ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

Chuyên đề 2:

Kỹ năng bảo vệ An toàn thông tin trên môi trường số

Nội dung

1. Các nguy cơ phổ biến: lừa đảo trực tuyến, giả mạo, tấn công
2. Cách xây dựng mật khẩu mạnh, quản lý tài khoản, xác thực 2 lớp
3. Kỹ năng nhận diện tin giả, cung cấp dữ liệu

Phần 1

CÁC NGUY CƠ PHỔ BIẾN: LỪA ĐẢO TRỰC TUYẾN, GIẢ MẠO, TẤN CÔNG

Tình hình ATTT tại Việt Nam và trên thế giới.

* Việt Nam - một trong những quốc gia bị tấn công mạng nhiều nhất:

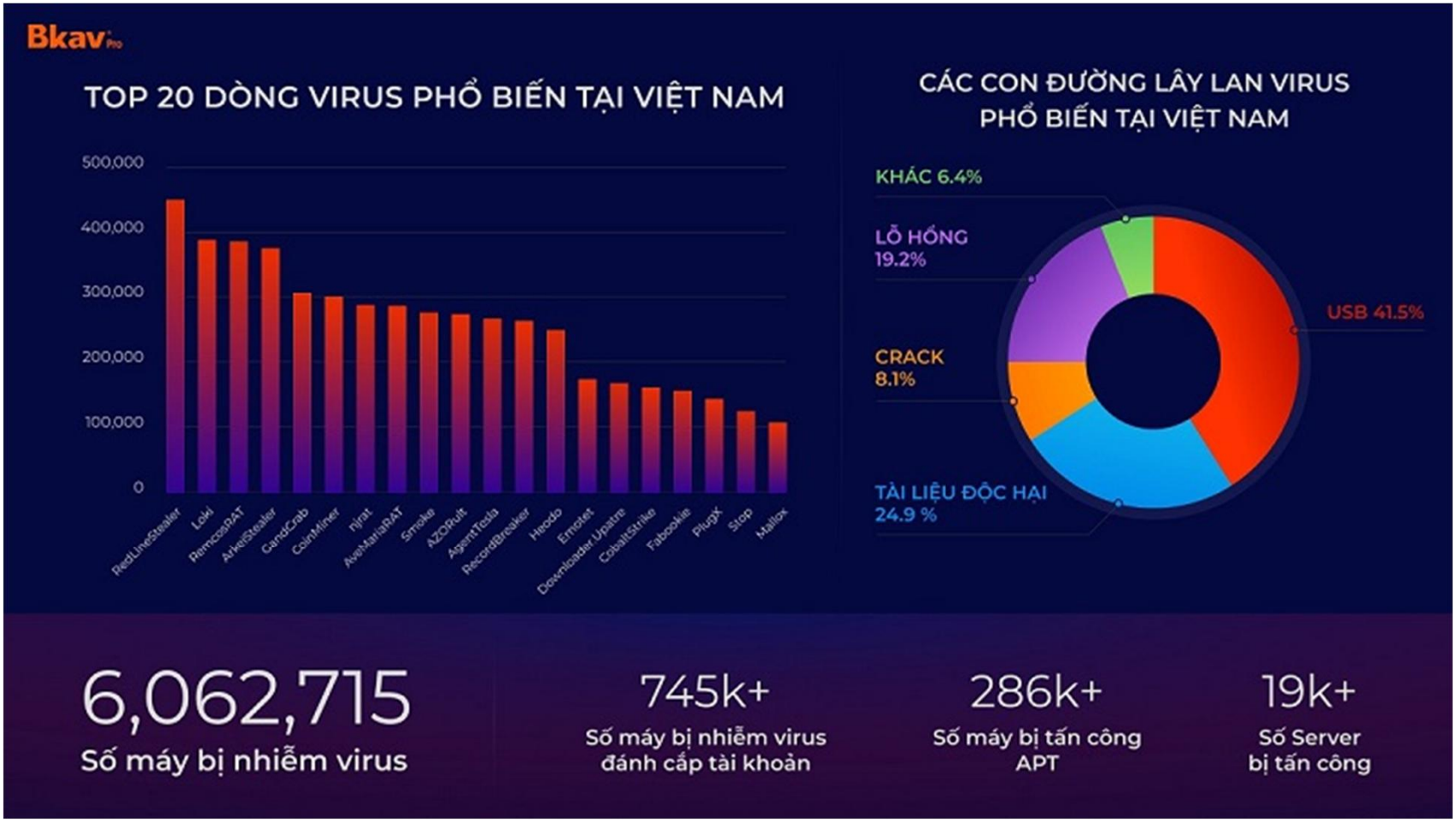
- Việt Nam nằm trong nhóm 3 quốc gia bị tấn công mạng nhiều nhất tại khu vực châu Á - Thái Bình Dương.
- 6 tháng đầu năm 2023, phát hiện gần 17 triệu cảnh báo dấu hiệu hoạt động tấn công mạng (tăng 240% so với năm 2022).

Tình hình ATTT tại Việt Nam và trên thế giới.

- Trong 3 năm qua, Bộ Công an phát hiện hàng trăm cá nhân, tổ chức liên quan bán dữ liệu cá nhân:
  + Thu thập, mua bán trái phép phát hiện được lên tới gần 1.300 GB, trong đó có nhiều dữ liệu cá nhân nội bộ, nhạy cảm.
- Báo cáo của BKAV 12/2023: Thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam ở mức 17,3 nghìn tỷ VND (tương đương 716 triệu USD) => ***Giảm so với các năm trước***

Tình hình ATTT tại Việt Nam và trên thế giới.

- Tình hình an ninh mạng trong nước vẫn nổi cộm nhiều vấn đề nóng khi tấn công bằng virus mã hóa dữ liệu tiếp tục gia tăng, nhắm vào các máy chủ trọng yếu;
- Máy tính không có kết nối Internet cũng có thể bị tấn công gián điệp APT (Advanced Persistent Threats);
- Lừa đảo tài chính trực tuyến không có dấu hiệu hạ nhiệt bởi nguồn cơn là tài khoản ngân hàng rác…



Tình hình ATTT tại Việt Nam và trên thế giới.

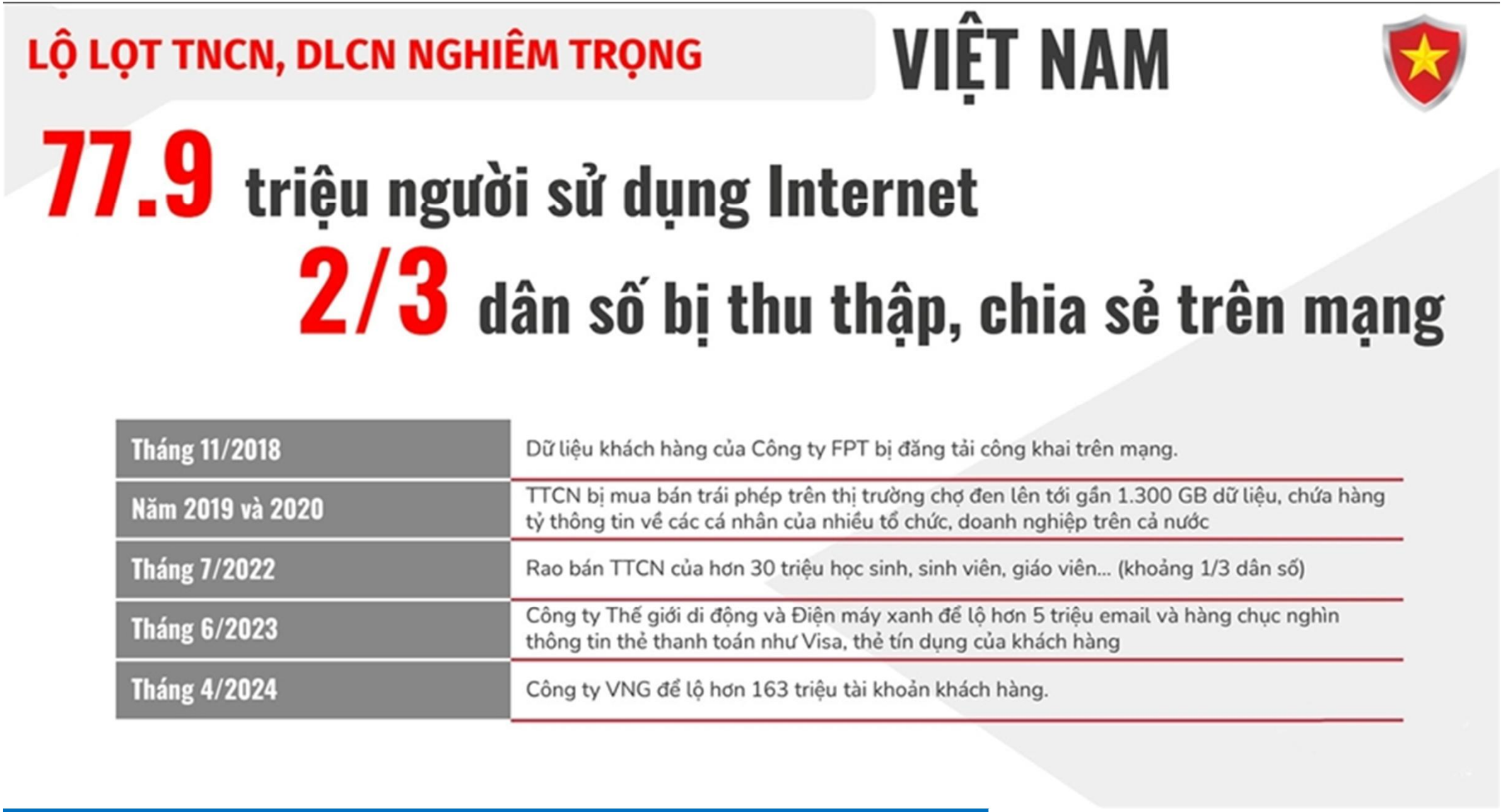
- Tài khoản ngân hàng rác là nguồn cơn của lừa đảo tài chính qua mạng;
- Tỷ lệ người dùng nhận được tin nhắn, cuộc gọi lừa đảo tiếp tục gia tăng. Nếu năm 2022, con số này là 69,6% thì trong năm 2023 là 73%.
- Các kênh trên Facebook, Telegram, Twitter… việc mua bán tài khoản ngân hàng rác diễn ra nhộn nhịp.


