

CHUYÊN ĐỀ 1

AN TOÀN AN NINH THÔNG TIN

CHUYÊN ĐỀ 1

AN TOÀN, AN NINH THÔNG TIN

- Nhận thức về an toàn an ninh thông tin
- Hệ thống các văn bản
- Thiết lập máy tính an toàn
- ATTT khi sử dụng mạng không dây
- Kỹ năng phòng chống mã độc
- Sử dụng mạng xã hội an toàn

NHẬN THỨC VỀ AN TOÀN AN NINH THÔNG TIN

- Khái niệm về an toàn & an ninh thông tin
- Hệ thống & Tài nguyên thông tin
- Các mối đe dọa, Nguy cơ tấn công, Nguyên nhân
- Biện pháp ngăn chặn

Khái niệm về an toàn & an ninh thông tin

- Thông tin là gì?
- An toàn thông tin?
- An ninh thông tin?



Khái niệm về an toàn & an ninh thông tin

➤ Thông tin:

- Theo nghĩa thông thường, thông tin là tất cả **các sự kiện, sự việc, ý tưởng, phán đoán** làm tăng thêm sự hiểu biết của con người.

➤ An toàn thông tin:

- Là sự bảo vệ thông tin và các hệ thống thông tin tránh **bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi** hoặc **phá hoại** trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

➤ An ninh thông tin:

- Là việc bảo đảm thông tin trên mạng **không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.**

- **Hệ thống:** Là tập hợp các máy tính gồm phần cứng, phần mềm, dữ liệu, các thiết lập cấu hình, cơ chế vận hành..v.v.
- **Tài nguyên thông tin:**
 - Phần cứng
 - Phần mềm
 - Dữ liệu (*quốc gia, quốc phòng, sản xuất, kinh doanh..*)
 - Môi trường truyền thông (*mạng, truyền dẫn, giao thức..*)
 - Môi trường làm việc
 -

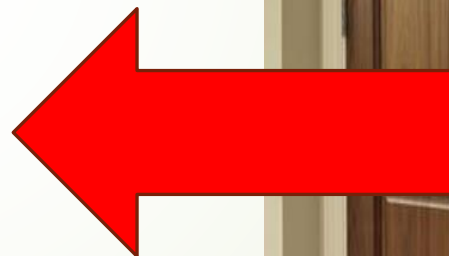
5 tính chất trong an toàn thông tin

- **Tính bí mật:** tránh lộ thông tin đến những đối tượng không được xác thực hoặc để lọt vào các hệ thống khác.
- **Tính toàn vẹn:** dữ liệu không thể bị chỉnh sửa mà không bị phát hiện.
- **Tính sẵn sàng:** thông tin phải luôn luôn sẵn sàng khi cần thiết.
- **Tính xác thực:** đảm bảo rằng dữ liệu, giao dịch, kết nối hoặc các tài liệu đều là thật.
- **Tính không thể chối cãi:** không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác.

Các mối đe dọa

- **Phá hoại:**
 - Phá hỏng thiết bị phần cứng
 - Phá hỏng phần mềm
 - Phá hỏng dữ liệu
 - Phá hỏng các thiết lập cấu hình...
- **Sửa đổi:**
 - Dữ liệu
 - Thiết lập cấu hình
- **Can thiệp:**
 - Hệ thống bị truy cập trái phép
 - Đánh cắp thông tin
 - Tấn công điều khiển....

An ninh truyền thống



An ninh tài sản số

Internet



Nguy cơ tấn công

➡ Từ bên trong:

- ➡ Người có quyền truy cập hệ thống
- ➡ Kẻ giả mạo người có quyền truy cập

➡ Từ bên ngoài:

- ➡ Hacker
- ➡ Cracker
- ➡ Các phần mềm độc hại...

➡ Giao dịch mạng:

- ➡ Lừa đảo qua hệ thống mạng xã hội, website: facebook, email,...

