PHƯƠNG THỨC TẤN CÔNG VÀ BIỆN PHÁP PHÒNG CHỐNG

- Các phương thức tấn công
- Biện pháp phòng chống tấn công

2.1. Phương thức tấn công (1)

Khái quát các phương thức, kỹ thuật tấn công của tin tặc đối với các thiết bị đầu cuối

- Tấn công xâm nhập, chiếm quyền điều khiển (thiết bị)
- Tấn công giả mạo (Social Engineering, Phishing)
- Tấn công từ chối dịch vụ (lạm các thiết bị IoT, ví dụ Camera đã từng xảy ra. Các loại thiết bị khác cũng có thể bị khác thác theo cách tương tự)
- Tấn công phá hoại dữ liệu, hệ thống
- Đánh cắp dữ liệu, nghe trộm trên đường truyền
- Tấn công thay đổi giao diện
- Tấn công sử dụng mã độc
- …

2.1. Phương thức tấn công (cont')

❖ Social Engineering (SE):

- Là phương thức tấn công phi kỹ thuật, lợi dụng sự thiếu hiểu biết của người dung hoặc các đối tượng khác liên quan đến bảo vệ hệ thống, để đột nhập vào hệ thống, đánh cắp thông tin mật, phá hủy hay làm hỏng hệ thống một cách trái phép.
- Có hai loại tấn công SE:
  - Human-Based: nghe trộm, nhìn trộm, gọi điện …
  - Mobile/Computer-Based: Phishing, Pop-up, Spam mail …

❖ Nguyên nhân dẫn đến tấn công Social Enginering?

- Các quy định/chính sách được thiết lập lỏng lẻo hoặc tuân thủ chưa tốt
- Do hacker ít hoặc không sử dụng công cụ để tấn công, nên rất khó giám sát, phát hiện bằng các công cụ tự động
- Không có phương thức tối ưu nào để chống lại
- Không có phần mềm hay phần cứng bảo vệ hiệu quả

2.1. Phương thức tấn công (cont')

- **Các giai đoạn tấn công Social Engineering**
  - Nghiên cứu, tìm hiểu mục tiêu (cơ quan/tổ chức)
  - Lựa chọn nạn nhân trong cq/tc
  - Phát triển, tạo dựng mối quan hệ
  - Khai thác mục tiêu
- **Phương thức tấn SE phổ biến – tấn công mạo danh (impersonation)**
  - Phương tiện: điện thoại, email, các trang mạng xã hội…=> thu thập các thông tin nhạy cảm
  - Giả danh lãnh đạo của cơ quan, tổ chức
  - Giả danh cán bộ kỹ thuật
  - Giả danh người dùng

2.1. Phương thức tấn công (cont')

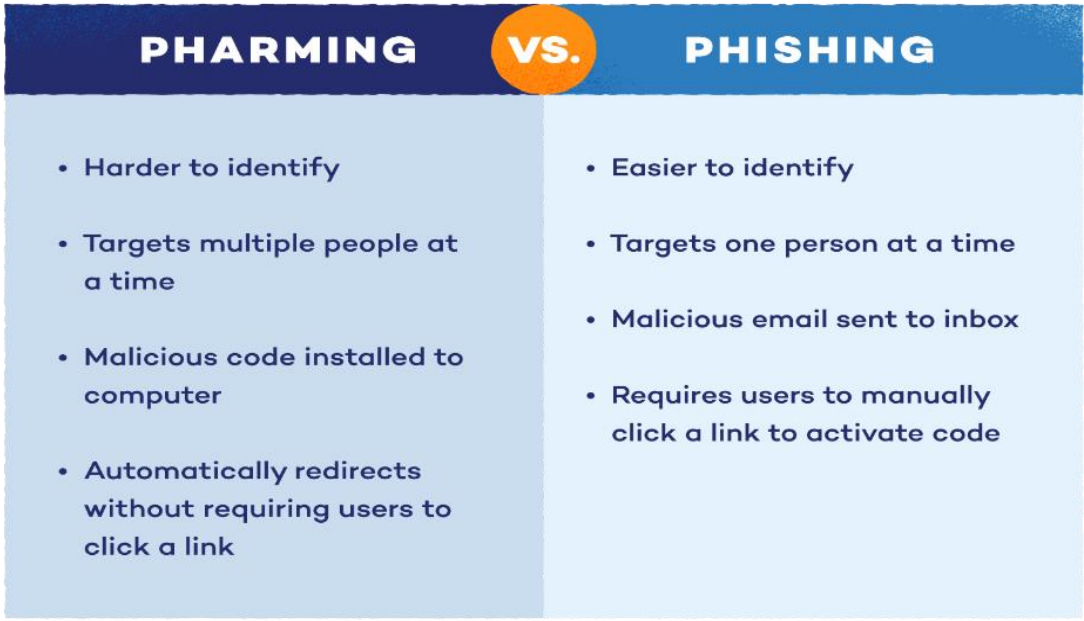
Phishing: là hình thức tấn công lợi dụng sự thiếu hiểu biết của người sử dụng (người dùng), khiến họ tương tác với các bẫy nguy hiểm của hacker.

Ví dụ:

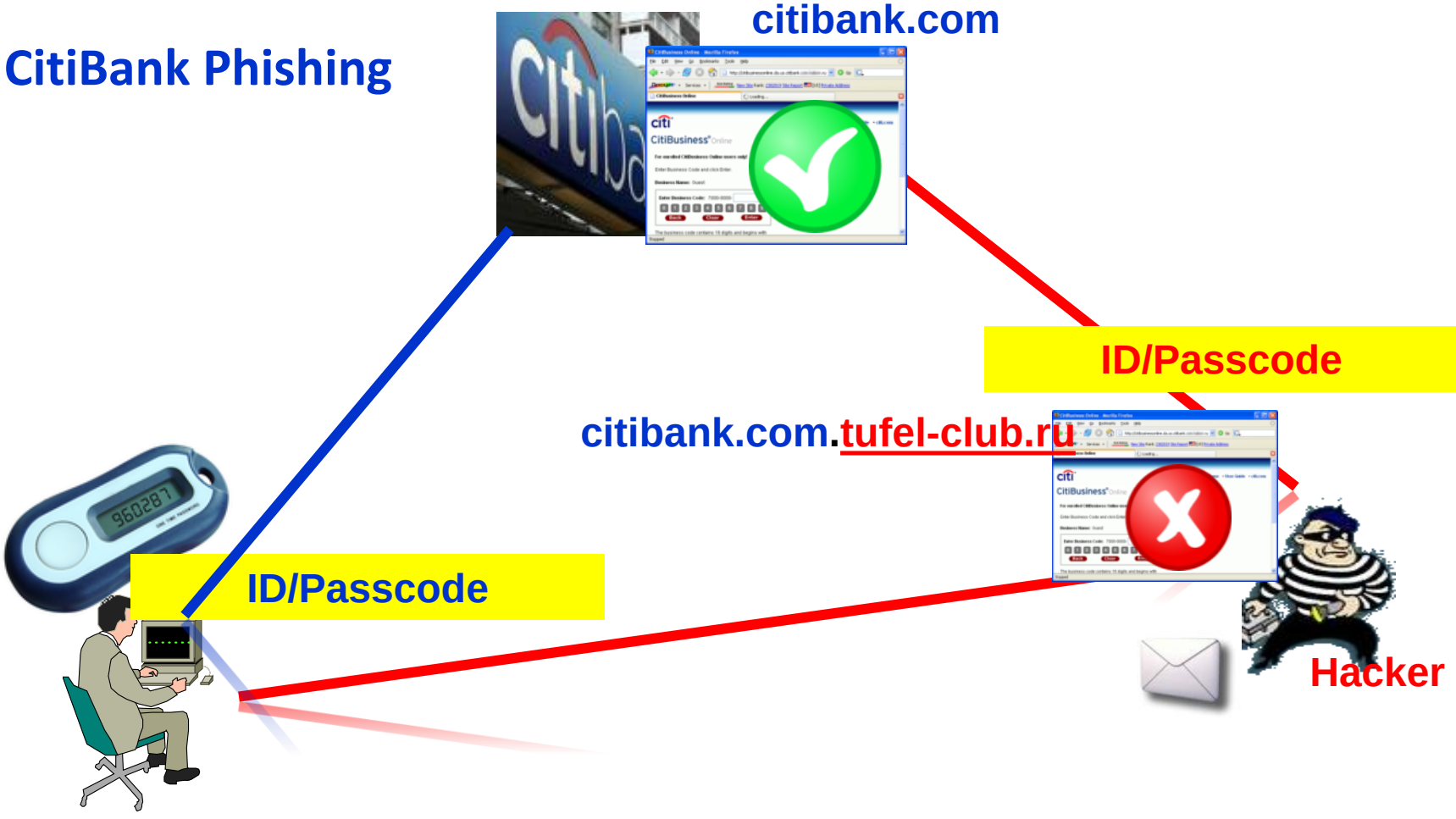
- Email có nội dung lừa đảo kèm theo theo file hoặc link độc hại
- Website giả mạo thu thập thông tin cá nhân …
- Đặc điểm Phishing
  - Dễ phát hiện
  - Nhắm 1 một mục tiêu tại 1 thời điểm
  - Email độc hại được gửi trong inbox
  - Yêu cầu người dung click vào đường link