730
MUA BÁN TÀI KHOẢN NGÂN...
4,549 subscribers
Pinned Message
DỊCH VỤ BANKING
DỊCH VỤ BANKING
Bank quẩy hạn mức 3-5 tỷ, bank online, bank ảo, thẻ tín dụng, visa, full hạn mức giao dịch (Làm theo thông tin cccd yêu cầu của ae)
Tài khoản doanh nghiệp theo tên công ty, check đầy đủ mã số thuế, khai thuế đầy đủ theo kỳ, giấy tờ chứng từ đầy đủ (Làm theo thông tin cccd yêu cầu của ae)
Cấp lại Mật khẩu, Otp , Định danh ngân hàng, nâng hạn mức
Mở khoá banking, Reset OTP, Rút tiền bị kẹt, yêu cầu giải trình..vv
Tool làm bank ảo Vpbank, shb, acb, msb, esimbank, vietinbank, vcb
Check thông tin ngân hàng, check sdt, check CIC..vv
Join


mua tài khoản ngân hàng
Tất cả
Bài viết
Mọi người
Reels
Nhóm
Nhóm
Mua bán tài khoản ngân hàng, thẻ ATM theo tên yêu cầu ✅
Công khai · 115K thành viên · Hơn 10 bài viết/ngày
Chuyên banking online ảo theo tên, banking quẩy, thẻ ATM uy tín online trên toàn quốc...
Tham gia
MUA BÁN TÀI KHOẢN NGÂN HÀNG/(CHECK PHỐT)
Công khai · 4,5K thành viên · 6 bài viết/ngày
MUA BÁN ATM NGÂN HÀNG UY TÍN ĐÃ QUA SÀN LỌC
Tham gia
MUA BÁN TÀI KHOẢN BANKING - THẺ ATM NGÂN HÀNG UY TÍ...
Riêng tư · 20K thành viên · 2 bài viết/ngày
🔥 UY TÍN - HỢP TÁC LÂU DÀI 🔥
LƯU Ý: GROUP KHÔNG TIẾP CÒ, MỜI
Tham gia

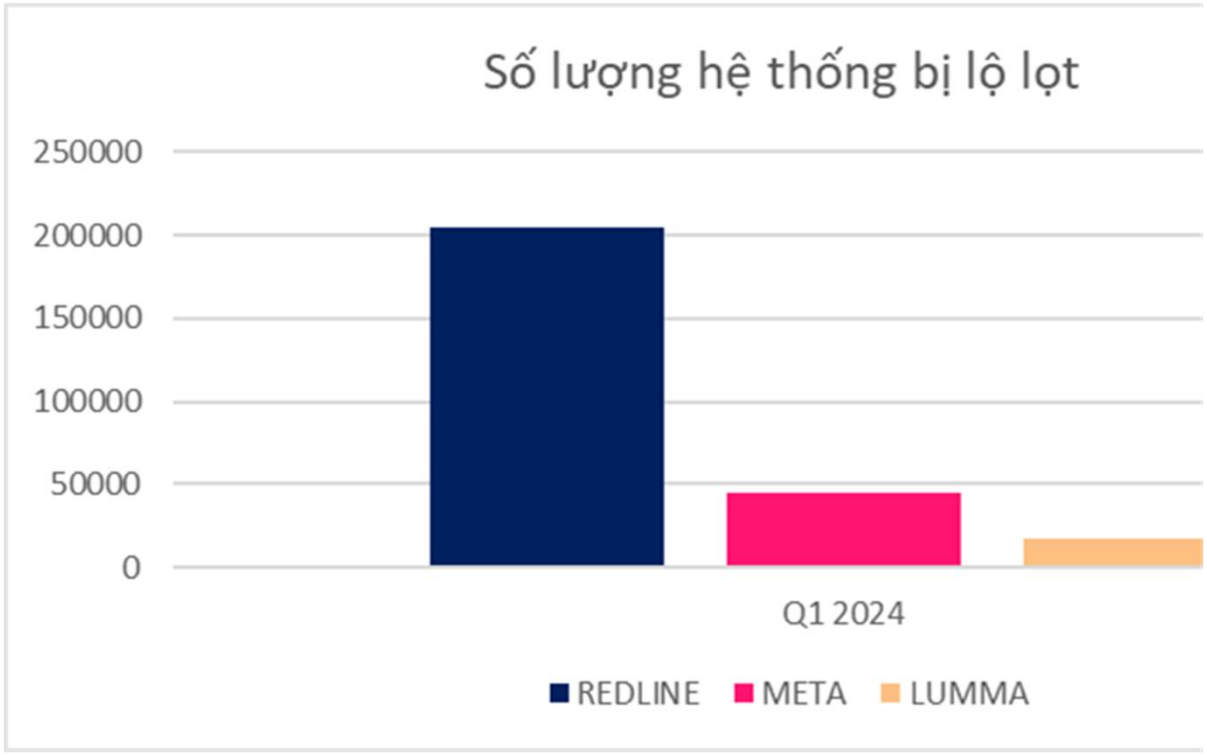

mua tài khoản ngân hàng
Bộ lọc
Nhóm công khai
Mua bán tài khoản ngân hàng, thẻ ATM t...
Tham gia
Nhóm Công khai · 115K thành viên
Giới thiệu
Chuyên banking online ảo theo tên, banking quẩy, thẻ ATM uy tín online trên toàn quốc tele :
Thành viên
Dương là quản trị viên. Ngọc Ánh và 2 thành viên khác là người kiểm duyệt.
Hoạt động trong nhóm
113 bài viết mới hôm nay
214 bài viết mới trong tháng qua
Tổng số 115K thành viên
+ 499 trong tuần trước
Tạo khoảng 3 năm trước

Vấn đề lộ lọt dữ liệu cá nhân



Vấn đề lộ lọt dữ liệu cá nhân

- Các dòng mã độc Stealer được phát tán rộng tại Việt Nam có thể kể đến như: **Meta Stealer, Redline, Lumma, VietCredCare**.



Theo VNPT CTIP report


tuổi trẻ online

MỚI NHẤT XEM NHIỀU VIDEO THỜI SỰ THẾ

Kinh doanh Tài chính Doanh nghiệp Mua sắm

16/12/2024 10:11 GMT+7

Người Việt mất 18.900 tỉ đồng vì bị lừa đảo trong năm 2024

ĐỨC THIỆN

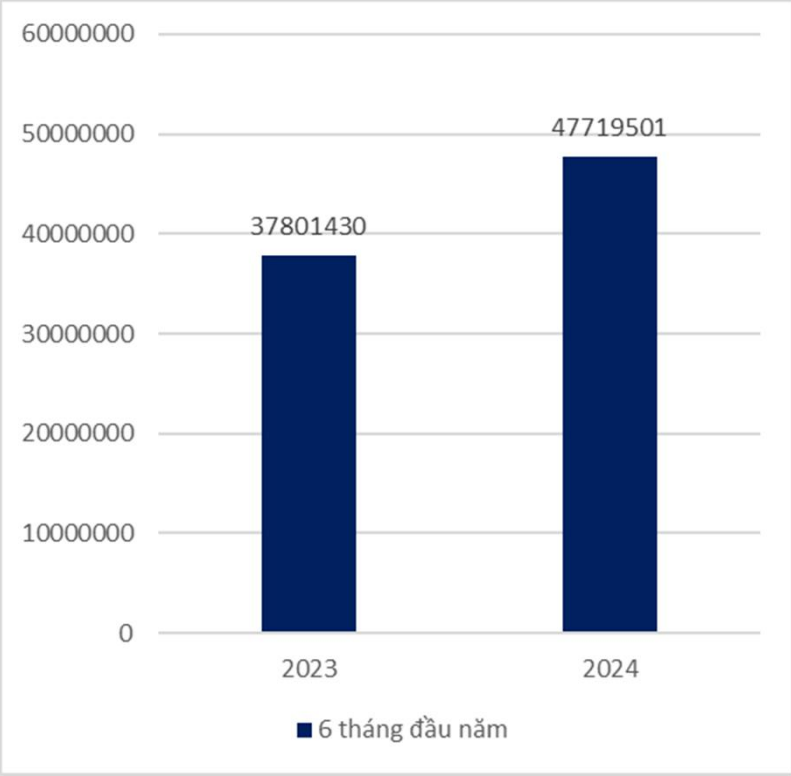
Tuổi Trẻ trên Google News

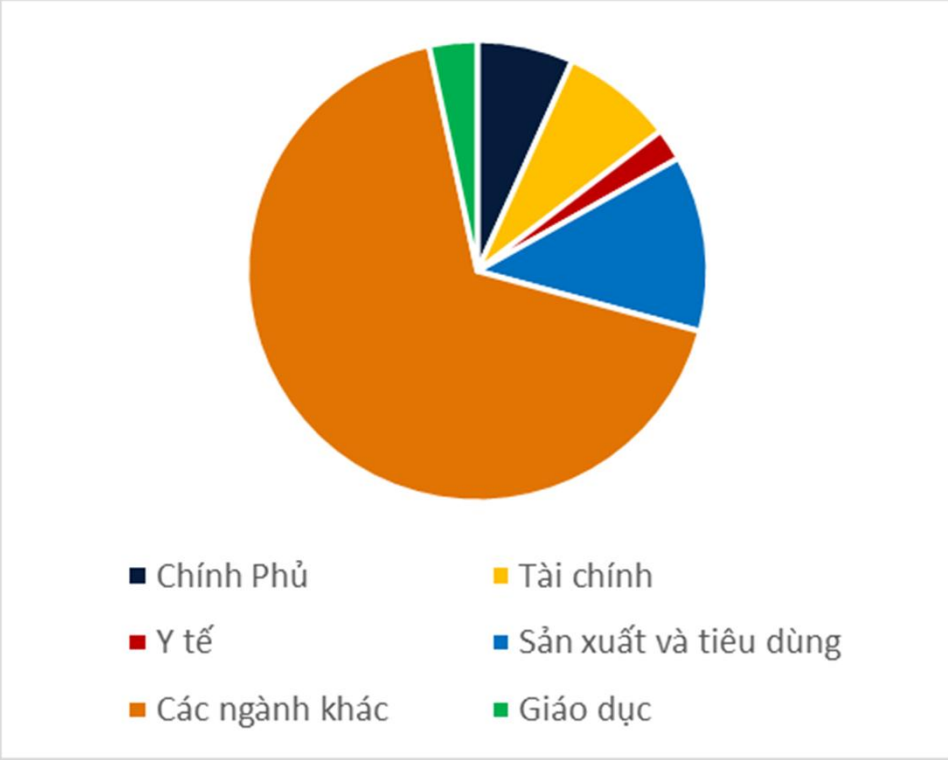
Nghe đọc bài 3:16 1x Nữ miền Bắc

Lừa đảo trực tuyến tiếp tục hoành hành trong năm 2024, cứ 220 người dùng điện thoại thông minh tại Việt Nam thì có 1 người trở thành nạn nhân của lừa đảo. Hình ừa đảo phổ biến nhất là mời gọi đầu