➡ Khách quan:

- ➡ Sự phát triển nhanh của KHCCN tạo ra CN mới, kỹ thuật mới
- ➡ Lỗ hổng phần mềm...

➡ Chủ quan:

- ➡ Nhận thức về an toàn an ninh thông tin chưa đầy đủ, chưa quan tâm
- ➡ Kiến thức, kinh nghiệm, năng lực, kỹ năng
- ➡ Chính sách an ninh chưa chặt chẽ
- ➡ Đầu tư hạ tầng phần cứng, phần mềm chưa đáp ứng
- ➡ Thiết lập cấu hình, phân quyền không chặt chẽ

Biện pháp ngăn chặn

➤ Phần cứng:

- Thiết bị tường lửa
- Thiết bị giám sát
- Thiết bị chống xâm nhập...

➤ Phần mềm:

- Bản quyền phần mềm
- Phần mềm diệt virus
- Cập nhật các bản vá lỗi

➤ Chính sách:

- Chính sách an toàn và bảo mật: đơn vị, người dùng
- Tăng cường nhận thức, kỹ năng cho người sử dụng

HỆ THỐNG CÁC VĂN BẢN QUY ĐỊNH VỀ AN TOÀN, AN NINH THÔNG TIN

- Văn bản Luật
- Nghị định, thông tư
- Văn bản của tỉnh Nghệ An

Hệ thống các văn bản về ATTT

➤ Văn bản Luật:

- Luật an toàn thông tin Mạng (86/2015/QH13 - 19/11/2015)
- Luật An ninh Mạng (24/2018/QH14 - 12/06/2018)

➤ Nghị định, Thông tư:

- Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn HTTT theo cấp độ
- Thông tư số 03/2017/TT-BTTTT hướng dẫn Nghị định 85/2016/NĐ-CP

➤ Văn bản của tỉnh Nghệ An:

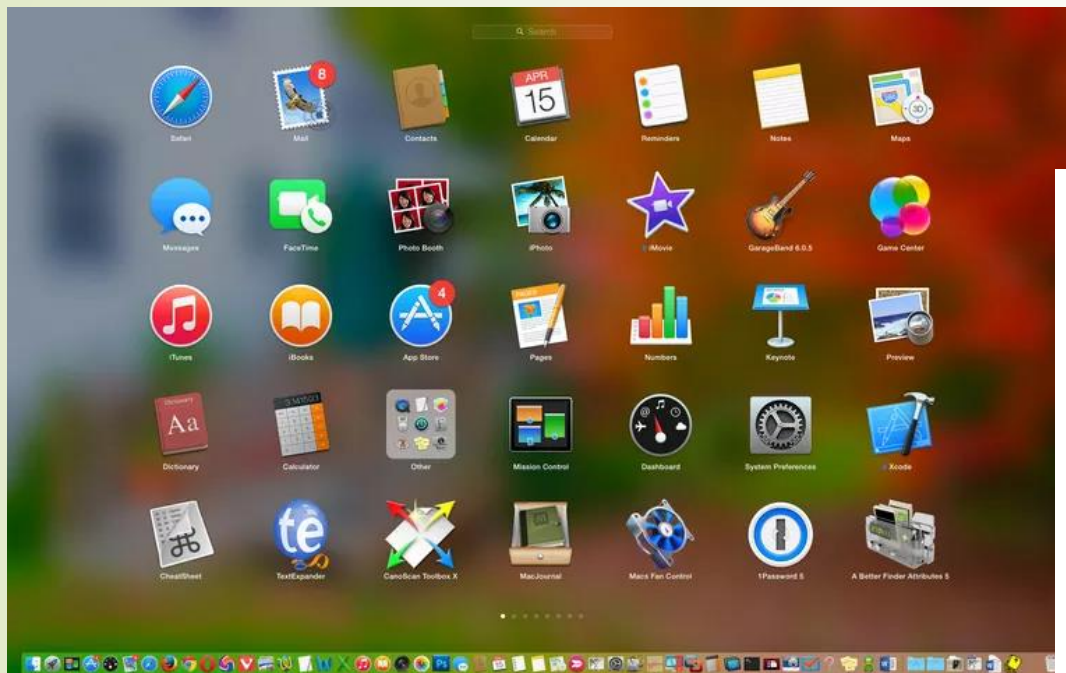
- Quyết định số 87/2016/QĐ-UBND ngày 28/12/2016 của UBND tỉnh Nghệ An về việc ban hành quy chế đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Nghệ An