❖ Pharming attack:

- Khó bị phát hiện
- Nhắm nhiều mục tiêu người dung cùng một thời điểm
- Cài mã độc vào máy tính
- Tự động chuyển hướng mà không yêu cầu người click vào link



2.1. Phương thức tấn công (cont')



2.1. Phương thức tấn công (cont')

2- Tải mã độc về máy đồng thời thực thi

3- Mã độc kết nối đến máy chủ điều khiển

4- Hacker điều khiển từ xa

1- Gửi email lừa đảo kèm link

2.1. Phương thức tấn công (cont')

Spear Phishing

Nhắm đến mục tiêu cụ thể trong tổ chức (một người hoặc nhóm người)

Whaling

Nhắm vào những người có chức vụ cao trong tổ chức (những người nắm giữ nhiều thông tin quan trọng)

Spam email (Junk email)

Là loại thư (thư rác) mà người nhận không mong muốn, không được yêu cầu, cảm thấy phiền hà.
Hacker có thể Spam email để gửi cho cho nhiều người với mục đích thu thập thông tin của người dùng, phát tán mã độc

2.1. Phương thức tấn công (cont')

Tấn công APT

APT = Advanced + Persistent + Threat

Advanced:

- Là kỹ thuật tấn công tiên tiến, có tính tàng hình rất cao (nhằm tránh sự phát hiện). Attacker thường sử dụng ít công cụ nhất để triển khai tấn công mục tiêu. Nghĩa là, hacker sẽ sử dụng tổng hợp các kỹ thuật (technical & nontechnical) tạo thành chiến dịch có quy mô và có chiến lược rõ ràng.

Persistent :

- **M**ối đe doạ, hay kẻ tấn công ẩn trú trong mạng mục tiệu trong một thời gian dài, có khi kéo dài trong nhiều năm => mang tính dai dẳng

Threat:

- Phải là attacker giỏi. Do đó cần có nguồn lực lớn nhằm tạo ra các công cụ đặc chủng để hoạt động dai dẳng;
- Attacker có thể bao gồm cả các chuyên gia thuộc Chính phủ.

Lừa đảo tiền gửi ngân hàng

- Giả danh nhân viên ngân hàng để liên hệ với khách hàng:
  - Gọi điện thu thập số tài khoản, tên tài khoản, mật khẩu…
  - Gửi email giả mạo thu thập thông tin về tài khoản, tên tài khoản, mật khẩu, mã OTP

Chiếm dụng tài khoản mạng xã hội

- Hacker chiếm đoạt tài khoản mạng xã hội (facebook) để lừa đảo, mạo danh người quen để vay tiền, xin tiền…
- Chiếm tài khoản mạng xã hội yêu cầu nộp tiền chuộc

Chiếm dụng tài khoản mạng xã hội

Trong thời gian từ tháng 10-2020 đến nay, 5 nghi phạm đã gây ra hơn 40 vụ hack Facebook, chiếm đoạt trên 2 tỉ đồng của khoảng 20 bị hại tại nhiều tỉnh thành trên cả nước
https://tuoitre.vn/nhom-thanh-nien-hack-hon-40-tai-khoan-facebook-chiem-doat-hon-2-ti-dong-20210902223152706.htm

B1: chiếm quyền điều khiển của tài khoản fb, đổi mật khẩu, tìm hiểu hoạt động (lịch sử nói chuyện) để có thông tin tạo niềm tin
B2: Mua số tài khoản NH trùng tên trên fb
B3: sử dụng đoạn video ghi hình khuôn mặt chủ tài khoản đã cung cấp từ trước (nếu nạn nhân yêu cầu kiểm tra)

2.2. Biện pháp phòng chống tấn công mạng

- Biện pháp về con người, nguồn nhân lực
- Quy trình, chính sách
- Công nghệ

2.2. Biện pháp phòng chống tấn công mạng

❖ Biện pháp về con người, nguồn nhân lực

- Thành lập các bộ phận kiêm nhiệm, bán chuyên trách, chuyên trách về ATTT
- Bố trí nhân lực phụ trách các công việc, vị trí phù hợp
- Thường xuyên đạo tạo, tập huấn cho đội ngũ làm về an toàn thông tin
- Triển khai các chương trình đào tạo, các hoạt động nâng cao nhận thức về an toàn thông tin đối với người dùng
- Thu hút và đãi ngộ đối với cán bộ làm về ATTT

2.2. Biện pháp phòng chống tấn công mạng

❖ Quy trình, chính sách (quy định)

- Xây dựng chính các chính sách áp dụng cho hoạt động đảm bảo ATTT, ví du: chính sách đối với người dùng, với việc cấu hình an toàn thiết bị mạng, thiết bị an toàn mạng, …
- Xây dựng các quy trình: quy trình ứng cứu sự cố an toàn thông tin, quy trình quản lý, vận hành hệ thống thông tin…

2.2. Biện pháp phòng chống tấn công mạng

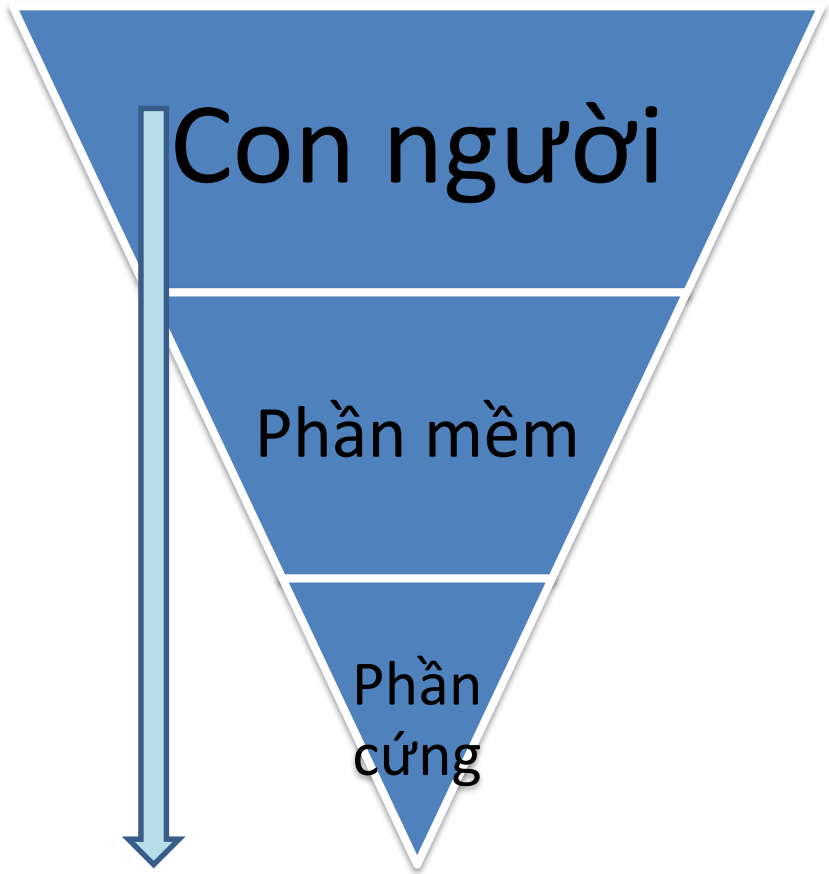
❖ Công nghệ

- Trang bị hạ tầng thiết bị an toàn mạng: tường lửa, hệ thống giám sát …
- Triển khai hệ thống anti-virus
- Triển khai hệ thống chống tấn công DDoS
- Nâng cấp và cập nhật bản vá cho HĐH, các ứng dụng

