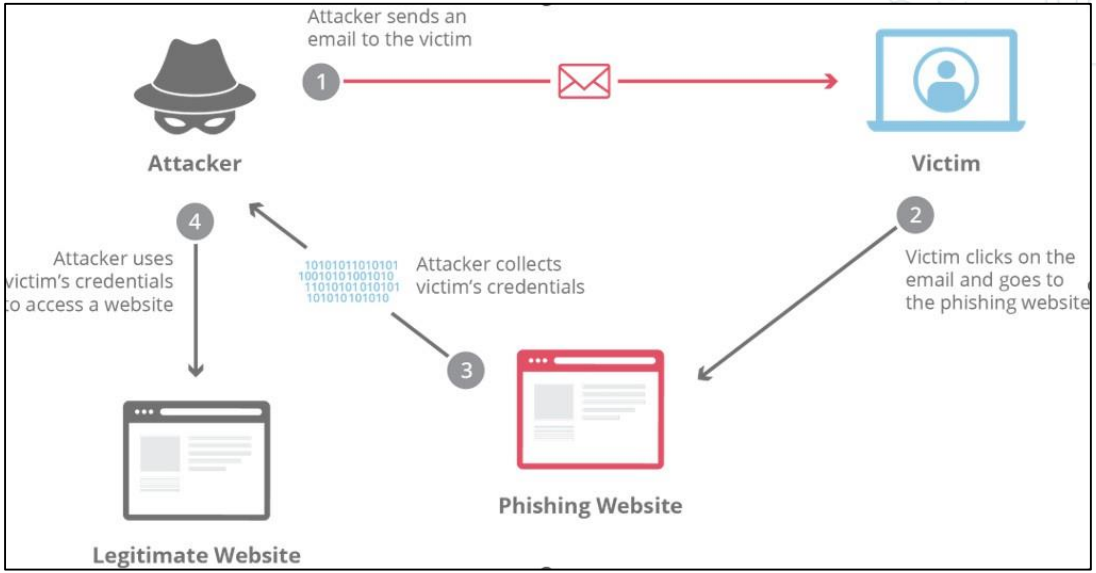
2. Tấn công từ chối dịch vụ (Dos và DDoS)

- Tấn công gây nghẽn mạng (UDP Flood và Ping Flood).
- Tấn công SYN flood (TCP).
- Tấn công khuếch đại DNS.

4. Khai thác lỗ hổng bảo mật

Thông thường các hacker sẽ ưa thích khai thác các lỗ hổng zero-day (0-day Vulnerability)

- Chặn các truy cập vào hệ thống mạng và dữ liệu quan trọng (Ransomware).
- Cài đặt thêm phần mềm độc hại khác vào máy tính người dung.
- Đánh cắp dữ liệu (Spyware).
- Phá hoại phần cứng, phần mềm, làm hệ thống tê liệt, không thể hoạt động.
- Gây quá tải hệ thống mạng bằng lượng truy cập lớn đến từ nhiều nguồn để chặn các truy cập thực của người dùng.
- Gây cạn tài nguyên máy chủ, ngăn chặn việc nhận các yêu cầu kết nối mới.
- Chiếm đoạt tài sản, tống tiền, gây thiệt hại về tài chính, hoạt động.



5. Tấn công trung gian (Man-in-the-middle attack)

- Sniffing.
- Packet Injection.
- Loại bỏ SSL.

6. Tấn công cơ sở dữ liệu

- Đánh cắp những tài liệu quan trọng, hacker sẽ chèn một đoạn mã độc hại vào server sử dụng ngôn ngữ SQL

7. Tấn công chuỗi cung ứng

Tấn công mạng nhắm vào một doanh nghiệp thông qua các nhà cung cấp (provider/vendor) của doanh nghiệp đó hoặc phần mềm quan trọng trong chuỗi cung ứng

8. Một số hình thức tấn công khác

- Tấn công nội bộ tổ chức.
- Tấn công dựa trên IoT

3.