<http://hotro.nait.vn/index.php?id=attt>

THIẾT LẬP MÁY TÍNH AN TOÀN

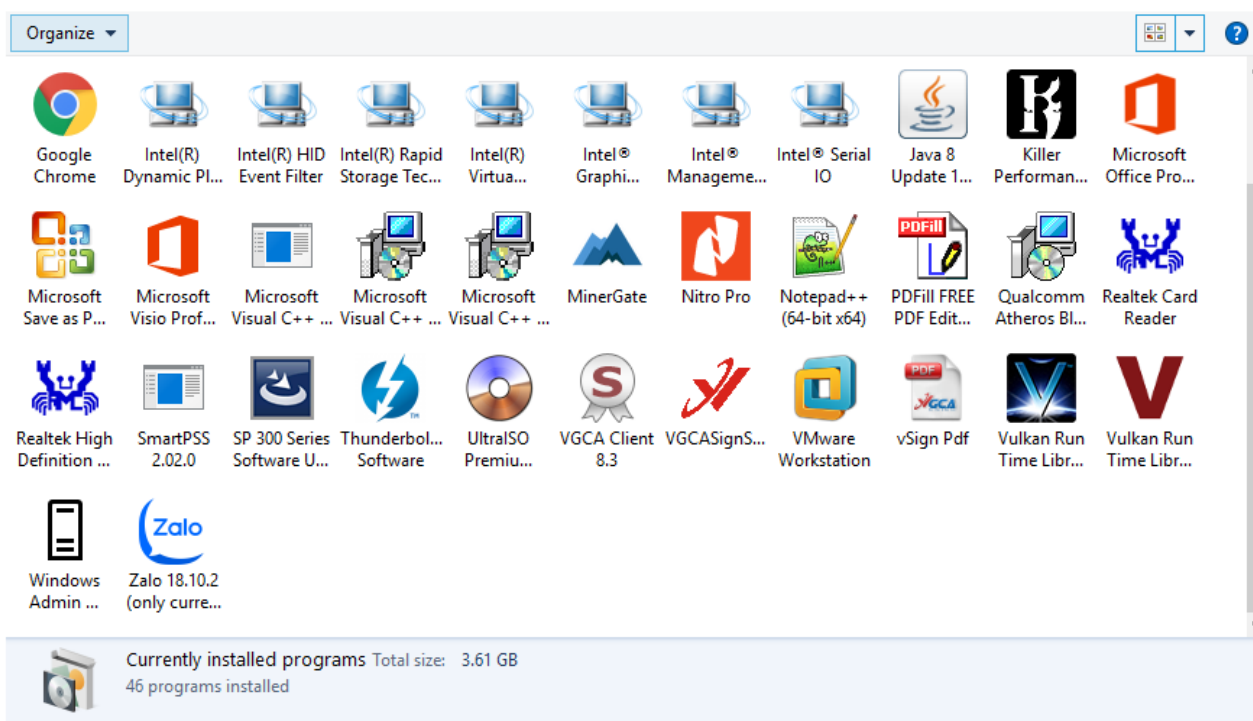
- Xóa các phần mềm không cần thiết
- Kích hoạt chức năng tường lửa
- Nâng cấp các phần mềm và hệ điều hành Windows
- Cài đặt phần mềm diệt virus
- Tạo mật khẩu mạnh