2.2. Biện pháp phòng chống tấn công mạng

Xu hướng đầu tư cho ATTT (thế giới)

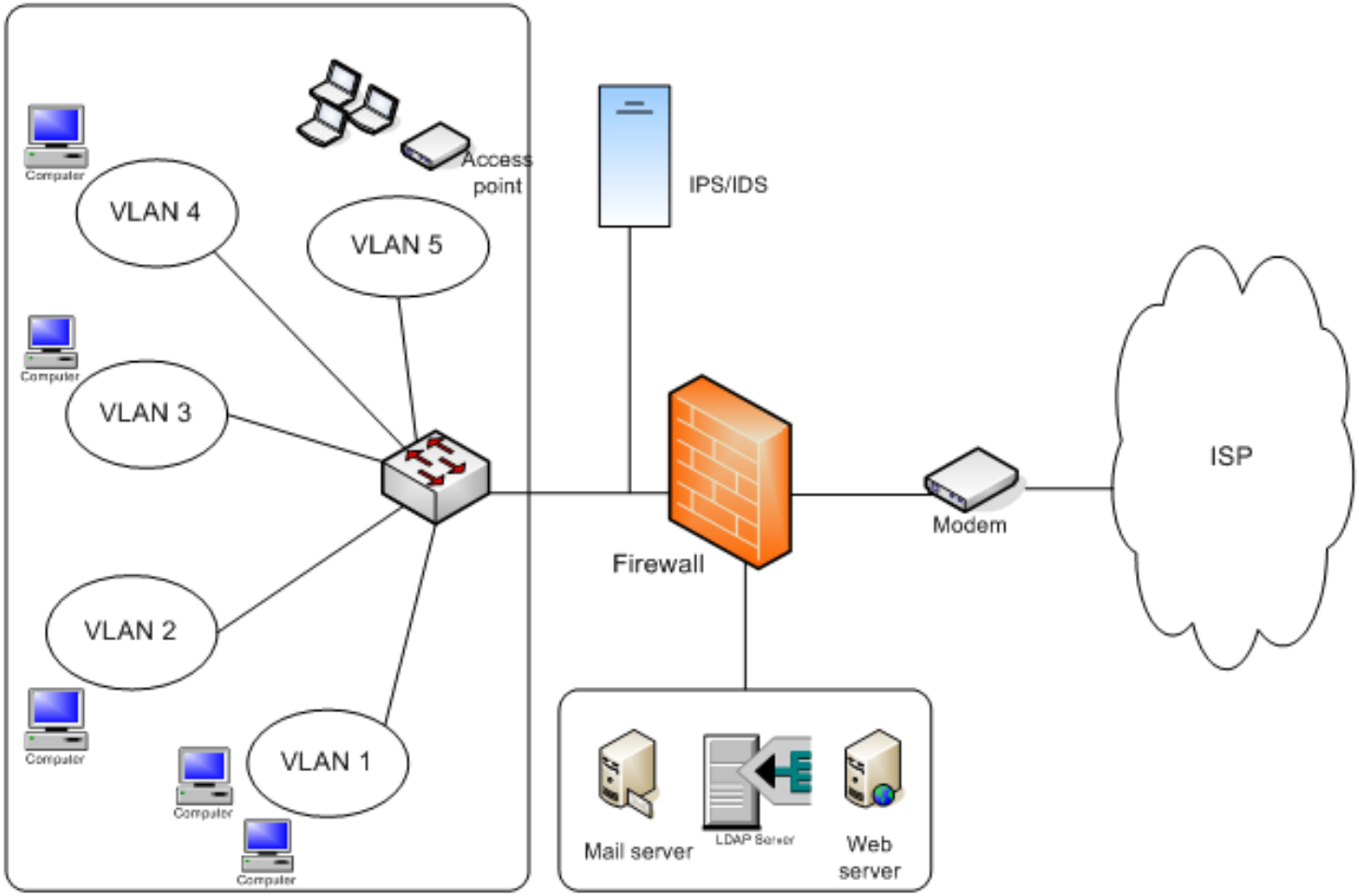
Xu hướng trước đây



Xu hướng hiện tại

2.2. Biện pháp phòng chống tấn công mạng

❖ Mô hình mạng an toàn



2.2. Biện pháp phòng chống tấn công – Các nguyên tắc bảo vệ dữ liệu

❖ 03 tác động của các cuộc tấn công mạng:

- Thứ 1: phá hủy, làm hỏng hoặc thay đổi dữ liệu
- Thứ 2: Làm lộ lọt những dữ liệu bí mật
- Thứ 3: Mất khả năng cung cấp dịch vụ khi người dùng cần truy xuất dữ liệu

❖ Nguyên tắc bảo vệ dữ liệu:

Trước hết dữ liệu cần được phân loại dựa trên các tiêu chí sau:

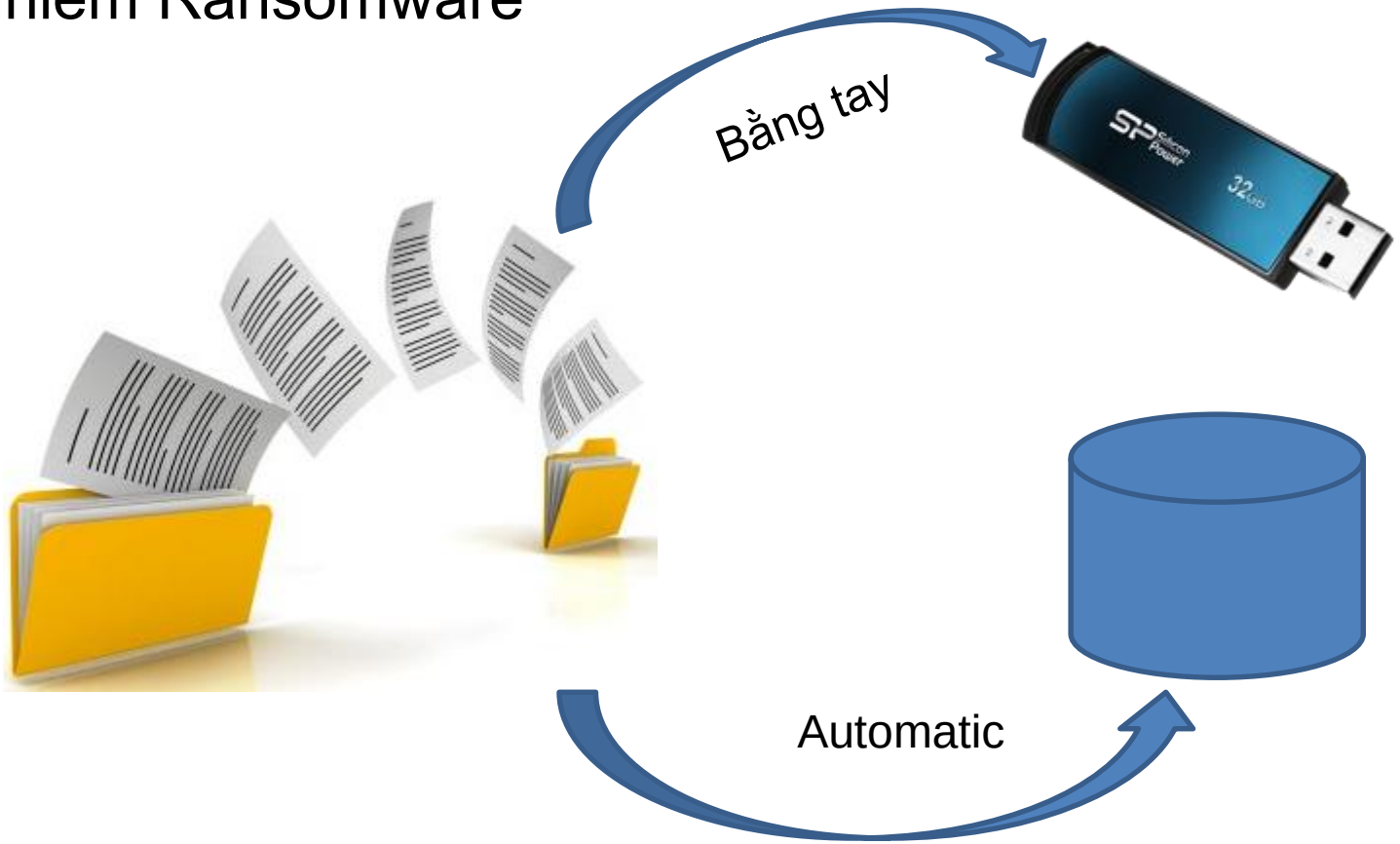
- Dữ liệu cần đảm bảo tính toàn vẹn
- Dữ liệu cần đảm bảo bảo tính bí mật
- Dữ liệu cần đảm bảo tính sẵn sàng