CÁC KỸ NĂNG CƠ BẢN ĐỂ PHÒNG TRÁNH:

1. Thiết lập mật khẩu mạnh, an toàn:

Mật khẩu chính là hàng phòng thủ đầu tiên và quan trọng để chống lại tấn công mạng

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	123456	< 1 Second	3,469,508
2	123456789	< 1 Second	993,222
8	1234567	< 1 Second	27,162
9	khongbiet	1 Day	24,013
10	123123	< 1 Second	22,037

- Sử dụng mật khẩu mạnh
- Sử dụng một mật khẩu duy nhất cho từng tài khoản quan trọng như email, tài khoản ngân hàng,…
- Giữ bí mật mật khẩu bằng cách nhớ hoặc để ở nơi chỉ mình bạn có thể biết và đọc nó
- Thiết lập các tùy chọn khôi phục mật khẩu và hãy cập nhật chúng một cách thường xuyên: 3 tháng, 6 tháng,..

GỢI Ý CÁCH ĐẶT MẬT KHẨU MẠNH

- Mật khẩu ít nhất phải có 8 ký tự
- Sử dụng 4 loại ký tự bao gồm: chữ hoa, chữ thường, số và ký tự đặc biệt (@ $ # %...)
- Không dùng các mật khẩu dễ đoán, biết như: họ tên, ngày sinh, số điện thoại, tên người thân,…)

2. Kích hoạt chức năng tường lửa (Firewall)

Hướng dẫn:

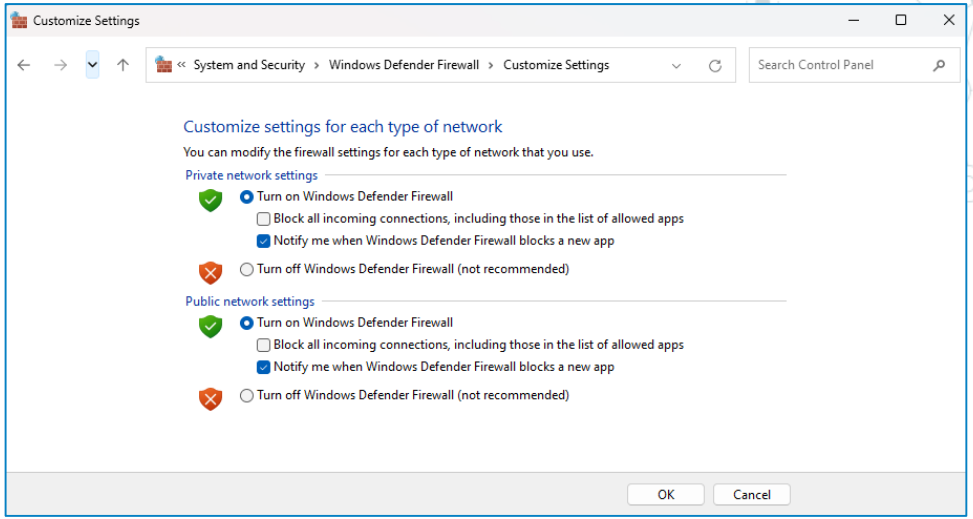
Bước 1: Tại thanh Tìm kiếm, bạn nhập vào **Control Panel**.

Bước 2: Chọn tiếp vào **Windown Defender Firewall**.

Bước 3: Nhấn chọn **Turn Windows Defender Firewall on or off**.

Bước 4: Lựa chọn **Turn on Windows Defender Firewall** (ở cả mục Private network settings và Public network settings).

Bước 5: Nhấn **OK** để lưu lại thay đổi.



Lợi ích:

- Kiểm tra và sửa lỗi mạng WiFi, Internet.
- Báo cáo virus hoặc diệt virus cho máy tính của bạn.
- Giám sát các hoạt động gây bất lợi cho máy tính của bạn.
- Ngăn chặn những vấn đề gây nguy hại cho máy tính.
- Bảo vệ máy tính của bạn khỏi những tác hại khác.