Xóa các phần mềm không cần thiết



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

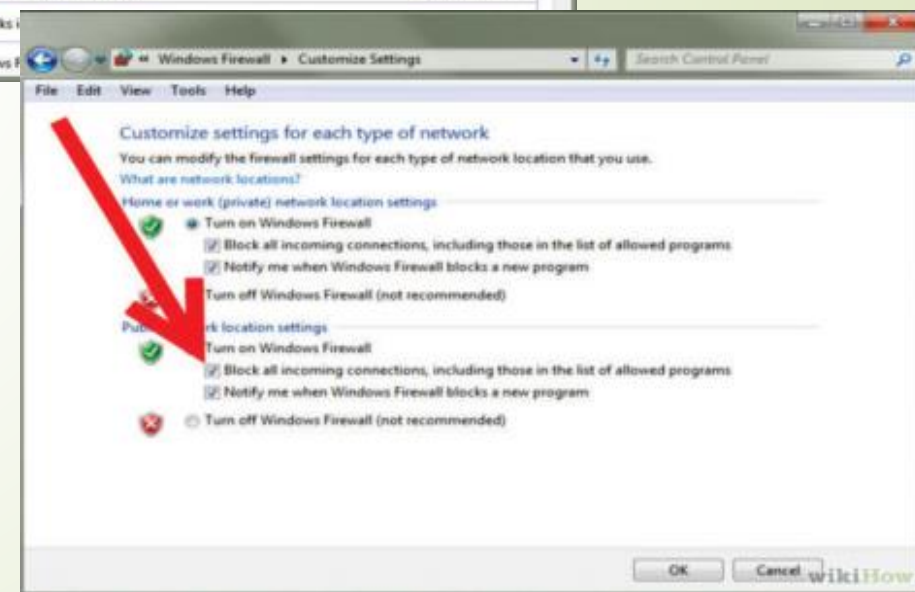
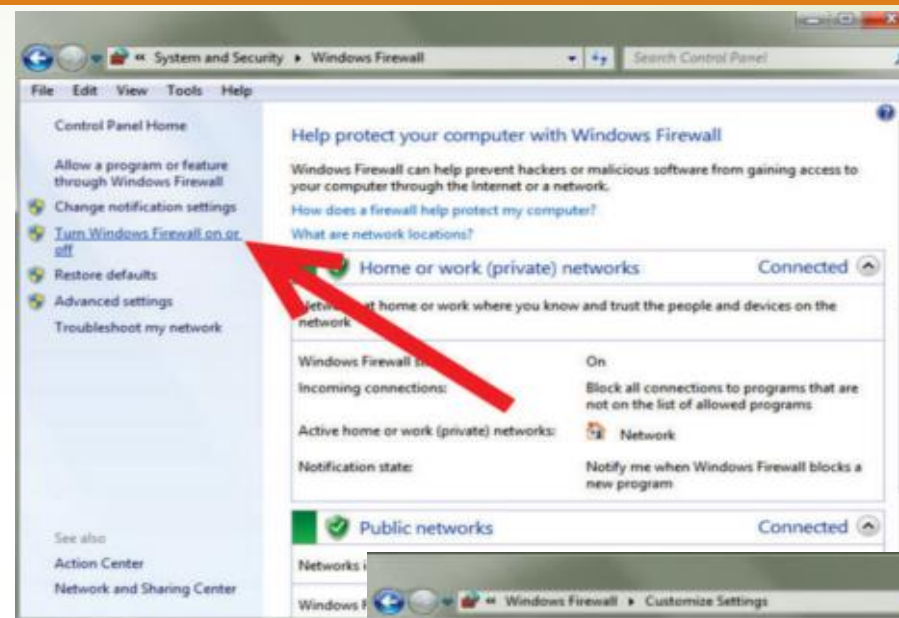