2.2. Biện pháp phòng chống tấn công – Các nguyên tắc bảo vệ dữ liệu

- Sau khi phân loại, tiến hành đánh giá rủi ro để trển khai các biện pháp bảo vệ phù hợp, như
  - Áp dụng giải pháp mã hóa dữ liệu đối với những dữ liệu mật
  - Định kỳ sao lưu dữ liệu ở những nơi an toàn để tránh các loại tấn công pháp hủy, mã hóa đòi tiền chuộc …
  - Đối với hệ thống cung cấp dịch vụ cần triển khai các giải pháp cân bằng tải, phát hiện và ngăn chặn tấn công …
  - Xây dựng quy trình, quy định và nâng cao nhận thức của người dùng để có thể tự bảo vệ được tài sản thông tin của mình trong nhiều tình huống.

SAO LƯU DỮ LIỆU (1)

- Phòng khi
  - Mất, xoá DL
  - Bị nhiễm Ransomware



MÃ HOÁ DỮ LIỆU (1) ?

Mã hoá những dữ liệu quan trọng phòng khi bị mất, đánh cắp hoặc copy dữ liệu trên thiết bị lưu trữ

TrueCrypt tool

Tools:
- BitLoker (sẵn có trên windows)
- Winrar – đặt mật khẩu cho file
- TrueCrypt (miễn phí, không còn an toàn)

Bảo vệ thiết bị di động (Mobile, Ipad, Iphone, tablet…)

1- Hạn chế tối đa sử dụng wifi công cộng (public Wi-Fi)

⇒Mất thông tin cá nhân:

- Thông tin tài khoản email
- Ngân hàng,
- Mạng xã hội…

Nếu buộc phải dùng thì nên sử dụng phần mềm: **Avira Phantom VPN**

https://www.avira.com/en/avira-phantom-vpn#start-download-vpn

Hặc: **CyberGhost, TunnelBear**

2- Nên sử dụng mạng 3G/4G trên smartphone

Bảo vệ thiết bị di động (Mobile, Ipad, Iphone, tablet…)

3- Không nên sử dụng Bluetooth nơi công cộng hoặc sử dụng xong cần tắt (disable)

4- Không nên tải sử dụng các phần mềm (app) không rõ nguồn gốc, vì có thể bị lây nhiễm mã độc trên máy

5- Hạn chế sử dụng các apps trên Google Play Store (GPS). GPS thường xuyên rà soát và loại bỏ, nhưng không đảm bảo đã sạch

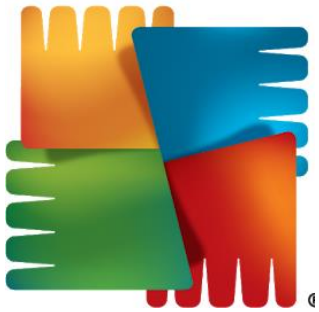
Cài đặt Anti-vius trên thiết bị di động (Mobile, Ipad, Iphone, tablet…)

Avast Antivirus 2018

Norton Mobile Security

Kaspersky Mobile Antivirus

McAfee Mobile Security & Lock



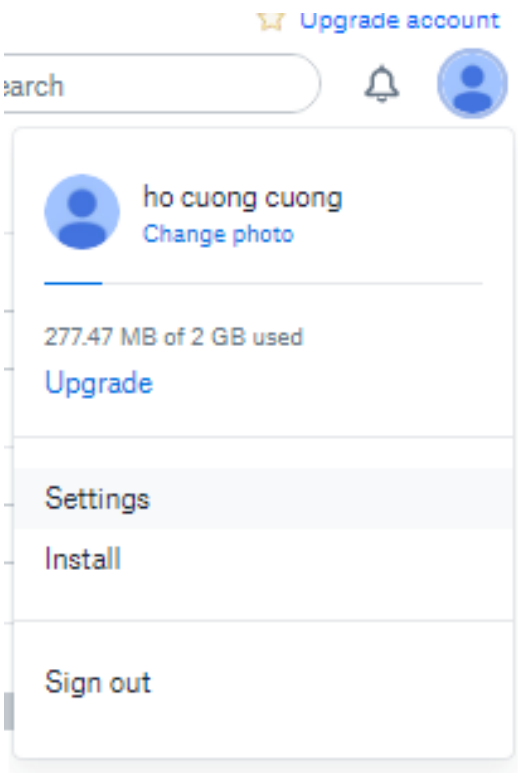
AVG AntiVirus 2018 for Android Security

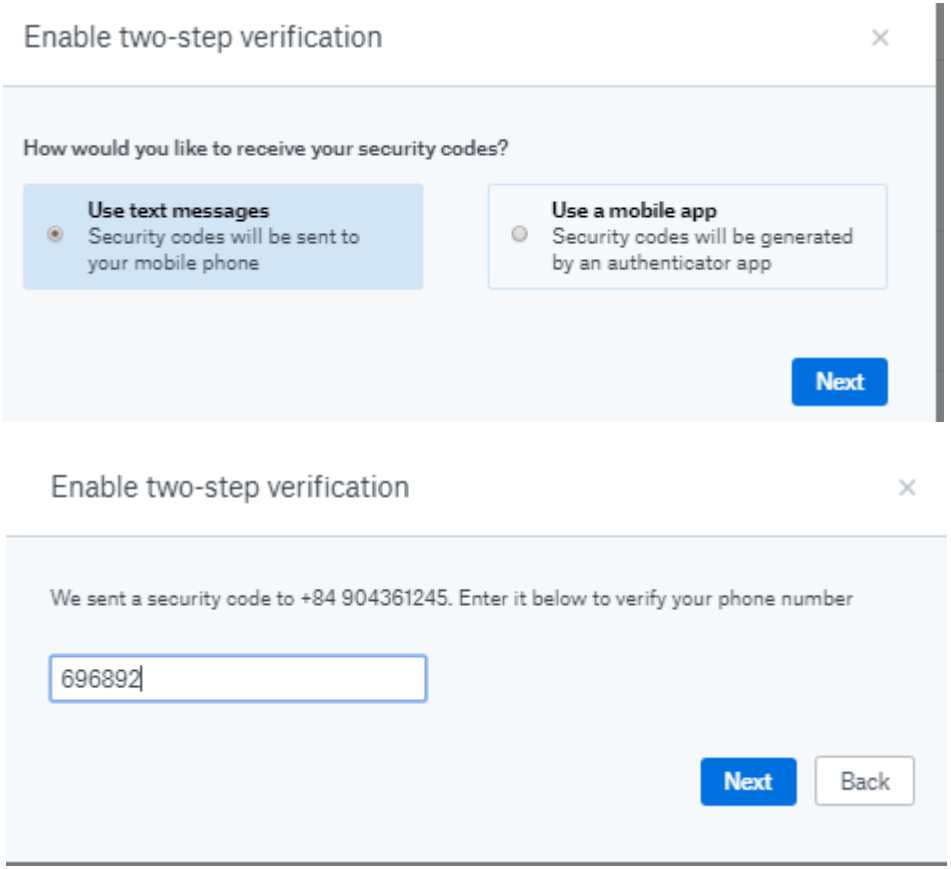
An toàn dữ liệu người dùng cá nhân trên đám mây