Vấn đề lộ lọt dữ liệu cá nhân

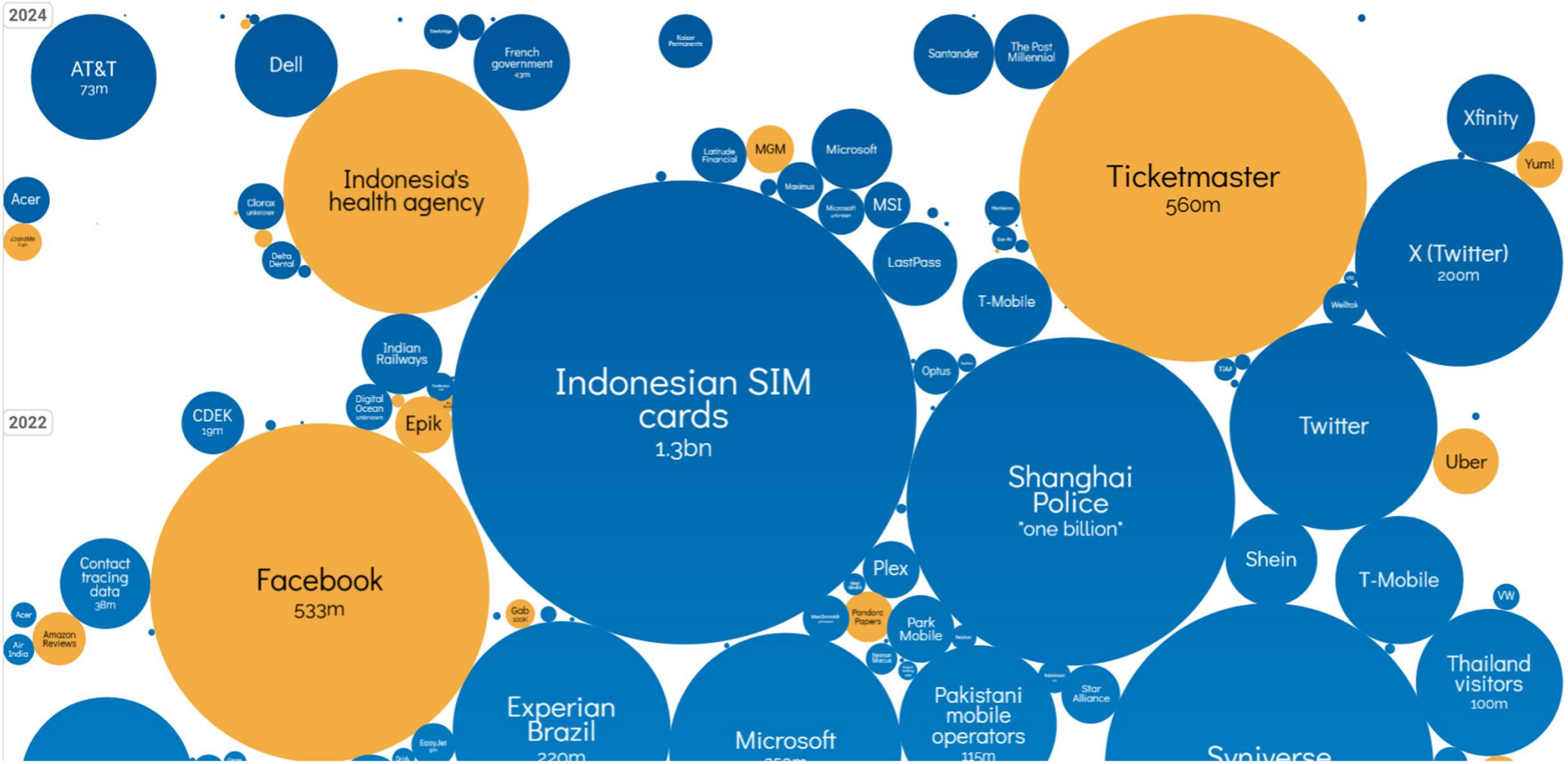
Số lượng bản ghi thông tin dữ liệu đăng nhập bị đánh cắp tăng **gấp 2** so với cùng kỳ năm 2023:





Theo VNPT CTIP report

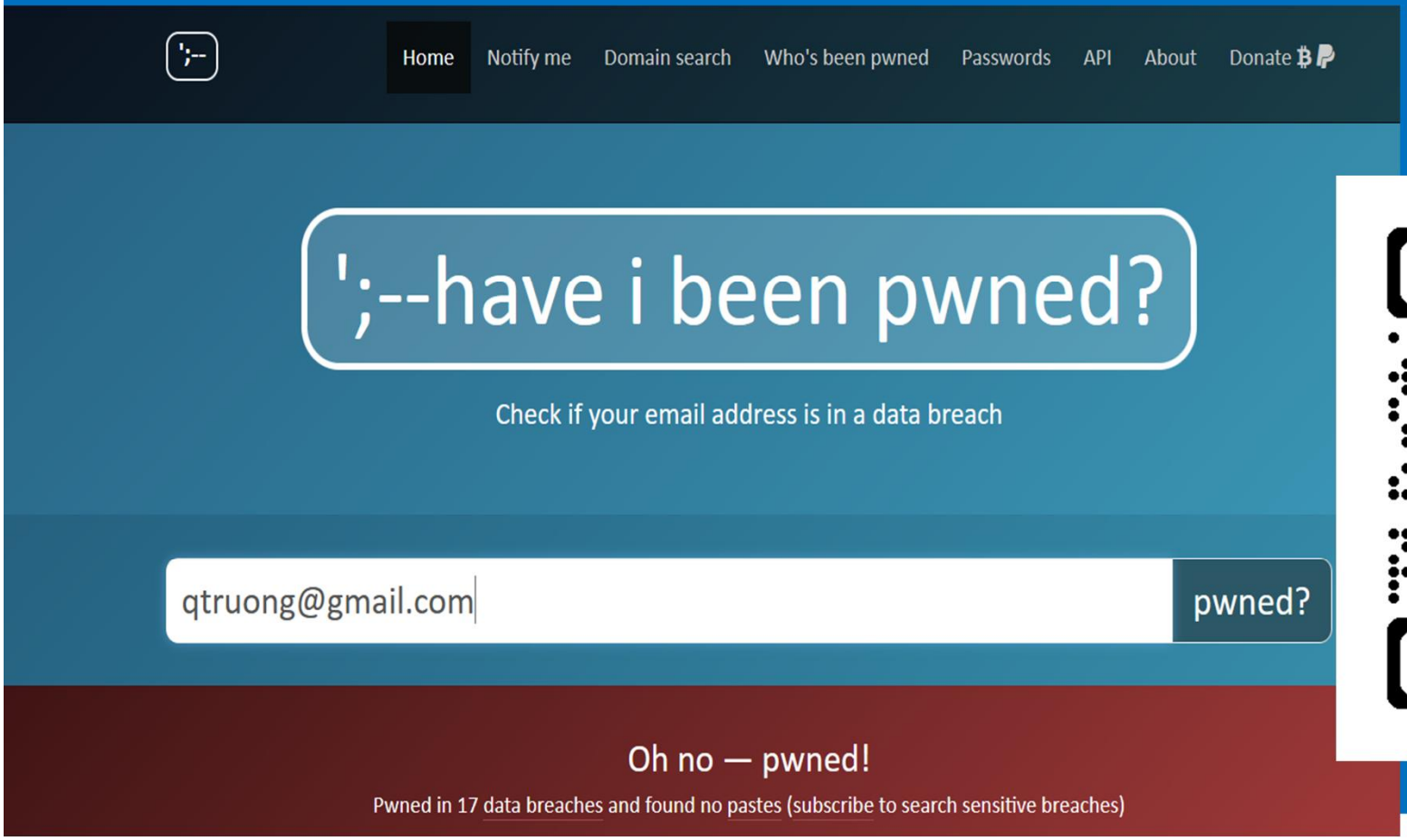
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Các vụ rò rỉ dữ liệu lớn trên thế giới

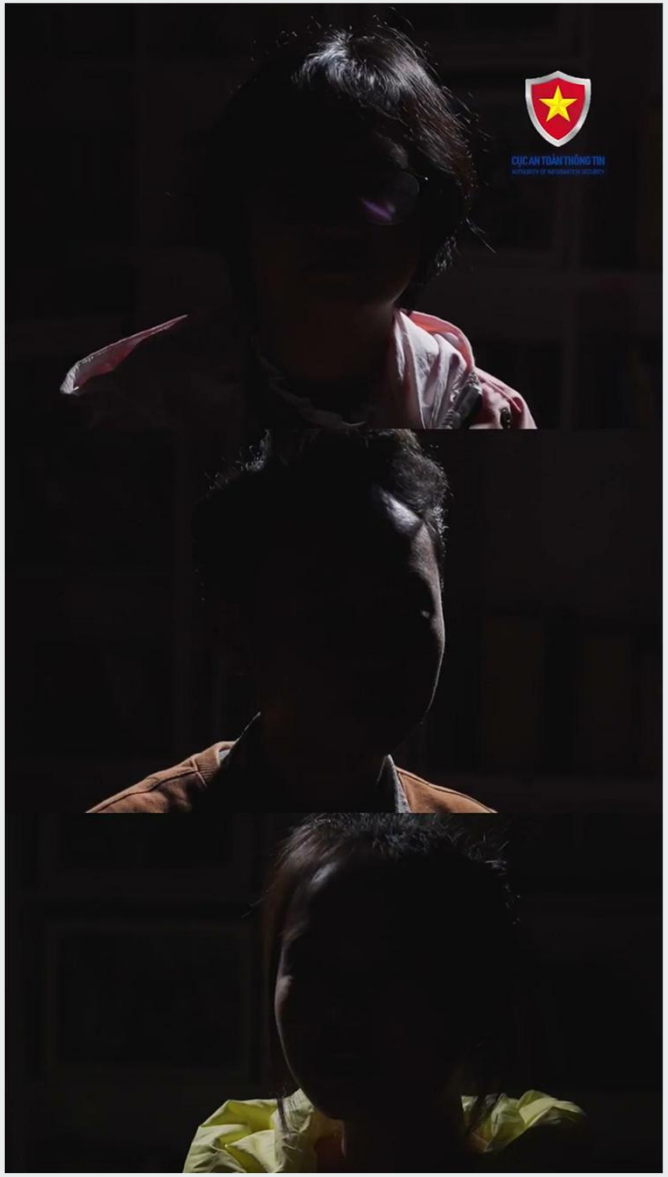
https://haveibeenpwned.com/

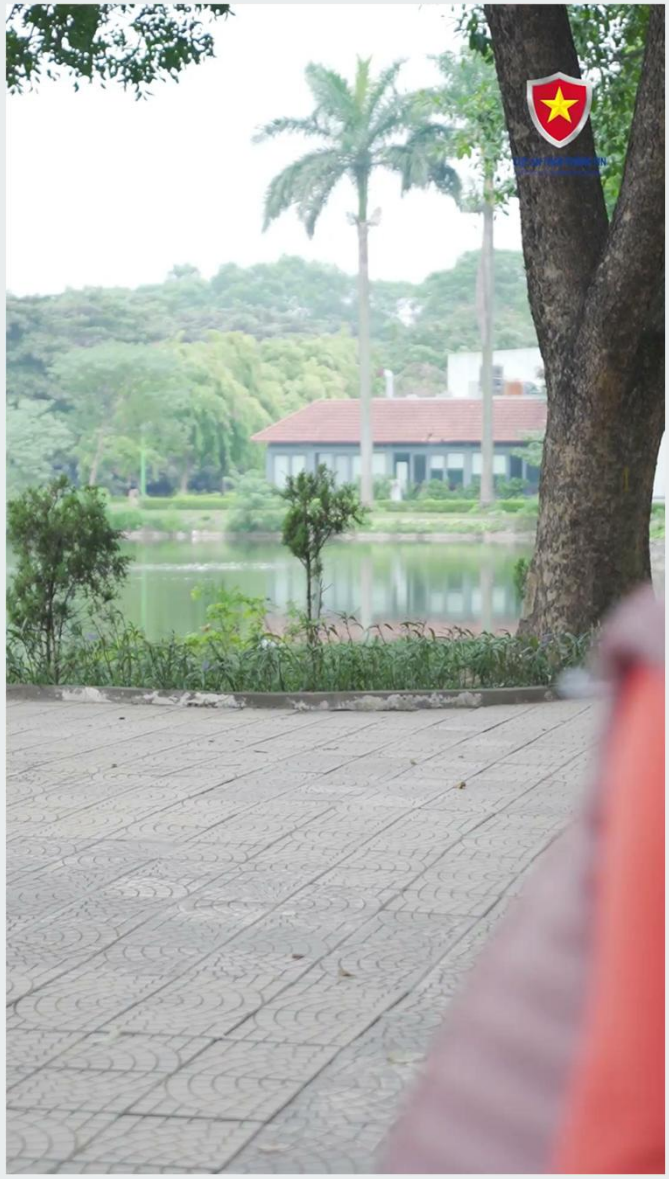
Thông tin cá nhân của bạn có bị rò rỉ không?