Xóa các phần mềm không cần thiết

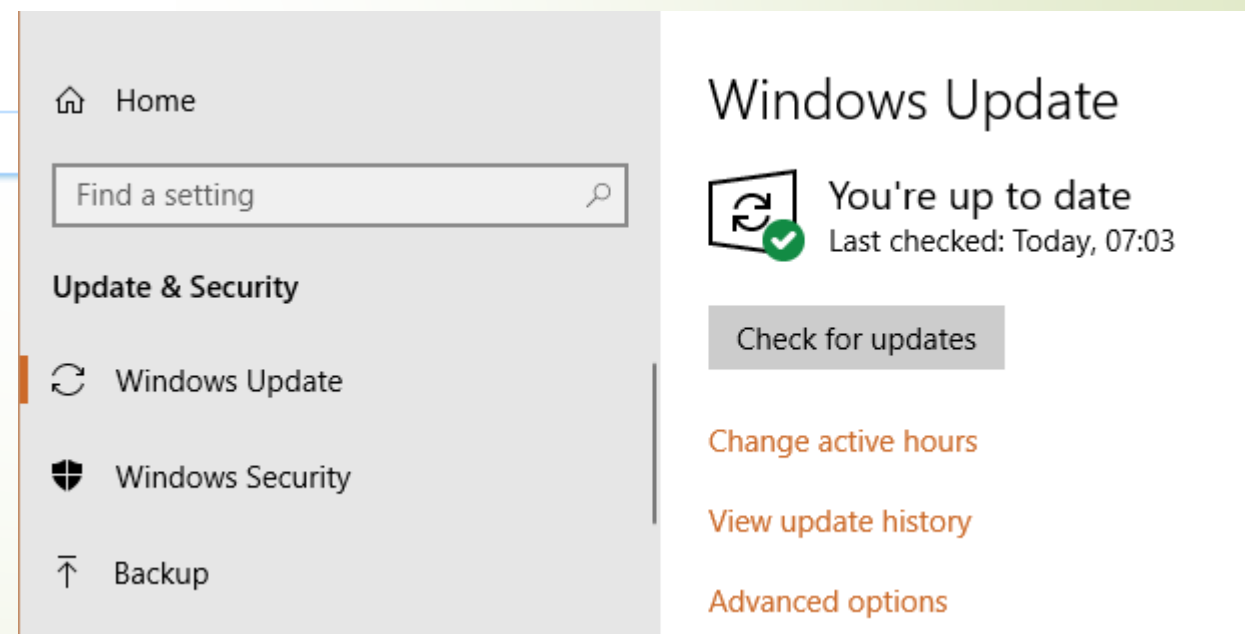
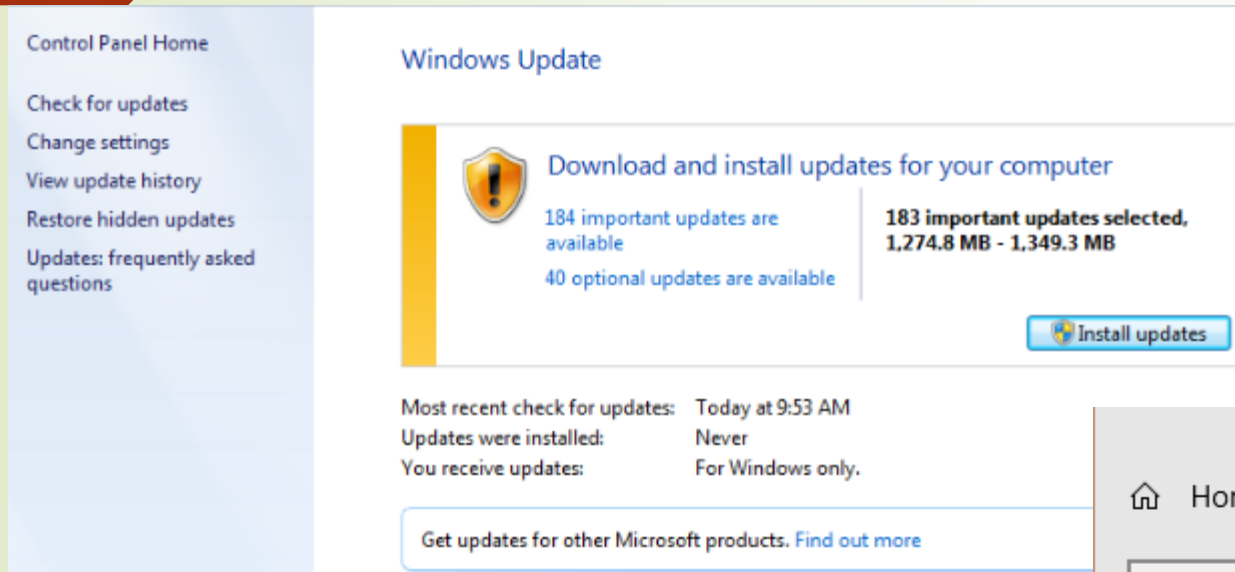
- Các máy tính mới thường được nhà sản xuất cài đặt sẵn các chương trình quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm.
- Các phần mềm này có thể chứa sẵn các nguy cơ mất an toàn thông tin
- Do đó, người dùng cần tháo bỏ các chương trình không cần thiết trên máy tính của mình ngay trong quá trình thiết lập ban đầu