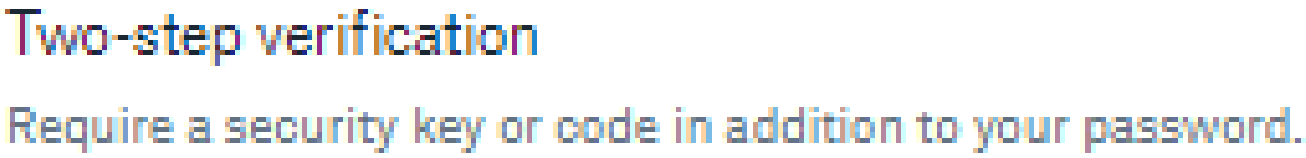
Chia sẻ lưu trữ đám mây, đồng bộ dữ liệu người dùng.

Google Drive

Bảo mật cho Dropbox (tương tự các dịch vụ khác)







Phòng chống mã độc trên PC, Laptop

Trojan Horse	Virus
Backdoor	Worms
Rootkit	Spyware
Ransomware	Botnet
Adware	Crypter

Các phần mềm anti-virus phổ biến, Cách phòng chống mã độc bằng Trend

Bkav Bản quyền
Giá từ 220.000đ/máy

Kaspersky Antivirus
Giá từ 169.000đ/máy

Norton Antivirus
Giá từ 139.000đ/máy

Avast Pro Antivirus
Giá từ 279.000đ/máy

Trend Micro Internet
Giá từ 149.000đ/máy

Bitdefender Antivirus
Giá từ 159.000đ/máy

Intel McAfee Antivirus
Giá từ 169.000đ/máy

Eset Nod32 Antivirus
Giá từ 119.000đ/máy

Avira Antivirus
Giá từ 279.000đ/máy

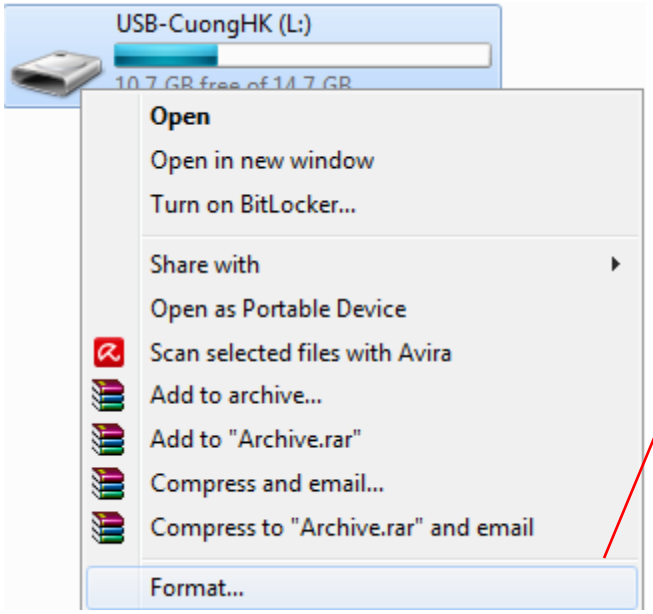
Cấu hình, sử dụng USB an toàn

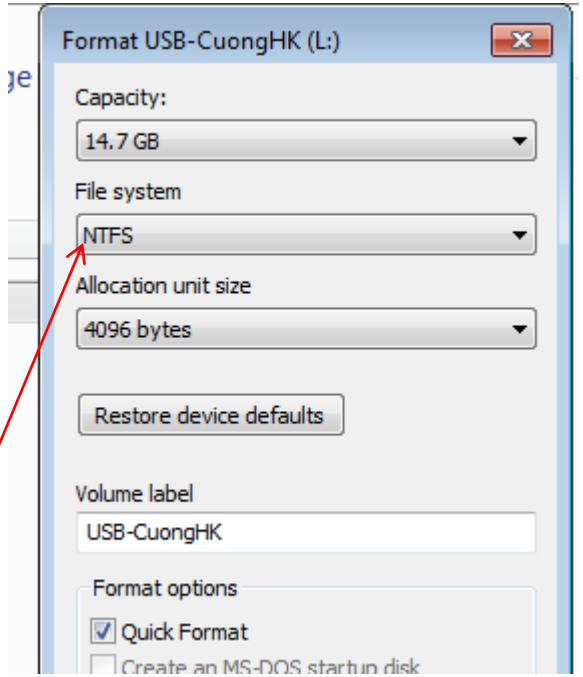
- Phòng chống lây nhiễm mã độc từ một máy tính đang bị nhiễm sang USB khi tương tác.
- Ngăn chặn (giảm thiểu) mã độc đang nằm trong USB lây sang máy tính => Không cho mã độc khởi chạy

Cấu hình, sử dụng USB an toàn

❖ Cách làm

- Bước 1:
  - Format ổ đĩa
  - Chuột phải chọn Format

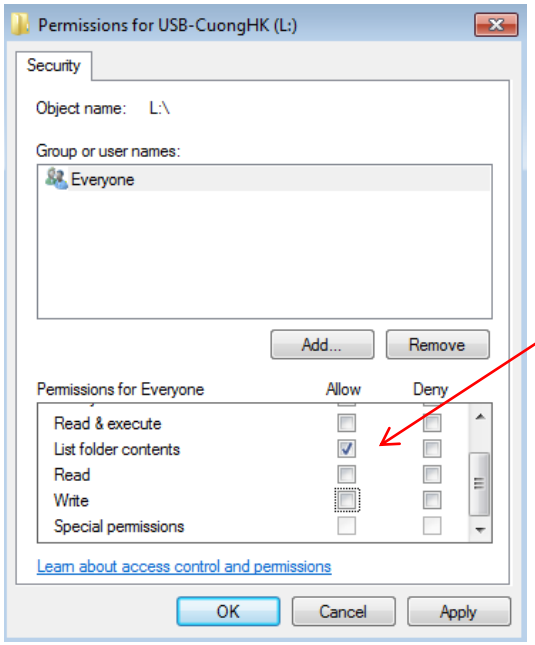


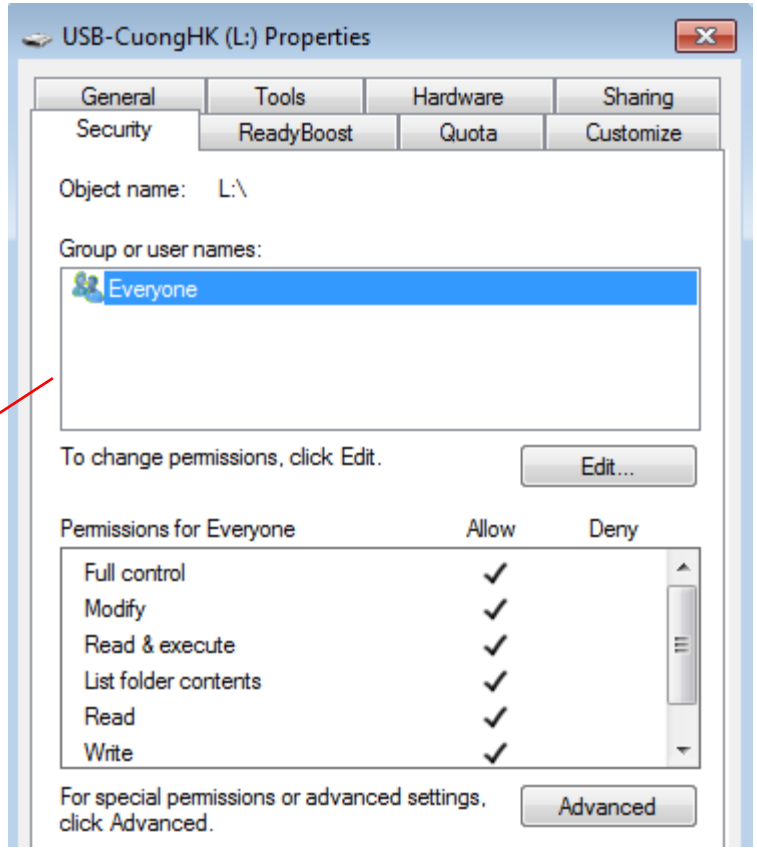


Cấu hình, sử dụng USB an toàn

- Bước 2: Tạo thư mục có tên DATA
- Bước 3: Quay trở lại thư mục gốc, chuột phải
- Bước 4: Thay đổi thuộc tính