3. Kích hoạt chương trình diệt virus (Windows Security)

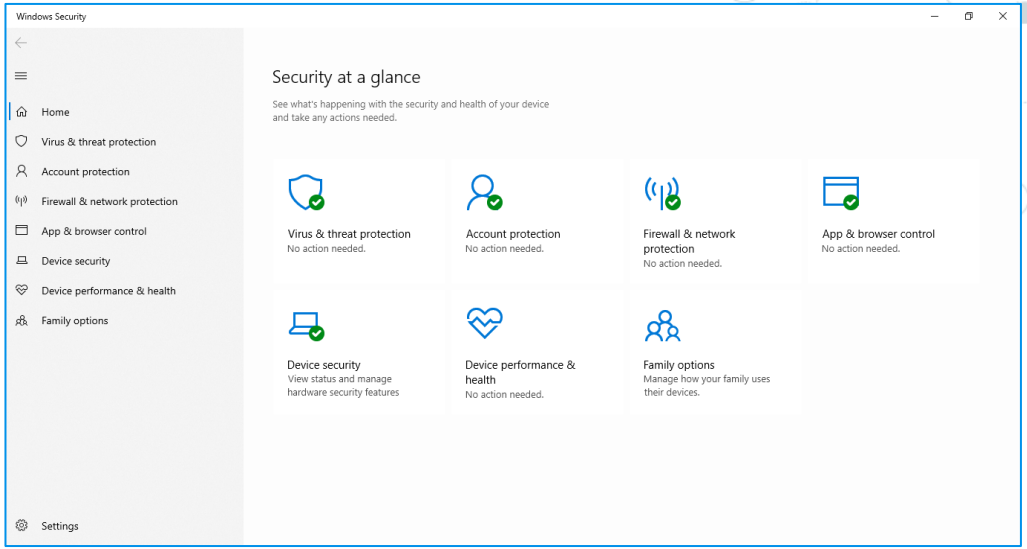
Hướng dẫn:

Bước 1: Tại thanh Tìm kiếm, bạn nhập vào **Windows Security**.

Bước 2: Nhấn vào **Virus & threat protection** ở phía bên trái.

Bước 3: Nhấn vào **Manage settings** (ở mục Virus & threat protection settings).

Bước 4: Chọn **On** (ở các mục Real-time protection, Cloud-delivered protection, Automatic sample submission, Tamper Protection).



- Lợi ích:
  - Ngăn chặn các mối đe dọa và virus
  - Bảo vệ tài khoản
  - Bảo vệ mạng
  - Kiểm soát ứng dụng
  - Bảo vệ thiết bị
  - Theo dõi tình trạng hoạt động của máy tính

4. Cập nhật phần mềm và hệ điều hành:

Việc quan trọng để đảm bảo rằng hệ thống máy tính luôn được bảo vệ và hoạt động tối ưu

Hướng dẫn:

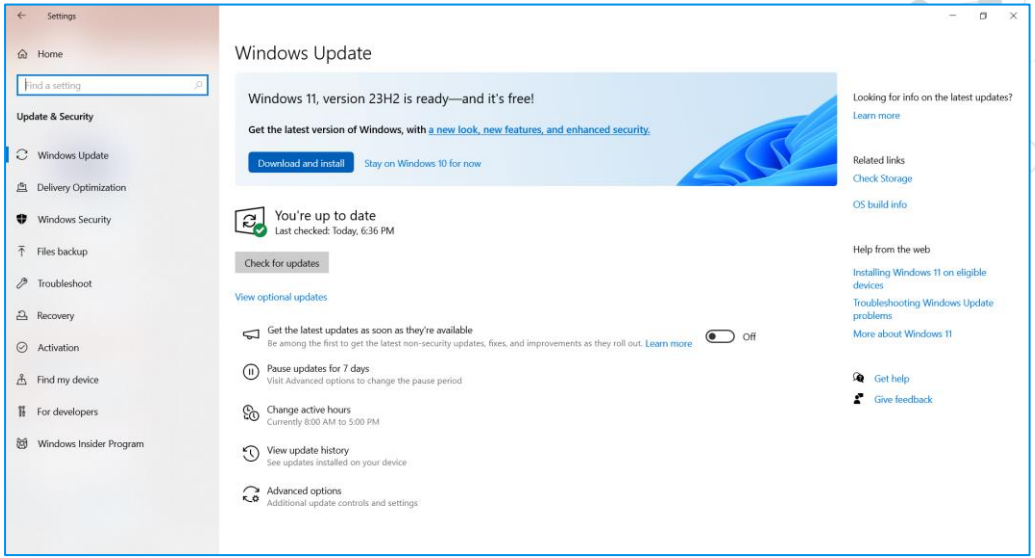
Bước 1: Mở cửa sổ **Start** và nhấp vào biểu tượng "răng cưa“ Settings (Cài đặt) ở góc dưới bên trái màn hình.