Các bài học lừa đảo phổ biến trong thời gian gần đây

Video: https://drive.google.com/drive/folders/12pXYrdCsACpFlh-wHIqzR3aH2YWsVWqX?usp=sharing





Ảnh hưởng của rủi ro mạng đến doanh nghiệp

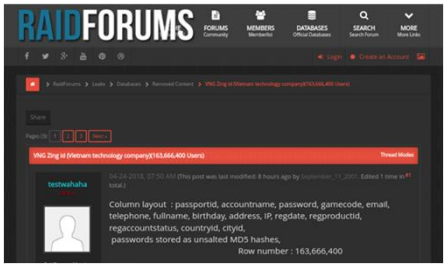
Thiệt hại kinh tế, gián đoạn hoạt động

Mã độc WannaCry, 2017

Sự cố CrowdStrike, 2024

Lộ thông tin cá nhân của khách hàng và nhân viên

Công ty VNG, 2024

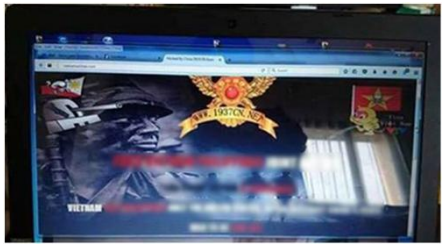


ChatGPT, 2023

Tổn hại danh tiếng của doanh nghiệp

Yahoo, 2013-2014

Vietnam Airlines, 2016



Khái niệm lừa đảo (phishing) trên môi trường mạng

Phishing là gì?

- Phishing là một hình thức lừa đảo trực tuyến, trong đó kẻ xấu giả mạo danh một thực thể đáng tin cậy để lừa người dùng cung cấp thông tin nhạy cảm, chẳng hạn như tên đăng nhập, mật khẩu hoặc thông tin thẻ tín dụng.

- Kẻ tấn công sử dụng các phương tiện như email, tin nhắn văn bản, tin nhắn trực tiếp, trang web giả mạo và mạng xã hội để tiếp cận nạn nhân và đánh lừa họ.

Khái niệm lừa đảo (phishing) trên môi trường mạng

Phishing là gì?

- Phishing là một trong những hình thức tấn công phổ biến nhất trên mạng và đã gây ra nhiều thiệt hại cho các tổ chức và cá nhân.

- Để tránh bị lừa đảo, người dùng cần phải hết sức cẩn trọng khi cung cấp thông tin nhạy cảm trên mạng và luôn luôn kiểm tra xem các thông tin yêu cầu có đáng tin cậy hay không trước khi cung cấp chúng.

Các loại hình của phishing

Một số loại hình phổ biến của phishing:

How phishing works (source).

- Phishing qua email.
- Phishing qua SMS
- Phising qua cuộc gọi/Video call
- Phishing thông qua nhân bản
- Phishing qua công cụ tìm kiếm
- Phishing sử dụng mã độc
- Mã hóa đòi tiền chuộc (Ransomware)

Các loại hình của phishing

Mục tiêu của phishing:

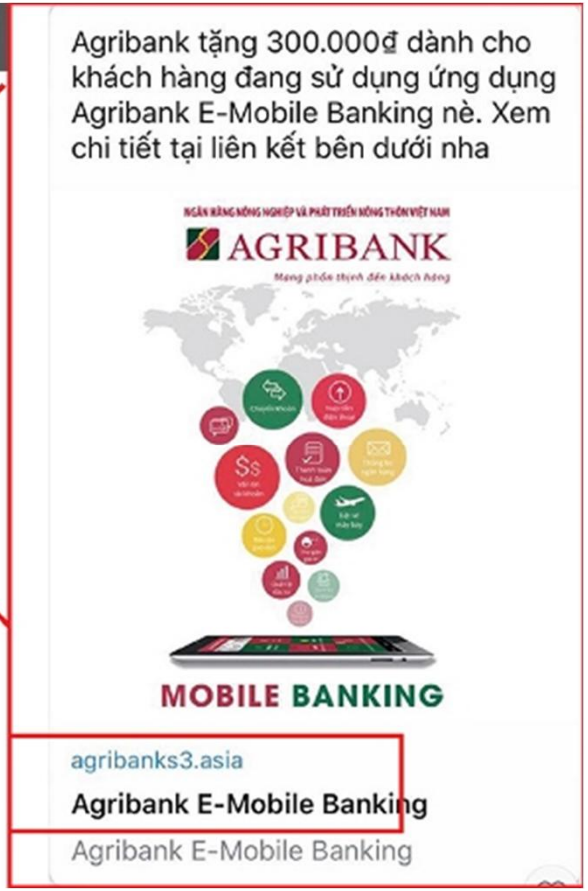
- Mục tiêu của phishing là lừa đảo, chiếm đoạt thông tin nhạy cảm hoặc tiền của người dùng.

Tại sao phishing đang gia tăng?

- Phishing đang gia tăng bởi vì nó là một trong những kỹ thuật tấn công đơn giản và hiệu quả nhất để tấn công người dùng và đánh cắp thông tin nhạy cảm.

How phishing works (source).

Các loại hình của phishing



Giả trang web của ngân hàng và thông tin y tế

Các loại hình của phishing

NCSC VN
National Cyber Security Center

CẢNH GIÁC THỦ ĐOẠN LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN
TUYỂN CỘNG TÁC VIÊN SÀN THƯƠNG MẠI ĐIỆN TỬ

- Cảnh giác, kiểm tra kỹ thông tin của đơn vị cung ứng việc làm
- Lợi dụng sự uy tín của các sàn TMĐT nổi tiếng như Lazada, Shopee, Tiki, Sendo, Vietlotts... Các đối tượng lừa đảo thường gửi cho nạn nhân các trang web giả mạo có giao diện gần giống với trang web chính thống.

NẠN NHÂN

- Người muốn làm cộng tác viên
- Người không có việc làm
- Người muốn kiếm thêm thu nhập tại nhà và kinh doanh online
- Học sinh, sinh viên muốn kiếm việc làm thêm

CẢNH BÁO

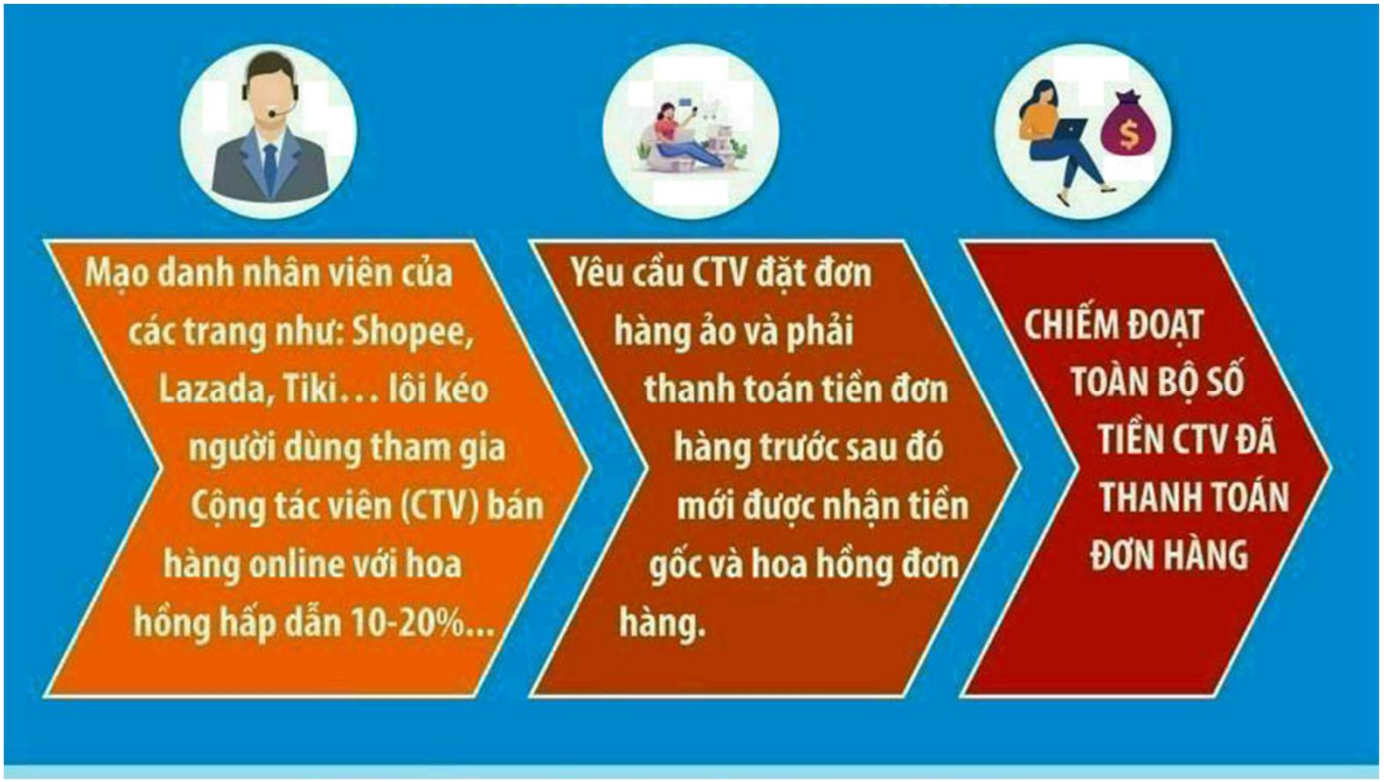
THỦ ĐOẠN

- Khi gặp trường hợp lừa đảo, gửi cảnh báo về địa chỉ canhbao.ncsc.gov.vn
- Kiểm tra thông tin chính thống (email, website, số điện thoại, địa chỉ,...) của các tổ chức, doanh nghiệp trên website: tinnhiemmang.vn
- Nâng cao nhận thức về an toàn thông tin để nhận biết các dấu hiệu lừa đảo qua khonggianmang.vn / dauhieuluadao.com

LIÊN HỆ

- Gửi link cài app
- Hứa hẹn làm ít, thu nhập cao (Ví dụ: Được hoàn tiền gốc và hoa hồng ngay từ nhiệm vụ đầu tiên,...)
- Hướng dẫn thanh toán đơn để chiếm đoạt tiền %, hoa hồng,...

Các loại hình của phishing



Phương thức lừa đảo của hacker

Các loại hình của phishing

Hình thức tấn công Phishing nâng cao

- Tấn công phishing thông qua việc sử dụng mã độc được cài cắm, lây nhiễm vào máy tính, điện thoại smartphone của nạn nhân.