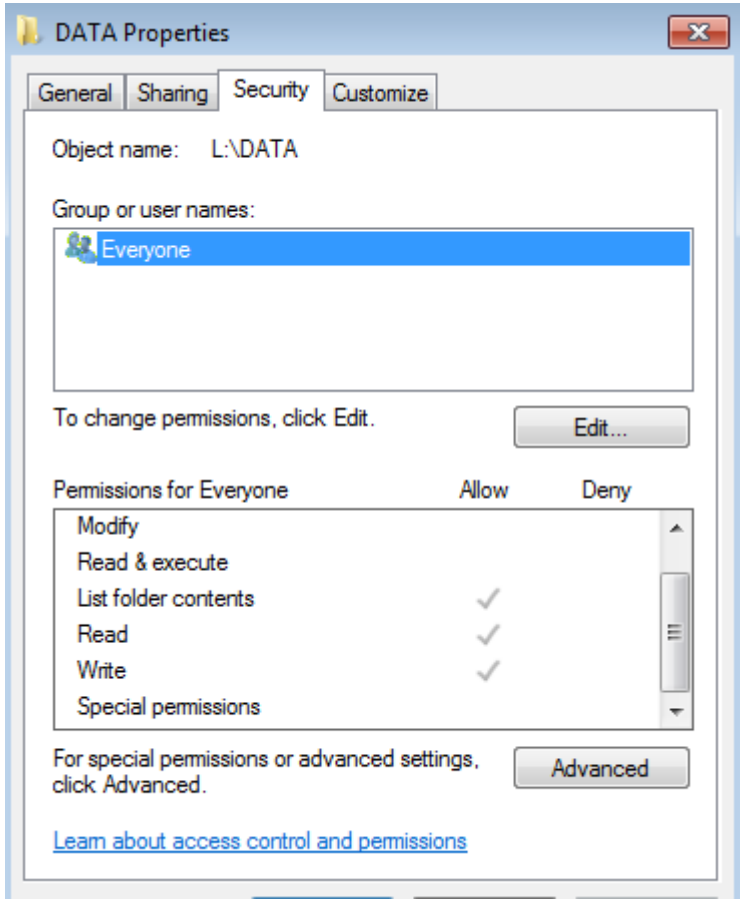
Chọn List folder Contents





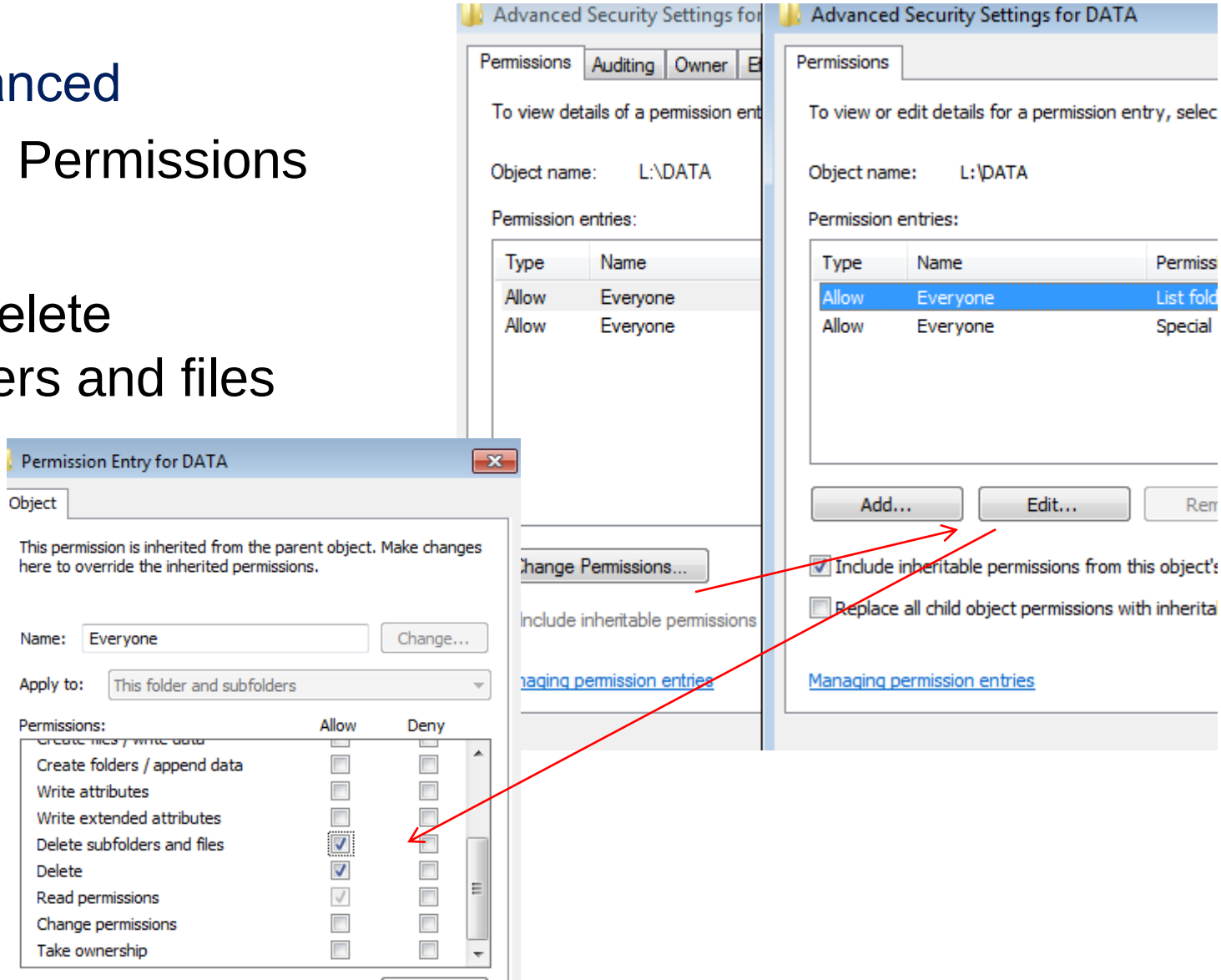
Cấu hình, sử dụng USB an toàn

- Chuột phải vào thư mục D
- Chọn Security
- Chọn
  - List folder contents
  - Read
  - Write



Cấu hình, sử dụng USB an toàn

- Chọn Advanced
  - Change Permissions
  - Edit
  - Chọn Delete subfolders and files
  - Delete



Sử dụng mạng xã hội (facebook) an toàn

3- 10 khuyến nghị khi tham gia mạng xã hội

(1) Yêu cầu đặt mật khẩu: mạnh, khó đoán, dễ nhớ (không ghi ra bất kỳ đâu), thường xuyên thay đổi, không chia sẻ