Bước 2: Trong cửa sổ Settings, chọn **Update & Security** (Cập nhật & Bảo mật).

Bước 3: Cửa sổ **Windows Update** được mở ra. Nhấn vào nút **Check for Updates** (Kiểm tra bản cập nhật).

Khi đó, hệ thống sẽ kiểm tra phiên bản hiện tại mà Microsoft đưa ra với phiên bản hiện tại trên máy tính của bạn, đồng thời tự động tải về bản cập nhật cần thiết.

Bước 4: Sau khi cập nhật xong, bấm **Restart** để khởi động lại máy tính.



5. Cài đặt phần mềm phòng chống mã độc:

Lớp lá chắn quan trọng bảo vệ người sử dụng khỏi các mã độc và virus.

Sử dụng phần mềm diệt virus có bản quyền:

Hiện nay trên thị trường có nhiều loại phần mềm diệt virus khác nhau, người sử dụng có thể mua và cài đặt để bảo vệ máy tính. Luôn dùng giải pháp phòng chống phần mềm độc hại như Anti-Virus, Endpoint Security để rà quét, tìm và loại bỏ các mã độc trên máy tính hoặc trên các thiết bị lưu trữ di động trước khi sử dụng.

6. Sao lưu dữ liệu quan trọng định kỳ, thường xuyên:

Bảo vệ dữ liệu quan trọng bằng cách **sao lưu chúng vào ổ cứng ngoài** hoặc **hệ thống lưu trữ trên hạ tầng đám mây**. Trường hợp thiết bị của bạn bị nhiễm phần mềm độc hại hoặc bị truy cập bởi hacker, dữ liệu của bạn có thể bị hỏng, bị xóa hoặc mã hóa đòi tiền chuộc ransomware.

Một số lưu ý:

- Đảm bảo thiết bị di động, ổ cứng ngoài sử dụng để sao lưu dữ liệu **tách biệt với thiết bị đang sử dụng** (Không kết nối liên tục qua dây cable vật lý hoặc mạng cục bộ).

- **Dịch vụ lưu trữ đám mây** rất hữu ích để lưu trữ một bản sao dữ liệu của mình ở nơi khác qua internet.

7. Cẩn thận khi mở link lạ, email và tin nhắn:

❋ Cần kiểm tra thật kỹ số điện thoại/địa chỉ email gửi đến, tránh trường hợp bị lừa bởi một số điện thoại/địa chỉ giả có cấu trúc gần giống địa chỉ thật.

❋ Đồng thời đề cao cảnh giác nếu nội dung tin nhắn gửi đến có liên quan đến việc xác minh, yêu cầu cung cấp thông tin cá nhân, thông báo về việc trúng thưởng hoặc về việc giao nhận một bưu gửi hay món tiền.

❋ Ngoài ra, người dùng cũng cần cảnh giác với các tập tin được đính kèm trong tin nhắn/email. Điều này là cần thiết ngay cả khi những tệp đính kèm này có đuôi file dưới dạng những tập tin phổ biến như .pdf, .doc hay .xls. Rất có thể, ẩn chứa trong những file đính kèm kia là những chương trình được cài cắm nhằm tự động tải mã độc về máy của người sử dụng hoặc dẫn đến một đường link độc.

8. Không cài đặt phần mềm không rõ nguồn gốc:

❋ Tương tự như việc không truy cập vào các đường link lạ, bạn cũng không nên cài đặt các phần mềm hay ứng dụng không rõ nguồn gốc, bẻ khóa để bảo mật thông tin cá nhân. Các phần mềm này thường có nguy cơ cao bị nhiễm virus, malware, hoặc phần mềm độc hại khác. Điều này có thể dẫn đến mất thông tin cá nhân, hư hỏng hệ thống, hoặc lây lan sang các thiết bị khác trong mạng. Các cracker có thể lợi dụng người dùng để đánh cắp các thông tin cá nhân và tài khoản ngân hàng để sử dụng vào những mục đích xấu. Ngoài ra, ứng dụng bẻ khóa còn có thể có nhiều lỗi vặt, gây ảnh hưởng đến trải nghiệm sử dụng và sai lệch kết quả đầu ra.

Vì vậy, nếu muốn cài đặt một phần mềm hay ứng dụng nào đó tốt nhất bạn nên truy cập và tải chúng trên các website chính thức đăng tải ứng dụng.