Kích hoạt chức năng tường lửa

- Các hệ điều hành đều tích hợp tường lửa nhằm bảo vệ người sử dụng khỏi các tấn công cơ bản. Hãy kích hoạt phần mềm tường lửa trước khi kết nối đến bất kỳ mạng máy tính nào (Internet/Wifi/LAN)



Nâng cấp phần mềm và hệ điều hành



- Hệ điều hành của máy tính lúc vừa cài đặt có thể là phiên bản cũ chưa được vá các lỗi bảo mật. Do đó, người sử dụng cần thiết lập chế độ tự động nâng cấp và thực hiện nâng cấp cho hệ điều hành và các phần mềm khác.
- Trong các tùy chọn về nâng cấp, người sử dụng có thể tùy chọn theo nhu cầu của mình. Tuy nhiên, có thể tùy chọn việc tự quyết định thực hiện nâng cấp theo yêu cầu của người sử dụng để đảm bảo không bị gián đoạn công việc do quá trình nâng cấp.

Cài đặt phần mềm diệt virus

- Phần mềm diệt virus là lớp lá chắn quan trọng bảo vệ người sử dụng khỏi các mã độc và virus



Tạo mật khẩu mạnh

Ký tự hoa, ký tự thường

Ký tự chữ số

Ký tự đặc biệt
(\$#%\"#%)



Tạo mật khẩu hai lớp (OTP - One Time Password)



Mã hóa dữ liệu quan trọng khi lưu vào USB



Mã hóa



AN TOÀN THÔNG TIN KHI SỬ DỤNG MẠNG WIFI

- Các nguy cơ có thể xảy ra
- Nguy cơ mất ATTT từ WiFi
- Những việc cần làm khi truy cập Internet bằng wifi
- Dễ dàng đánh cắp mật khẩu WiFi

Các nguy cơ có thể xảy ra

**Bị xâm phạm
dịch vụ**

Bị lợi dụng

Bị theo dõi

Bị tấn công

Nguy cơ mất ATTT từ WiFi



Những việc cần làm khi truy cập Internet bằng wifi

- ➡ Sử dụng mạng riêng ảo
- ➡ Sử dụng xác thực 2 bước
- ➡ Cẩn thận với tính năng tự động kết nối mạng không dây
- ➡ Xác minh mạng không dây
- ➡ Hạn chế việc đăng nhập