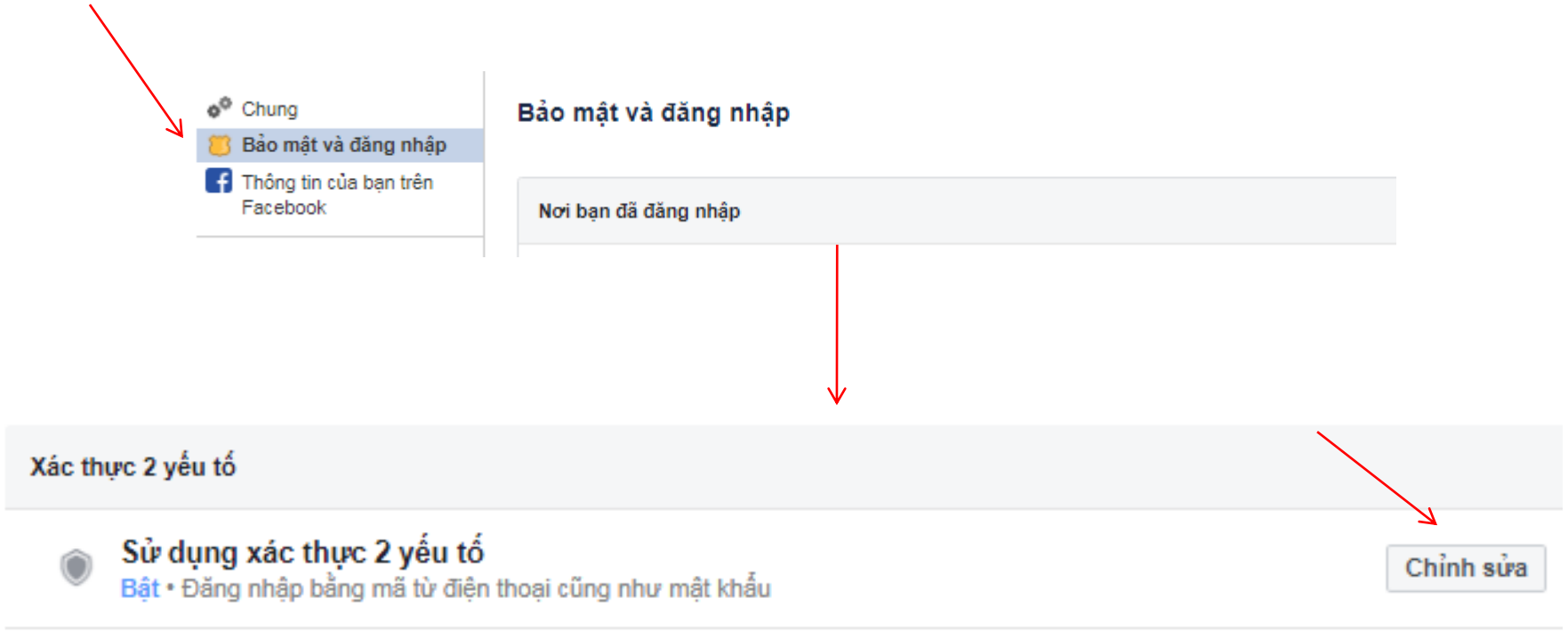
(2) Không nên chọn tính năng lưu mật khẩu trên trình duyệt cho đăng nhập lần sau (đặc biệt khi sử dụng trên máy tính người khác). Đăng xuất ngay sau khi sử dụng FB trên máy người khác (hoặc dùng chung máy tính)

(3) Hãy kiểm tra tên miền https://www.facebook.com/ trước khi tiến hành đăng nhập tài khoản