❋ Đồng thời trên các thiết bị điện thoại, bạn có thể hạn chế quyền truy cập dữ liệu, tắt cho phép ứng dụng theo dõi khi cài đặt, sử dụng các ứng dụng.

9. Không chia sẻ thông tin cá nhân bừa bãi:

❋ Hạn chế chia sẻ các thông tin liên quan tới tài khoản ngân hàng, thông tin về căn cước, số điện thoại, địa chỉ cư trú...trên mạng. Bảo đảm chỉ cung cấp thông tin cá nhân của mình cho cá nhân và tổ chức uy tín.

10. Phòng, chống tấn công phi kỹ thuật và lừa đảo trực tuyến:

KHÔNG cung cấp bất kỳ nội dung gì liên quan đến thông tin cá nhân hoặc thông tin tài khoản ngân hàng.

KHÔNG chuyển bất cứ khoản tiền nào để làm thủ tục vay tiền hoặc chứng minh tài chính.

KHÔNG đăng nhập vào đường link lạ, cài đặt ứng dụng nghi ngờ.

KHÔNG cung cấp mã OTP cho người khác biết

KHÔNG chuyển bất cứ khoản tiền nào để mua đơn hàng theo yêu cầu của đối tượng

HÀNH ĐỘNG NHANH NẾU ĐÃ BỊ LỪA ĐẢO:

- Không tiếp tục gửi tiền và chặn tất cả các liên lạc từ kẻ lừa đảo.
- Liên hệ ngay lập tức với ngân hàng và tổ chức tài chính của bạn để báo cáo lừa đảo và yêu cầu họ dừng mọi giao dịch.
- Thu thập và lưu lại bằng chứng, làm đơn tố giác gửi tới cơ quan công an nơi lưu trú.
- Cảnh báo cho gia đình và bạn bè của bạn về trò lừa đảo này để họ có thể đề phòng những trò lừa đảo tiếp theo có thể xảy ra.
- Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo tại Cổng không gian mạng quốc gia (khonggianmang.vn).

11. Sử dụng các công cụ an toàn thông tin:

❋ Sử dụng công cụ VirusTotal:

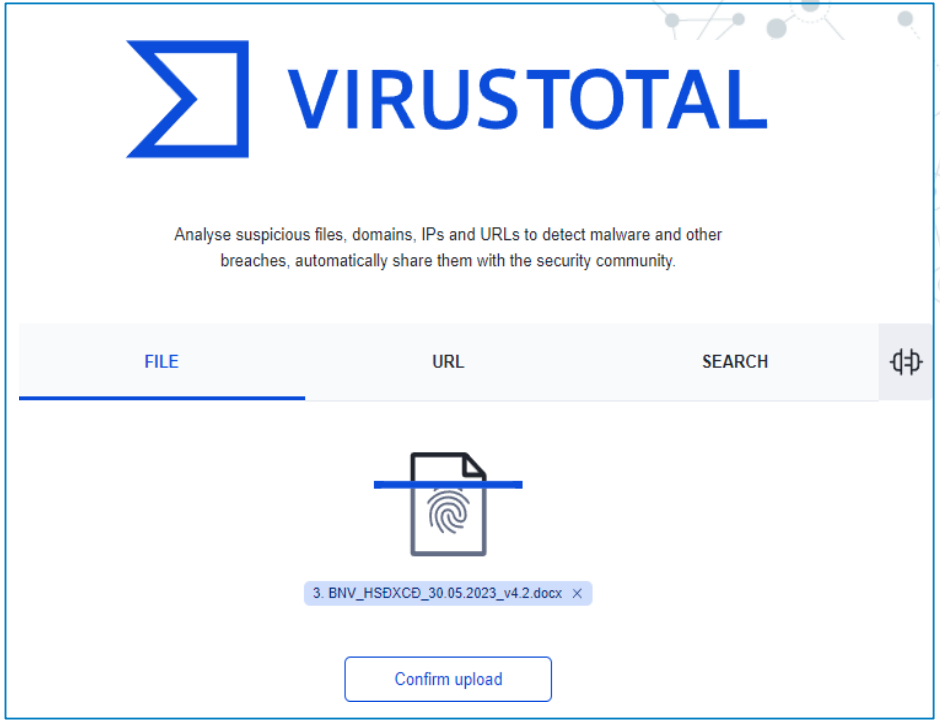
VirusTotal là công cụ quét virus trực tuyến miễn phí, giúp người dùng quét và phân tích các tập tin, địa chỉ URL để nhanh chóng phát hiện virus, worm, trojan và các loại phần mềm độc hại khác.