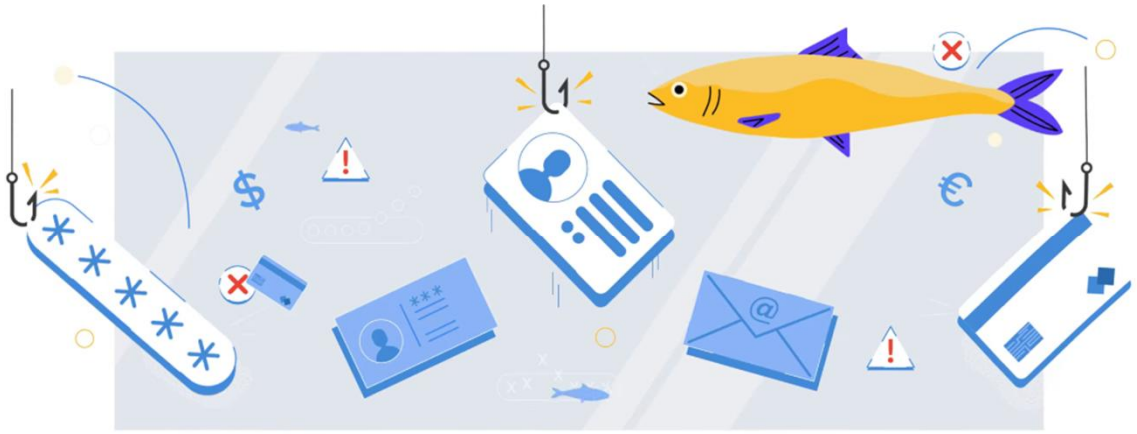
Cách phòng chống tấn công lừa đảo

Quiz phát hiện tấn công lừa https://phishingquiz.withgoogle.com/

Google Phishing Quiz

Developed by JIGSAW

English (United States)



Can you spot when you're being phished?

Phishing attacks attempt to trick unsuspecting users into revealing personal or financial information, often by mimicking content from well-known, trusted companies.

AI is already making phishing attacks more sophisticated, personalized, and common.

Think you can tell what's real or fake?

Take the quiz

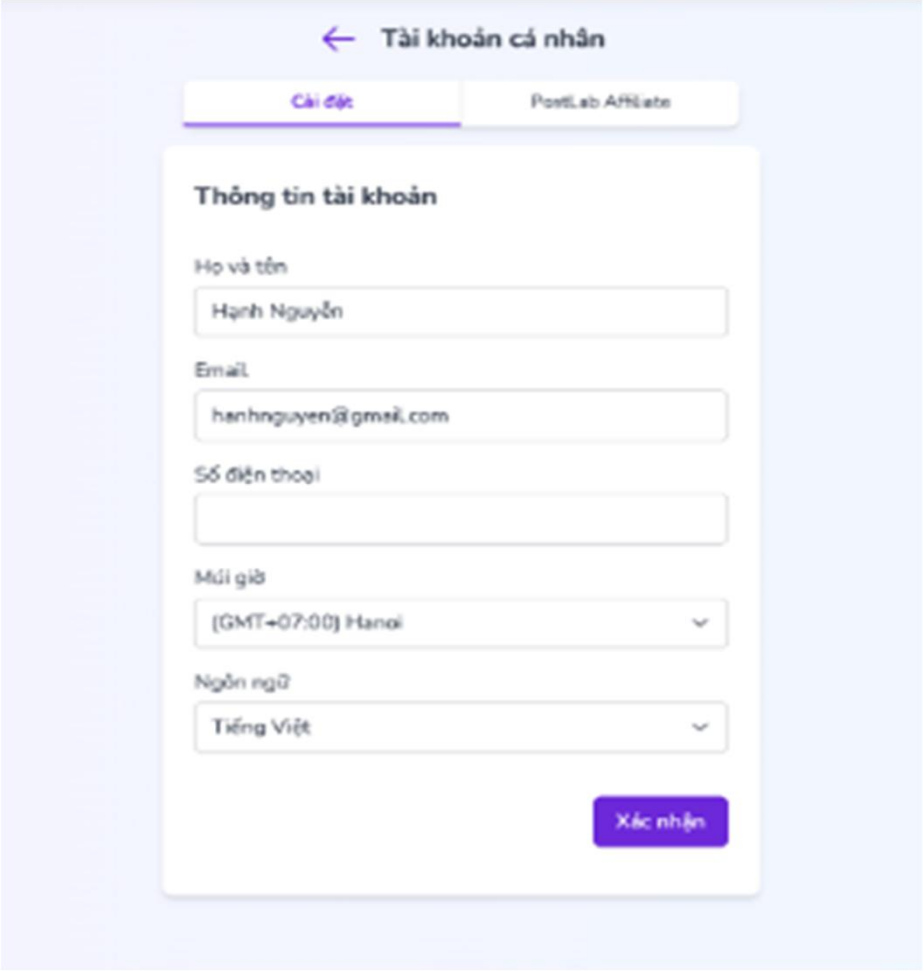
Phần 2

CÁCH XÂY DỰNG MẬT KHẨU MẠNH, QUẢN LÝ TÀI KHOẢN, XÁC THỰC 2 LỚP

Tại sao phải bảo mật tài khoản cá nhân?

Tài khoản cá nhân là gì?

- Tài khoản cá nhân là tài khoản được cấp phép để người sử dụng truy cập vào các dịch vụ và tính năng trực tuyến trên các trang mạng xã hội, các website thương mại điện tử hay các website cung cấp dịch vụ đến người dùng. Nó bao gồm các thông tin như tên, địa chỉ email, mật khẩu và một số thông tin khác.

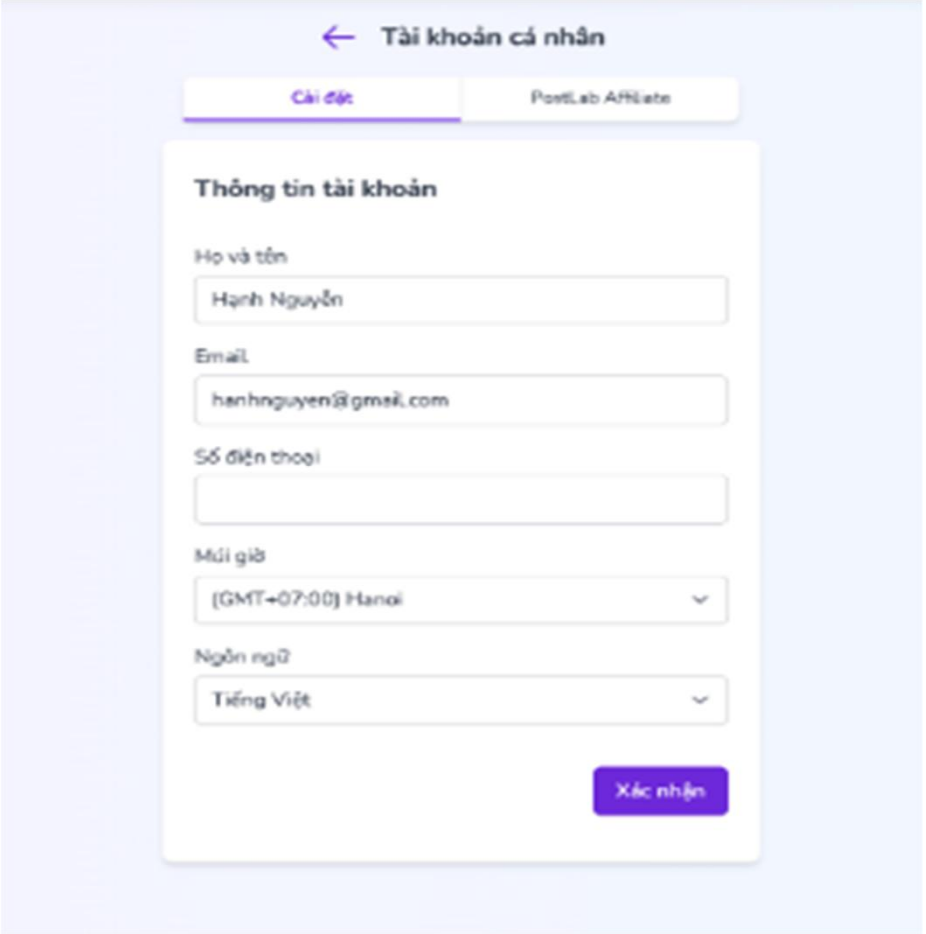


Tại sao phải bảo mật tài khoản cá nhân?

Đặc điểm của tài khoản cá nhân

• Tên đăng nhập (Username): Đây là thông tin duy nhất dùng để xác định và đăng nhập vào tài khoản của người dùng.

• Password: Là thông tin bảo mật cần được dùng bảo vệ và duy trì bí mật để ngăn chặn người khác truy cập trái phép.



Tại sao phải bảo mật tài khoản cá nhân?

Phương thức, thủ đoạn đánh cắp dữ liệu cá nhân

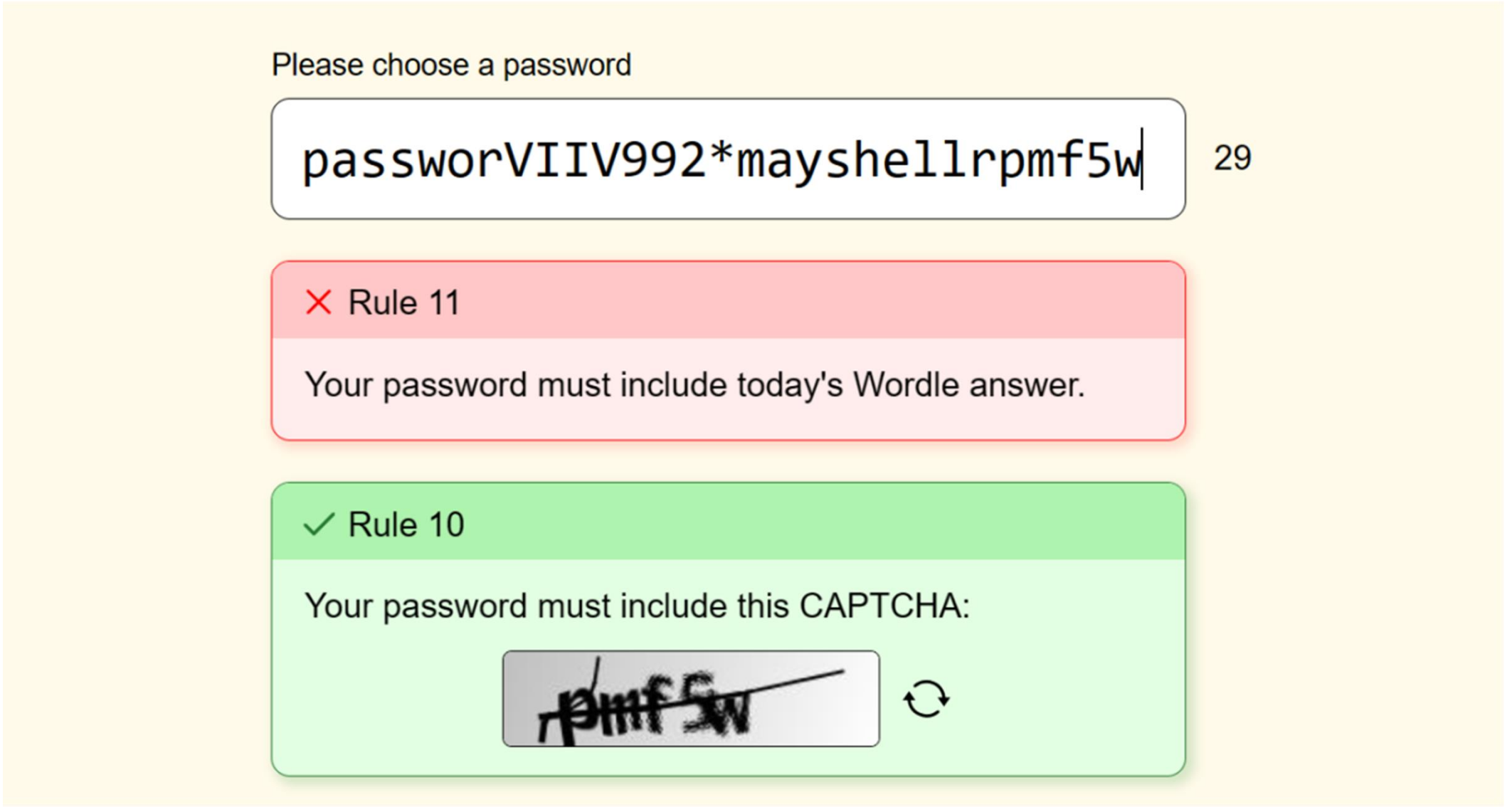
- Sử dụng mã độc
- Tấn công vào hệ thống lưu trữ dữ liệu cá nhân
- Lợi dụng sự chủ quan, lơ là và đánh vào tâm lý "hám lời" của người dân
- Các doanh nghiệp, công ty kinh doanh dịch vụ có thu thập dữ liệu cá nhân của khách hang
- Tấn công thông qua vật trung gian
- Tấn công qua các thiết bị thông minh

Một số cơ chế bảo mật tài khoản và thiết bị?