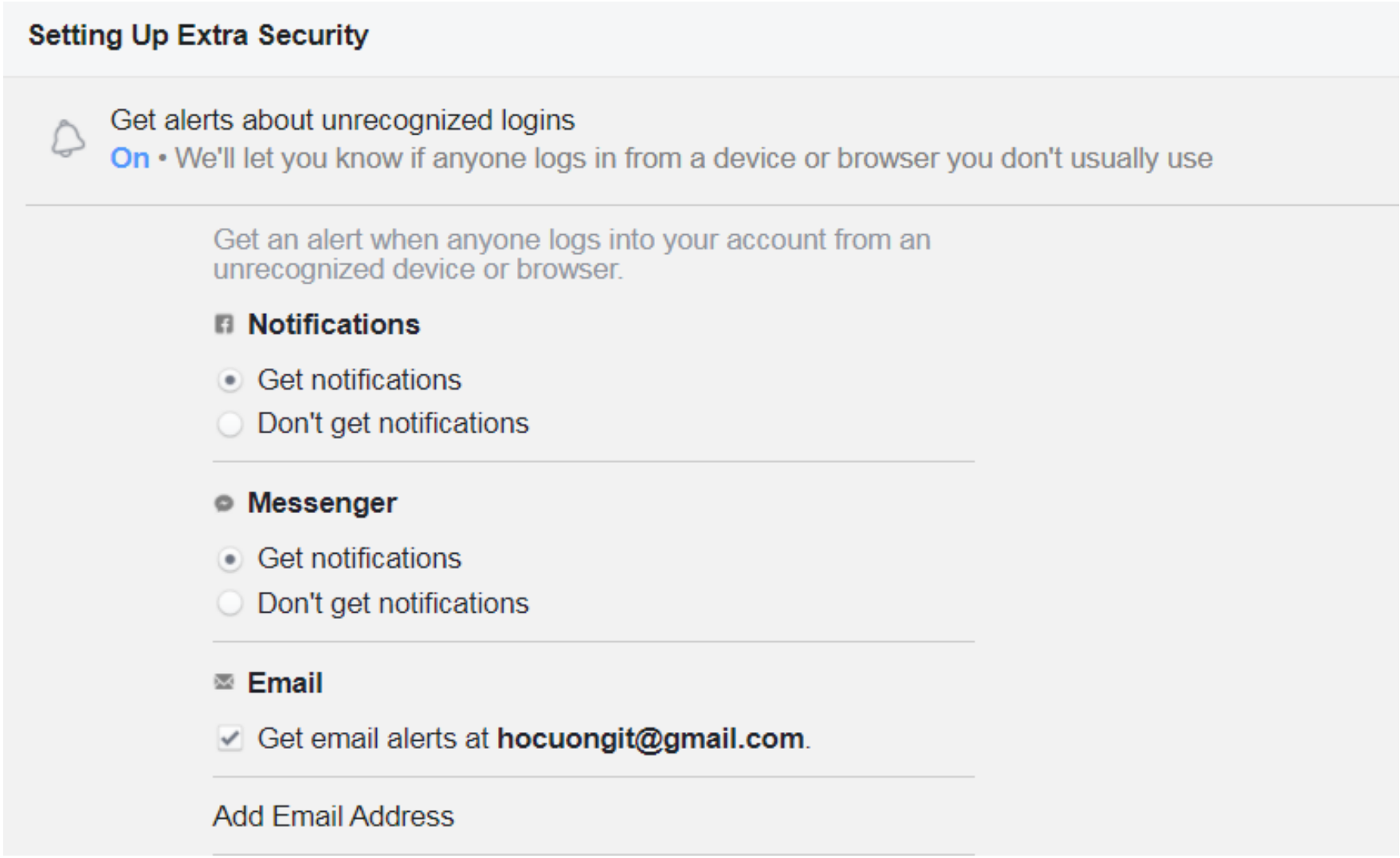
(4) Không trả lời các câu hỏi thăm dò

(5) Không kết bạn với những người chưa quen biết

Sử dụng mạng xã hội (facebook) an toàn



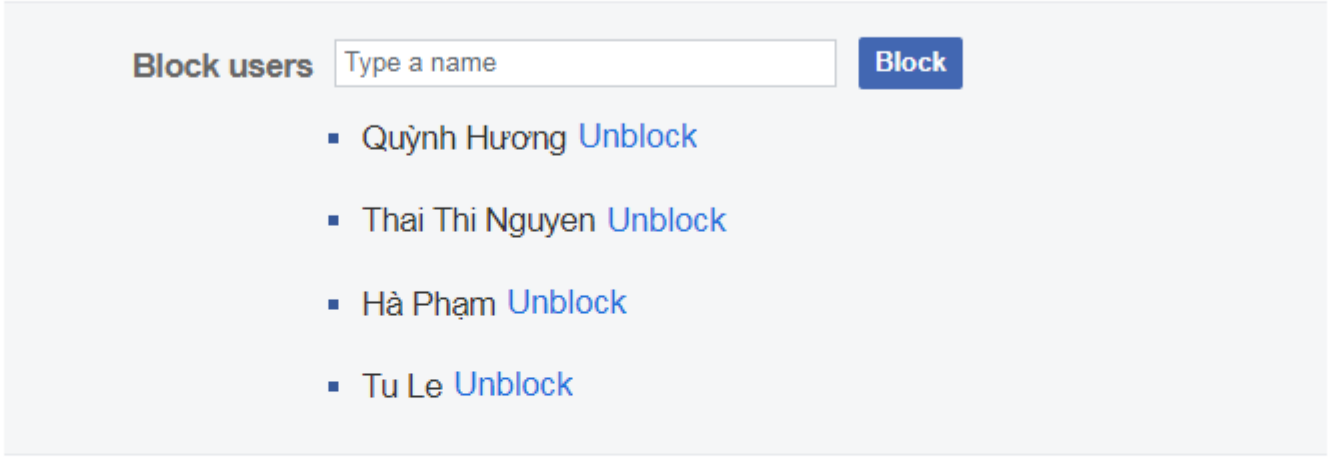
Sử dụng mạng xã hội (facebook) an toàn



Sử dụng mạng xã hội (facebook) an toàn

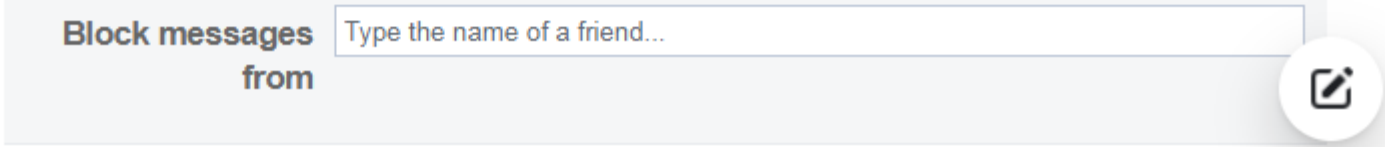
Block users

Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.



Block messages

If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app either. Unless you block someone's profile, they may be able to post on your timeline, tag you, and comment on your posts or comments. Learn more.



AN TOÀN KHI THANH TOÁN TRỰC TUYẾN

An toàn khi thanh toán trực tuyến (1)

1- Thanh toán trực tuyến là gì?

Thanh toán trực tuyến là dịch vụ giúp khách hàng thanh toán qua Internet khi mua hàng

2- Các hình thức thanh toán trực tuyến

(1) Thanh toán bằng thẻ

(2) Thanh toán qua cổng thanh toán (vd, F@st MobiPay)

(3) Thanh toán bằng ví điện tử (vd, Ví điện tử Mobivi – Ngân hàng BIV)

(4) Thanh toán bằng thiết bị di động thông minh (vd, liên kết theo mô hình Mobile Banking – Hệ thống bán hàng – Người tiêu dùng)

An toàn thanh toán trực tuyến (2)

(5) Thanh toán qua truyển khoản ngân hàng

3- 10 khuyến nghị đảm bảo an toàn khi thanh toán trực tuyến

(1) Hãy kiểm tra kỹ lưỡng xem người bán là ai?

Trường hợp mua sản phẩm từ người bán mà trước đây chưa từng thực hiện giao dịch thì hãy điều tra thông tin của họ. Nhìn thoáng qua có thể đó là trang web không độc hại nhưng thực tế trang web này có thể lại là trang web lừa đào (phishing). Để chuẩn bị trước cho trường hợp có vấn đề phát sinh khi giao dịch và thanh toán thì hãy ghi chú trước các thông tin như địa chỉ cửa tiệm, số điện thoại, địa chỉ thực tế.

An toàn thanh toán trực tuyến (3)

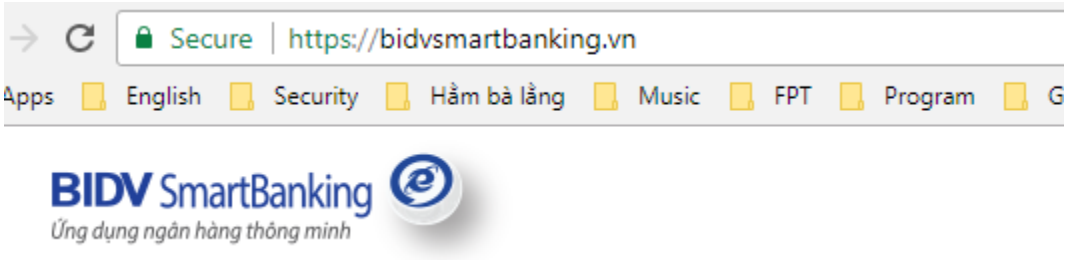
(3) Kiểm trang web có hợp pháp không?

Trước khi nhập thông tin cá nhân và thông tin tài khoản thanh toán khi thực hiện mua sắm trực tuyến, hãy kiểm tra xem trang web đó có an toàn hay không. Thông tin cần kiểm tra:

- Kiểm tra kỹ lưỡng tên miền

- Ẩn danh: Chrom Ctrl + Alt + N, Firefox Ctrl + Alt + P

- Kiểm tra khoá xanh (CA)



An toàn thanh toán trực tuyến (3)

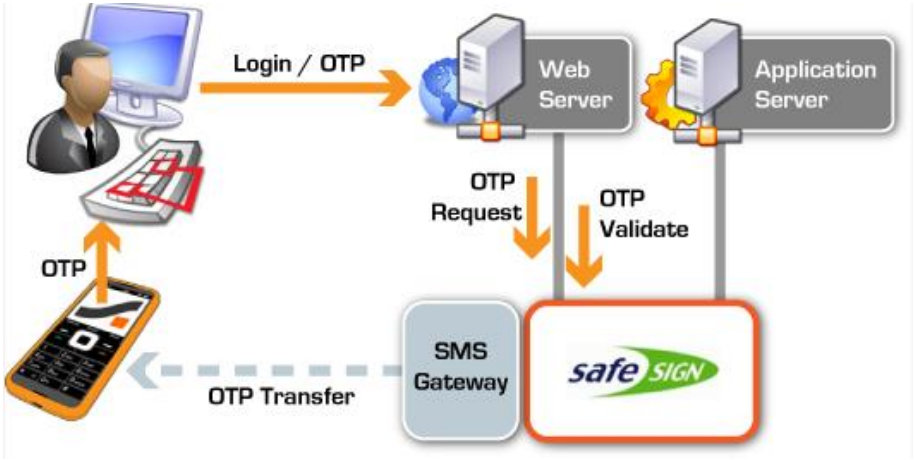
Không lưu thông tin đăng nhập trên trình duyệt => chọn **“Không bao giờ”**

Thoát ra khi không còn sử dụng

An toàn thanh toán trực tuyến (4)

(4) Khi sử dụng USB Token cho việc thanh toán

- Giữ gìn tránh đánh mất
- Không để lộ mã
- An toàn trước khi nhập mã



An toàn thanh toán trực tuyến (5)

(5) Cài đặt phần mềm Anti-virus để chống đánh cắp thông tin tài khoản, thông tin thẻ tín dụng

(6) Không nên sử dụng mạng wifi công cộng để giao dịch thanh toán, không dùng máy tính hay các thiết bị thông minh của người khác cho việc thanh toán

(7) Nên in và lưu lại màn hình xác nhận cuối cùng khi đặt hàng làm chứng từ hợp lệ, nếu phát sinh tranh chấp hoặc tra soát về sau

(8) Chủ thẻ tuyệt đối không trả lời, không cung cấp thông tin thẻ khi nhận được yêu cầu qua các kênh email, điện thoại, website có dấu hiệu nghi ngờ

An toàn thanh toán trực tuyến (6)

(9) Đăng ký dịch vụ BSMS cho thẻ và kiểm soát chặt chẽ chi tiêu phát sinh từ thẻ

(10) Lưu thông tin trung tâm hỗ trợ khách hàng để khi có vấn đề bất thường cần lập tức nhờ hỗ trợ


Thank you!