Tính năng:

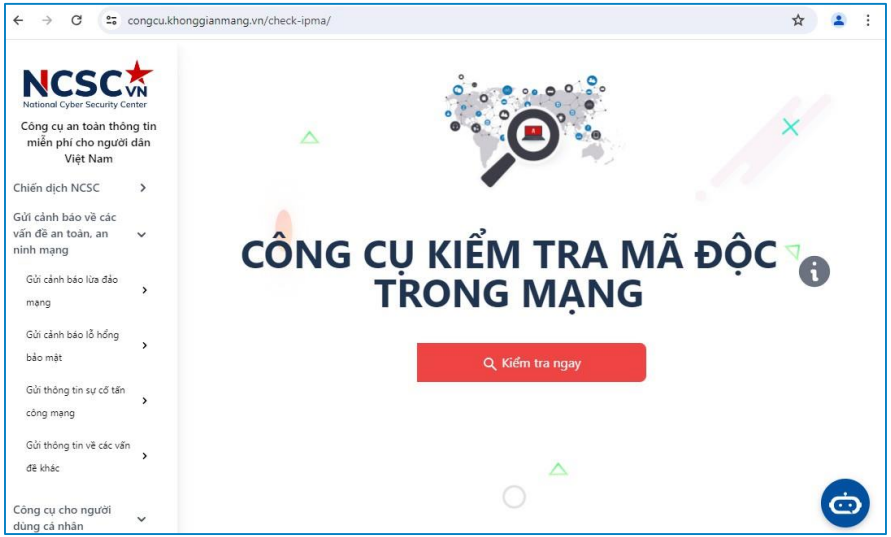
Kiểm tra 1 tệp/file trong máy tính;

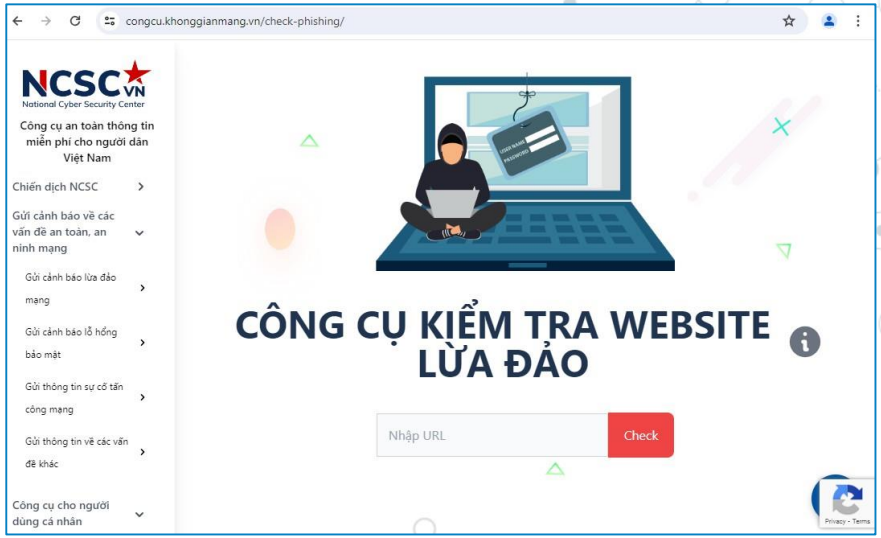
Kiểm tra 1 đường dẫn URL.