- Xem xét kỹ trước khi cài đặt ứng dụng lên thiết bị
- Sử dụng mật khẩu mạnh và xác thực hai yếu tố
- Hạn chế quyền truy cập dữ liệu
- Sử dụng mã hóa và kết nối an toàn
- Cập nhật phần mềm và chống malware
- Lưu dữ liệu định kỳ
- Kiểm tra và theo dõi hoạt động trực tuyến
- Cẩn trọng trong việc chia sẻ thông tin cá nhân
- Chú ý đến email và tin nhắn giả mạo
- Giáo dục và nâng cao nhận thức

Đặt mật khẩu mạnh

- Trò chơi đặt mật khẩu mạnh: https://neal.fun/password-game/



Một số cơ chế bảo mật tài khoản và thiết bị?

Xem xét kỹ trước khi cài đặt ứng dụng lên thiết bị

- Việc đánh giá kỹ lưỡng trước khi cài đặt ứng dụng là cực kỳ quan trọng để bảo vệ thông tin cá nhân.
- Nhằm hạn chế tình trạng rò rỉ dữ liệu cá nhân.
- Người dùng nên kiểm tra xem ứng dụng có các chứng chỉ bảo mật, phù hợp với quyền riêng tư và có chính sách bảo mật rõ ràng hay không.
- Nên tìm hiểu về nhà phát triển của ứng dụng, xem xét về uy tín và lịch sử của họ trong việc bảo vệ dữ liệu người dùng.

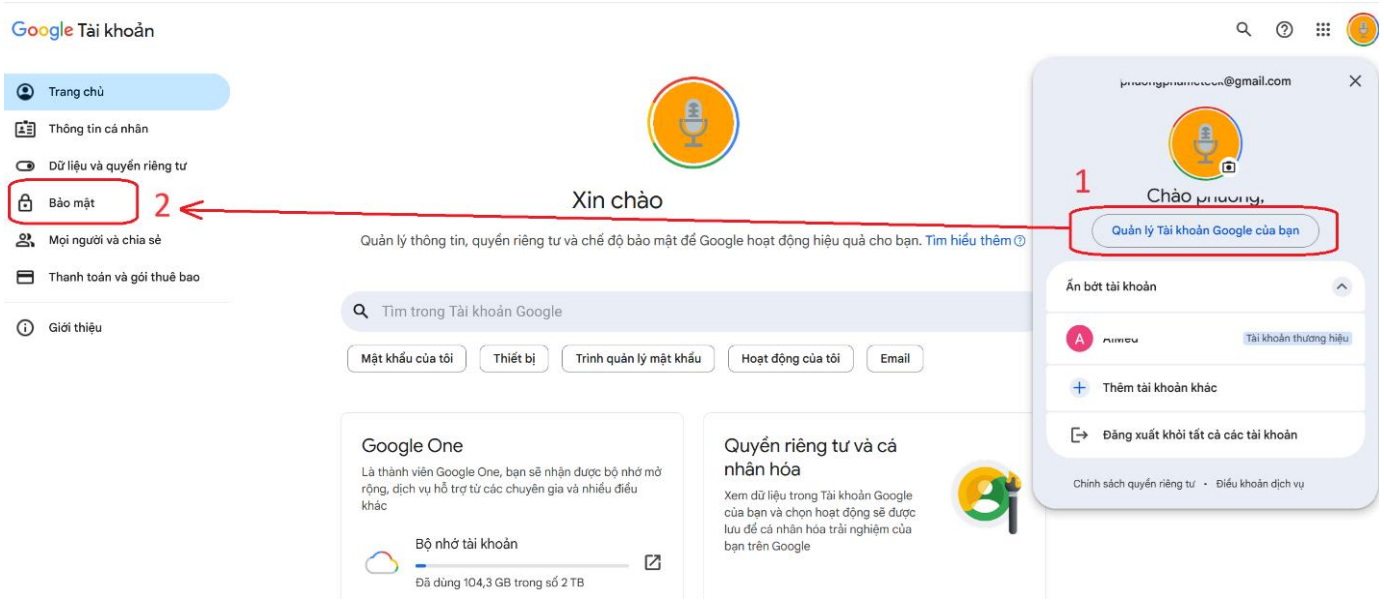
Một số cơ chế bảo mật tài khoản và thiết bị?

Sử dụng mật khẩu mạnh và xác thực hai yếu tố

- Đặt mật khẩu mạnh cho tài khoản
- Sử dụng một sự kết hợp của chữ cái, số và ký tự đặc biệt.
- Kích hoạt xác thực hai yếu tố để bảo vệ tài khoản.
- Thêm dấu vân tay để truy cập vào tài khoản.

Bảo vệ tài khoản trên Google

- Để quản lý tài khoản và tăng tính bảo mật cho tài khoản, Hãy truy cập địa chỉ https://myaccount.google.com



- Chọn **Bảo mật** để thiết lập các chế độ bảo vệ tài khoản như quản lý mật khẩu, xác minh 2 lớp (2FA), kiểm tra hoạt động của tài khoản, thiết lập email khôi phục, câu hỏi bảo mật và mã dự phòng ...

Một số cơ chế bảo mật tài khoản và thiết bị?

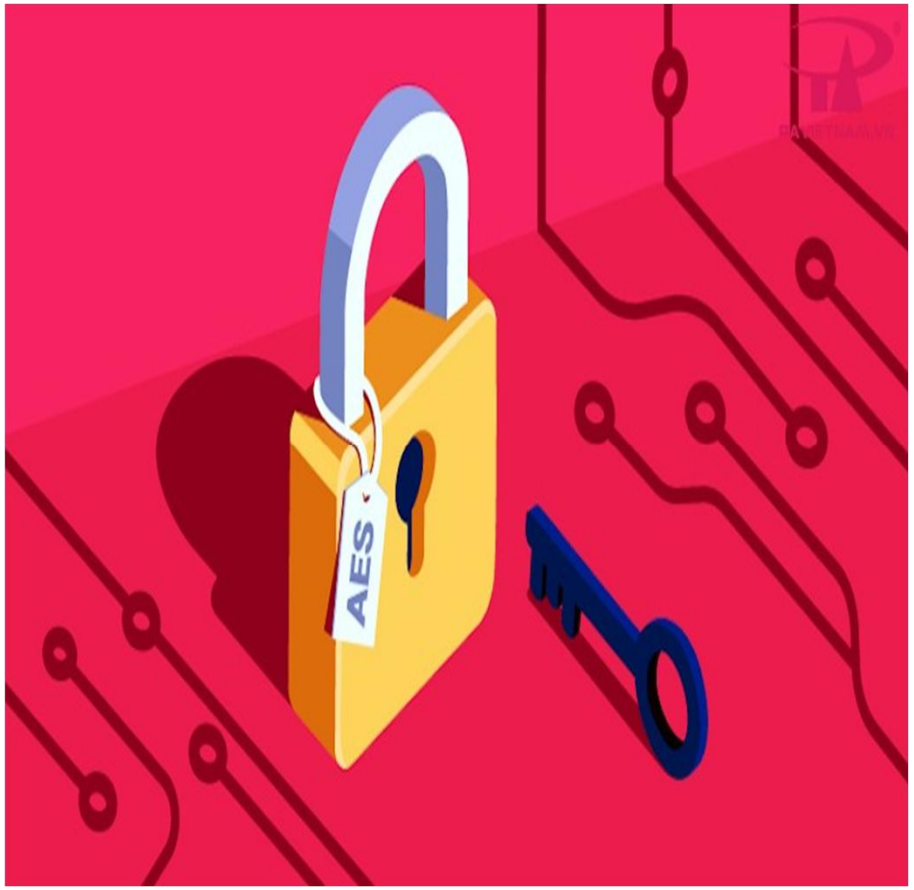
Hạn chế quyền truy cập dữ liệu

- Kiểm tra và điều chỉnh quyền truy cập dữ liệu của các ứng dụng trên thiết bị.
- Chỉ cấp quyền truy cập những thông tin cần thiết và hạn chế quyền truy cập.
- Điều này làm giảm khả năng thông tin cá nhân của bạn bị lộ.

Một số cơ chế bảo mật tài khoản và thiết bị?

Sử dụng mã hóa và kết nối an toàn

- Sử dụng các trang web có giao thức HTTPS
- tránh kết nối vào các mạng Wi-Fi công cộng không an toàn
- Sử dụng các công cụ mã hóa dữ liệu để bảo vệ thông tin



Một số cơ chế bảo mật tài khoản và thiết bị?

Cập nhật phần mềm và chống malware

- Cập nhật thường xuyên các bản vá lỗi và cải thiện bảo mật
- Luôn cập nhật các ứng dụng và hệ điều hành trên thiết bị
- Sử dụng phần mềm chống malware để ngăn chặn các phần mềm độc hại và tấn công từ hacker.

Một số cơ chế bảo mật tài khoản và thiết bị?