> Truy cập:
https://www.virustotal.com/gui/home/upload



11. Sử dụng các công cụ an toàn thông tin:





✵ Sử dụng công cụ Kiểm tra mã độc mạng

> Truy cập:
https://congcu.khonggianmang.vn/check-ipma/

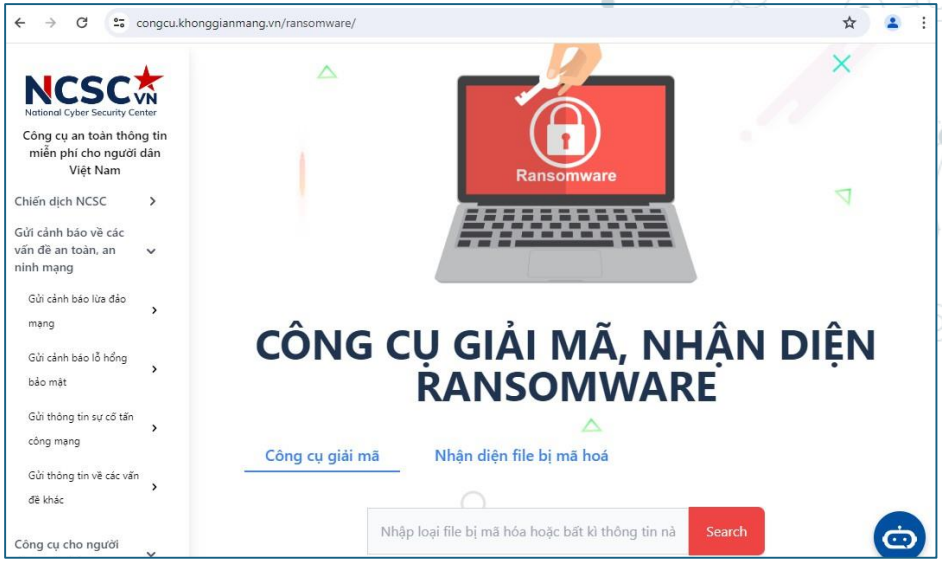
✵ Sử dụng công cụ Kiểm tra website lừa đảo

> Truy cập:
https://congcu.khonggianmang.vn/check-phishing/

11. Sử dụng các công cụ an toàn thông tin:

❋ **Sử dụng công cụ Kiểm tra lộ lọt thông tin tài khoản cá nhân**

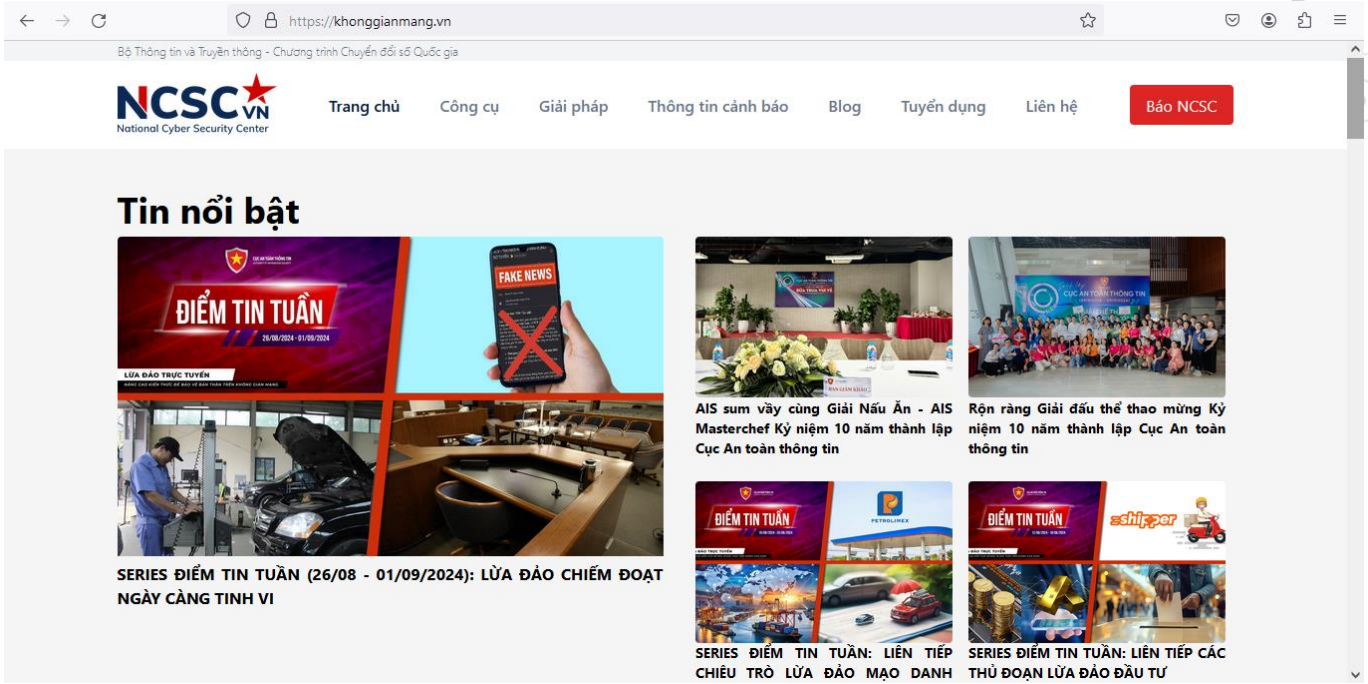
> Truy cập:
https://congcu.khonggianmang.vn/check-data-leak/