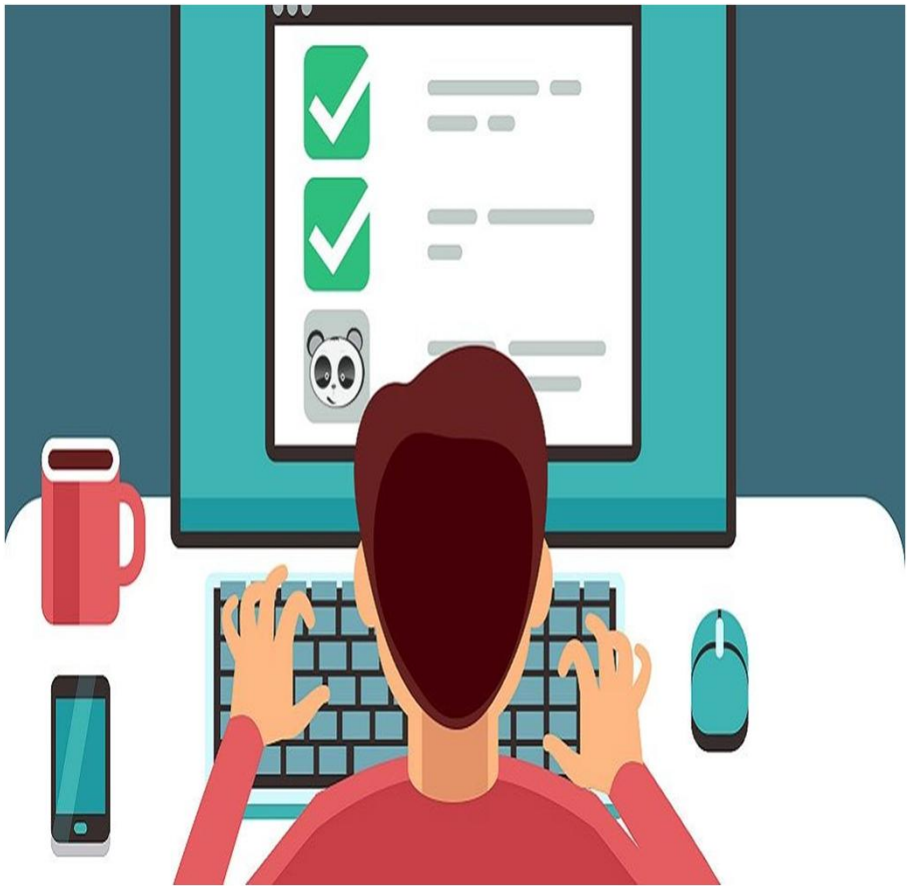
Lưu dữ liệu định kỳ

- Để đảm bảo an toàn cho dữ liệu cá nhân trên mạng người dùng cần thực hiện sao lưu dữ liệu định kỳ.
- Phòng tránh mất dữ liệu
- Đảm bảo tính toàn vẹn của dữ liệu
- Đảm bảo hiệu suất hệ thống

Một số cơ chế bảo mật tài khoản và thiết bị?

Kiểm tra và theo dõi hoạt động trực tuyến

- Kiểm tra và theo dõi hoạt động trực tuyến
- sử dụng các công cụ và ứng dụng quản lý mật khẩu để tạo và quản lý mật khẩu an toàn
- Kiểm tra các hoạt động đăng nhập và xem xét các hoạt động bất thường



Một số cơ chế bảo mật tài khoản và thiết bị?

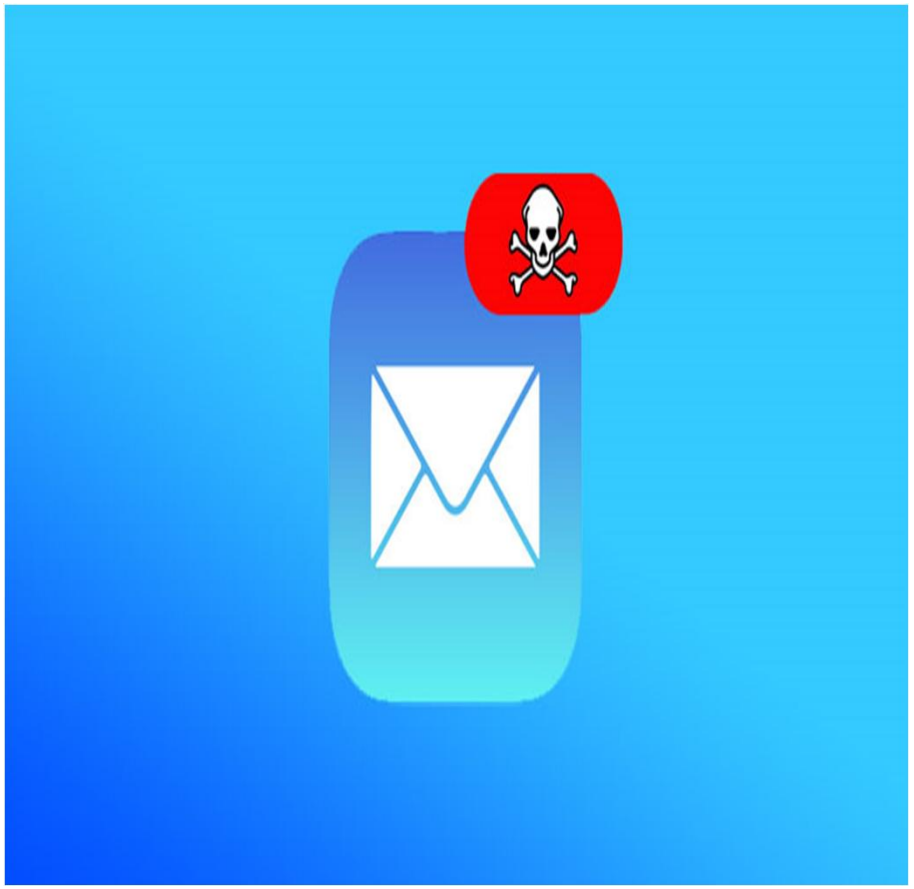
Cẩn trọng trong việc chia sẻ thông tin cá nhân

- Cẩn trọng khi chia sẻ thông tin cá nhân trên mạng
- Không nên công khai các thông tin, như: Ngày tháng, năm sinh, CCCD, số điện thoại, số tài khoản ngân hàng... lên các trang mạng xã hội.
- Đặc biệt CCCD chứa nhiều dữ liệu cá nhân quan trọng.

Một số cơ chế bảo mật tài khoản và thiết bị?

Chú ý đến email và tin nhắn giả mạo

- Hãy cẩn trọng với các email và tin nhắn giả mạo
- Kiểm tra kỹ nguồn gốc và tính xác thực của email trước khi cung cấp thông tin cá nhân hoặc nhấp vào các liên kết bên trong



Cách phòng chống tấn công lừa đảo

Các biện pháp phòng chống chung:

- Điều chỉnh cài đặt email.
- Tập trung vào từ khóa của email.
- Không cung cấp thông tin cá nhân.
- Tạo mật khẩu mạnh.
- Sử dụng phần mềm bảo mật.
- Cập nhật phần mềm.
- Đào tạo nhân viên.
- Xác thực thông tin của người gửi.
- Kiểm tra tài khoản thường xuyên.
- Giảm thiểu thông tin cá nhân trên mạng.

- Tóm lại, để phòng chống tấn công phishing, bạn cần cẩn thận và chú ý đến các thông tin, email và tin nhắn mà bạn nhận được trên mạng, cũng như sử dụng các giải pháp bảo mật để bảo vệ dữ liệu và thông tin cá nhân của mình.