❋ **Sử dụng công cụ Giải mã, nhận diện Ransomeware**

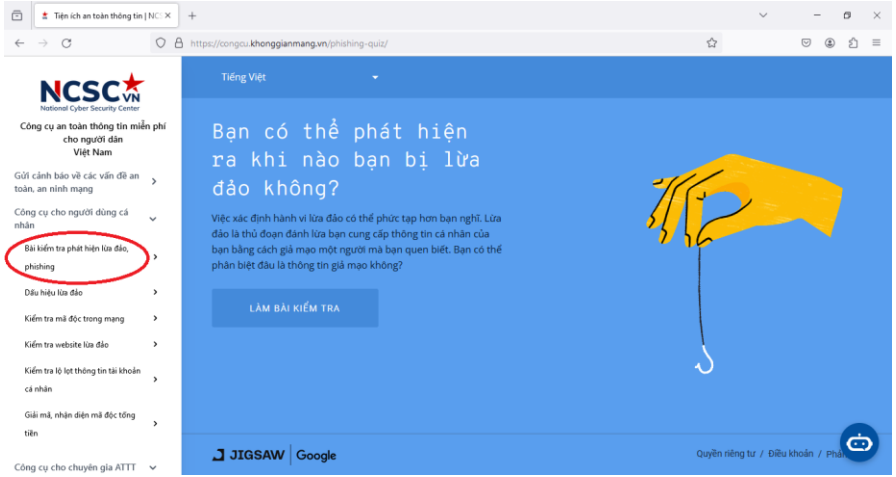
> Truy cập:
https://congcu.khonggianmang.vn/ransomware/

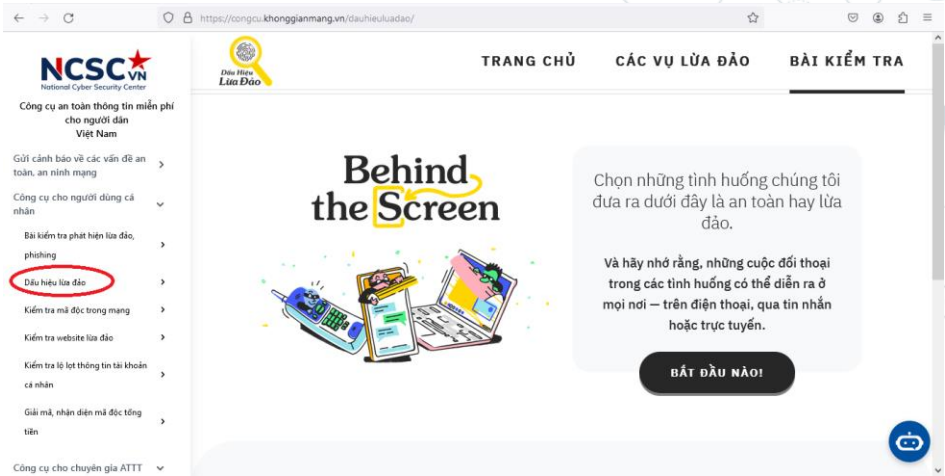
12. Nâng cao nhận thức:



https://khonggianmang.vn/

12. Nâng cao nhận thức:





❋ Làm các bài kiểm tra phát hiện lừa đảo, phishing qua email:

> Truy cập:
https://congcu.khonggianmang.vn/phishing-quiz/

❋ Làm các bài kiểm tra phát hiện lừa đảo, phishing qua tin nhắn:

> Truy cập:
https://congcu.khonggianmang.vn/dauhieuluadao/

THANKS YOU