Phần 3

KỸ NĂNG NHẬN BIẾT TIN GIẢ VÀ CUNG CẤP THÔNG TIN

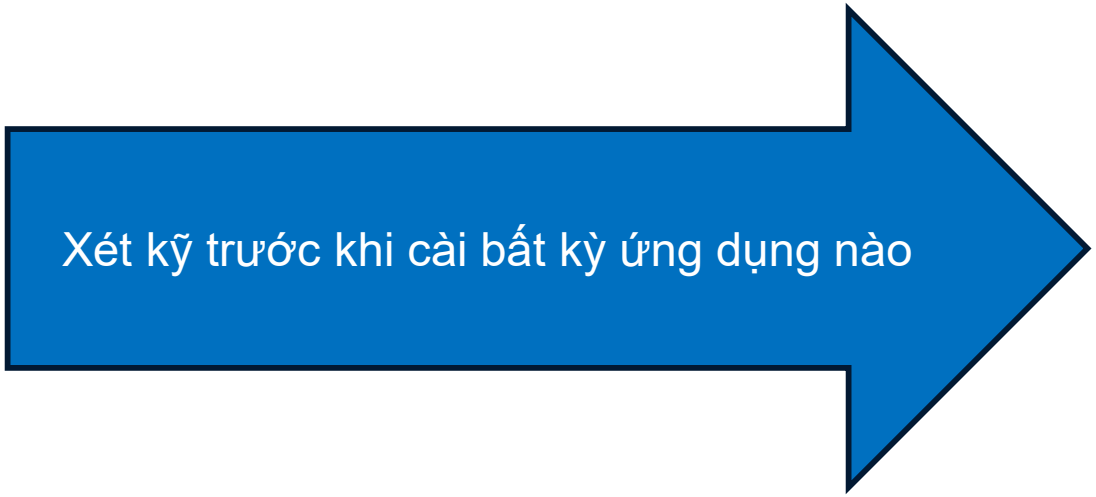
Nội dung

Nguyên tắc ngăn ngừa rò rỉ thông tin cá nhân

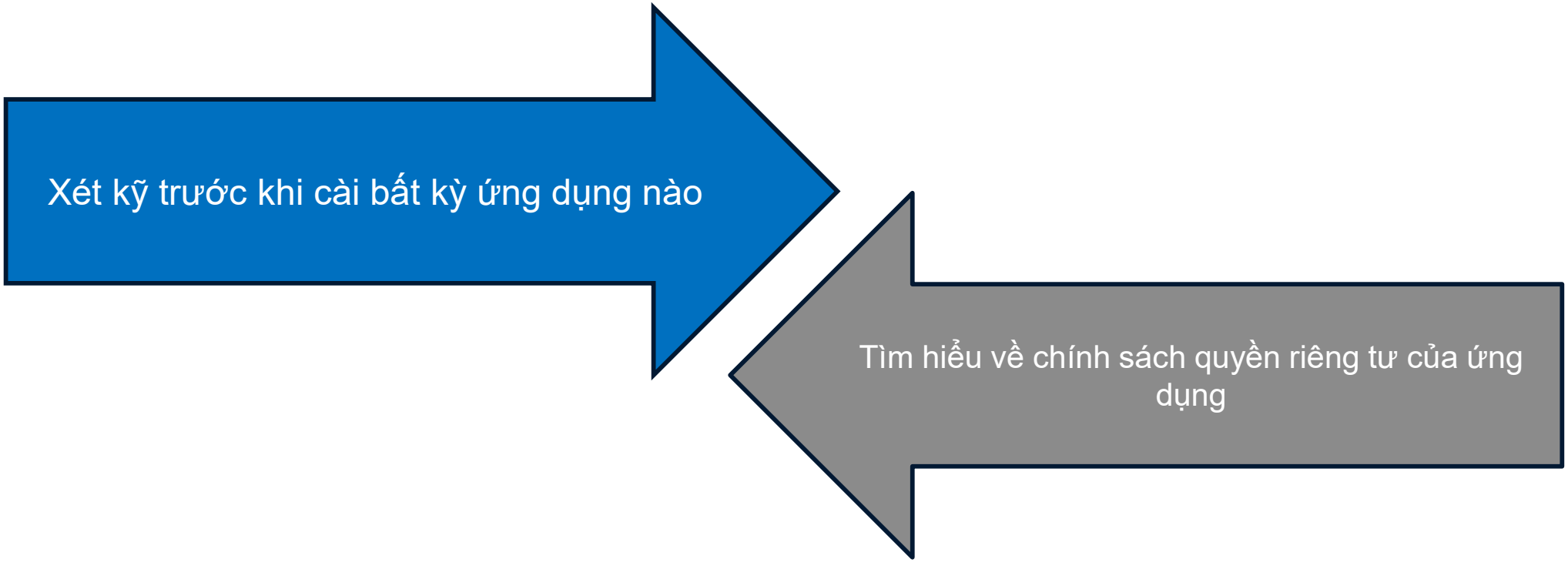
Sử dụng mạng xã hội an toàn

Nhận biết tấn công lừa đảo sử dụng AI và Deepfake

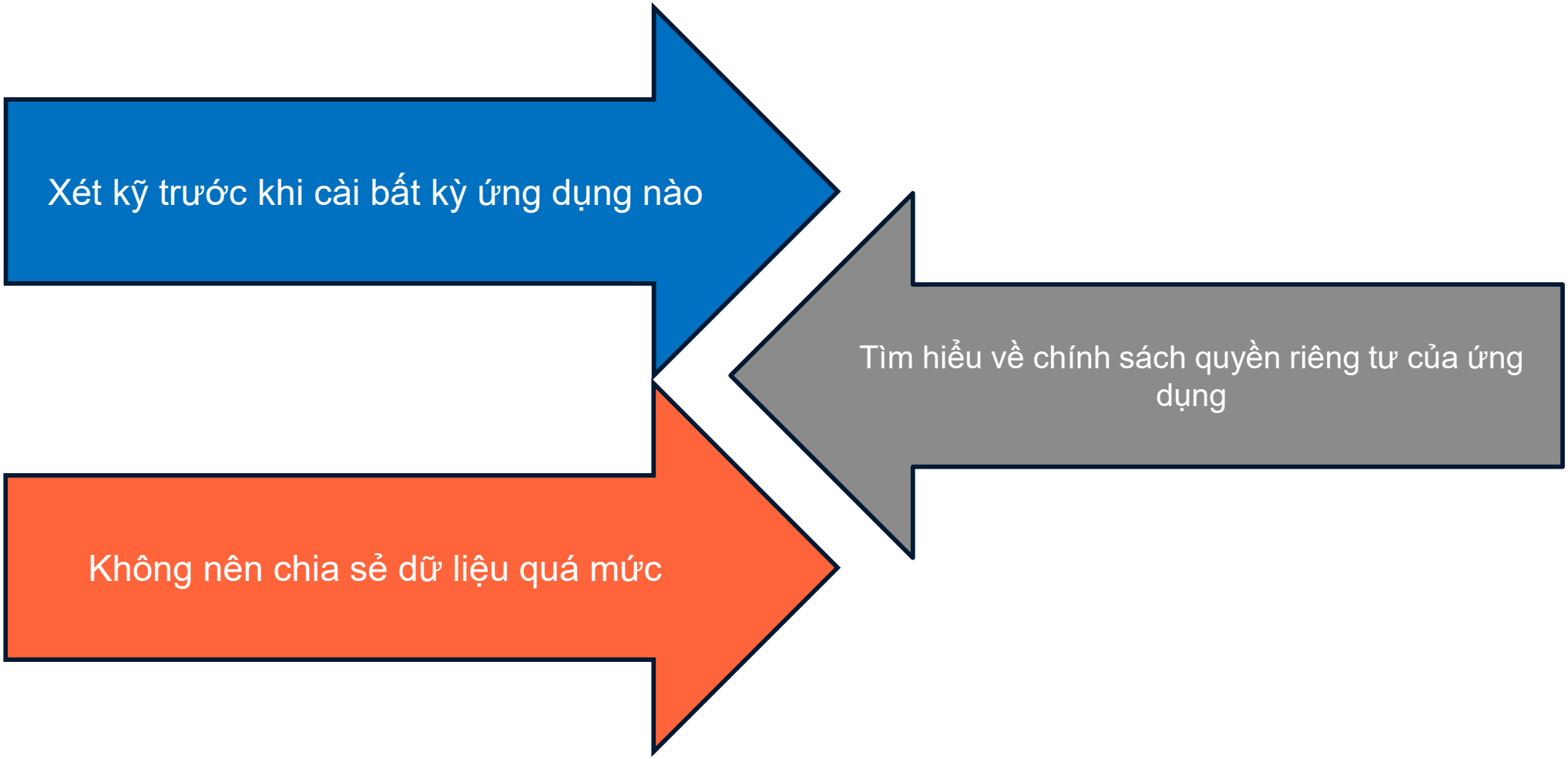
Nguyên tắc ngăn ngừa rò rỉ thông tin cá nhân



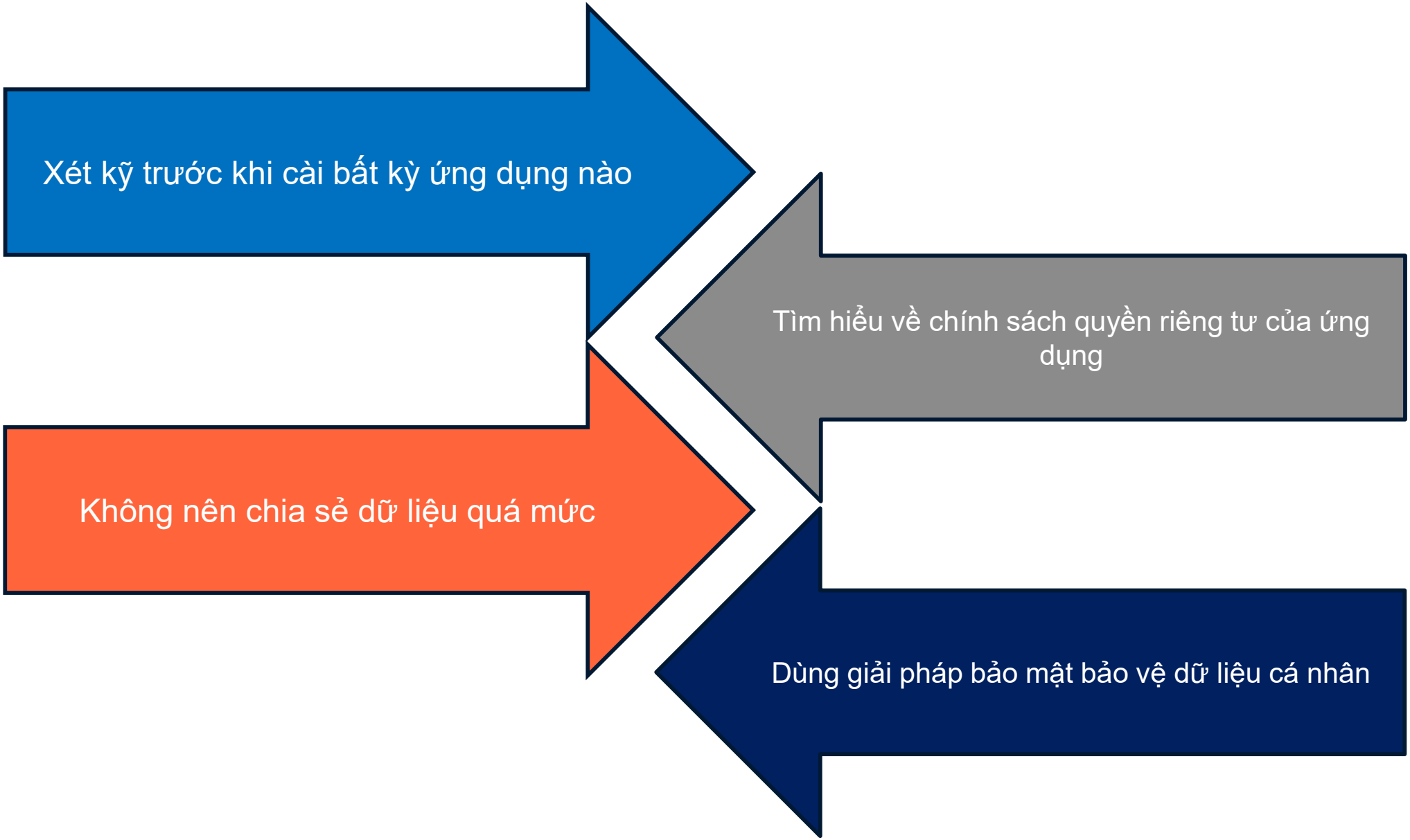
Nguyên tắc ngăn ngừa rò rỉ thông tin cá nhân



Nguyên tắc ngăn ngừa rò rỉ thông tin cá nhân



Nguyên tắc ngăn ngừa rò rỉ thông tin cá nhân



Sử dụng mạng xã hội an toàn

1. Bảo mật tài khoản:
 - Sử dụng mật khẩu mạnh.
 - Kích hoạt xác thực hai yếu tố (2FA).

2. Quản lý thông tin cá nhân:
 - Hạn chế chia sẻ thông tin cá nhân.
 - Kiểm tra cài đặt quyền riêng tư.

3. Cảnh giác với các liên kết và ứng dụng:
 - Tránh nhấp vào các liên kết không rõ nguồn gốc.
 - Kiểm tra cài đặt quyền riêng tư.

4. Hành vi trên mạng:
 - Không kết bạn với người lạ.
 - Hành xử lịch sự và tôn trọng:

Sử dụng mạng xã hội an toàn

5. Báo cáo và chặn:
 - Báo cáo hành vi xấu.
 - Chặn người dùng gây phiền toái.

6. Cập nhật thường xuyên:
 - Cập nhật phần mềm và ứng dụng.

7. Thận trọng với thông tin giả mạo:
 - Kiểm tra nguồn tin.
 - Không lan truyền tin đồn

Deepfake ngày càng giống thực và tự nhiên

Video deepfake

Tấn công lừa đảo sử dụng AI và Deepfake

Lừa đảo Deepfake là gì?

- Deepfake là công nghệ mô phỏng hình ảnh khuôn mặt con người, được đặt tên
theo cụm từ được kết hợp giữa "deep learning" (máy học) và "fake" (giả).

- Được dùng để nhằm phục vụ mục đích tốt, nhưng một số thành phần lại sử dụng cho mục đích lừa đảo, giả mạo, bôi nhọ hay thậm chí là làm ra tin giả kiểu video.

Tấn công lừa đảo sử dụng AI và Deepfake

Sự nguy hiểm của Deepfake

- Clip Deepfake lừa đảo sẽ gây ra những hệ lụy, bất tiện cho người dùng mỗi khi nhận được các cuộc gọi kiểu như thế này sẽ phải xác minh lại.

- Nguy hiểm hơn, trước các vụ lừa đảo Deepfake, việc người dùng chứng minh với ngân hàng mình bị lừa là rất phức tạp, mất thời gian và phải có sự tham gia của nhiều bên như nhà mạng hoặc công an.

Tấn công lừa đảo sử dụng AI và Deepfake

Sự nguy hiểm của Deepfake

Đối tượng bị nhắm đến:

- Những người trung niên vì họ thiếu kiến thức về an toàn thông tin.

- Người lâu nay rất khó bị lừa, người cẩn thận nhưng giờ cũng có thể sẽ là đối tượng bị lừa.

Tấn công lừa đảo sử dụng AI và Deepfake

Cách phát hiện và phòng chống Deepfake

- Một số dấu hiệu kỳ lạ:
 + Khuôn mặt thiếu tính cảm xúc và khá "trơ" khi nói, tư thế lúng túng, không tự nhiên...
 + Âm thanh không đồng nhất với hình ảnh, có nhiều tiếng ồn bị lạc vào clip hoặc clip không có âm thanh.
 + Tài khoản chuyển tiền không phải của người đang thực hiện cuộc gọi.

Tấn công lừa đảo sử dụng AI và Deepfake

Cách phát hiện và phòng chống Deepfake

- Phòng chống:
 + không tin tưởng các thông tin yêu cầu (cài phần mềm, đăng nhập vào website, cung cấp thông tin, chuyển tiền...) trên mạng mà cần phải xác minh lại.
 + Không nên truy cập vào các địa chỉ website lạ, không cài đặt các phần mềm lạ không rõ nguồn gốc, những phần mềm đòi hỏi yêu cầu cấp quyền truy cập cao vào thông tin người dùng, truy cập thẻ nhớ, danh bạ, vị trí, chụp ảnh,...

THANK YOU