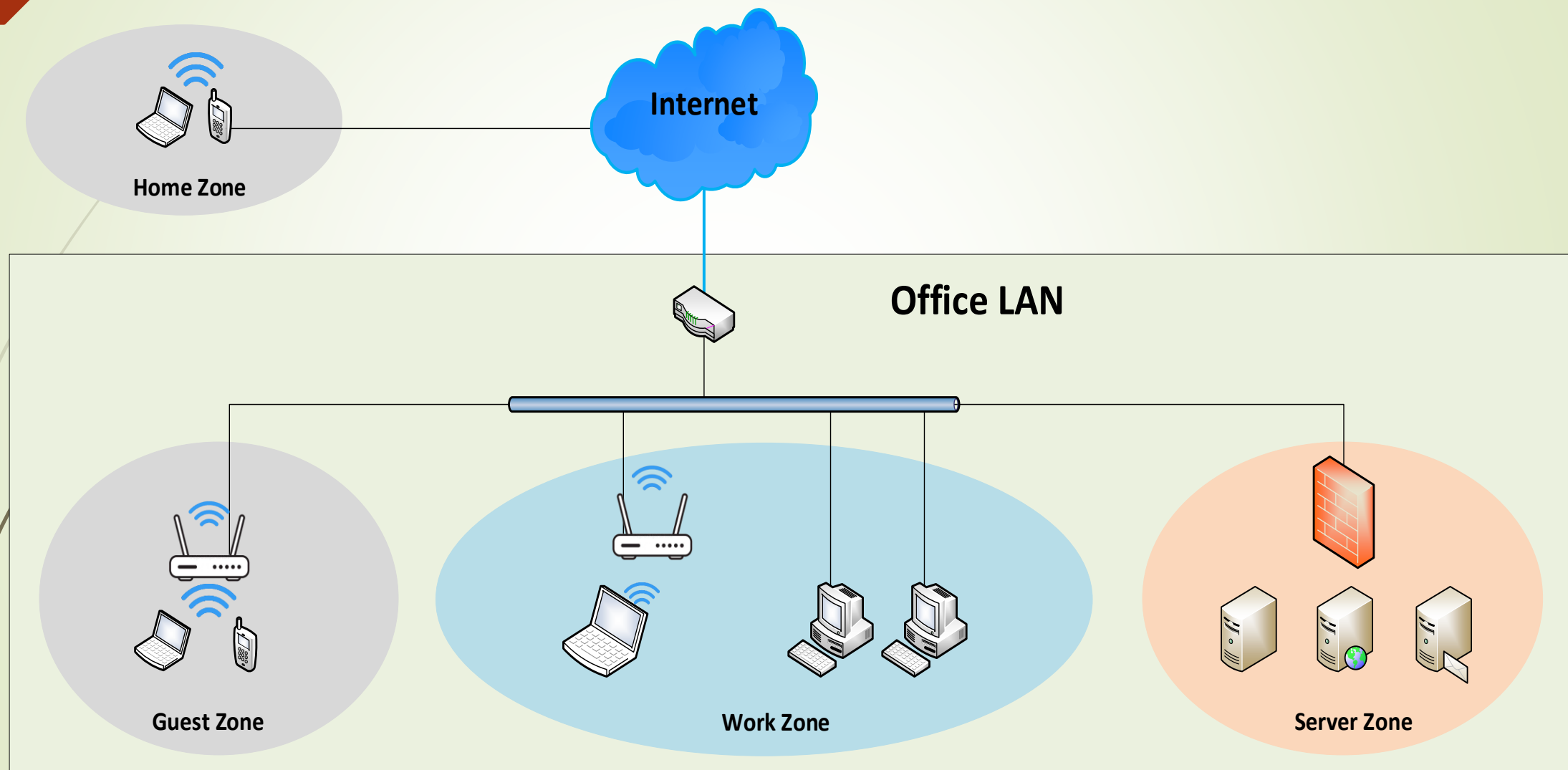
Dễ dàng đánh cắp mật khẩu WiFi



Bảo mật mạng WIFI công cộng



Bảo mật mạng WIFI công sở



Bảo mật mạng WIFI gia đình

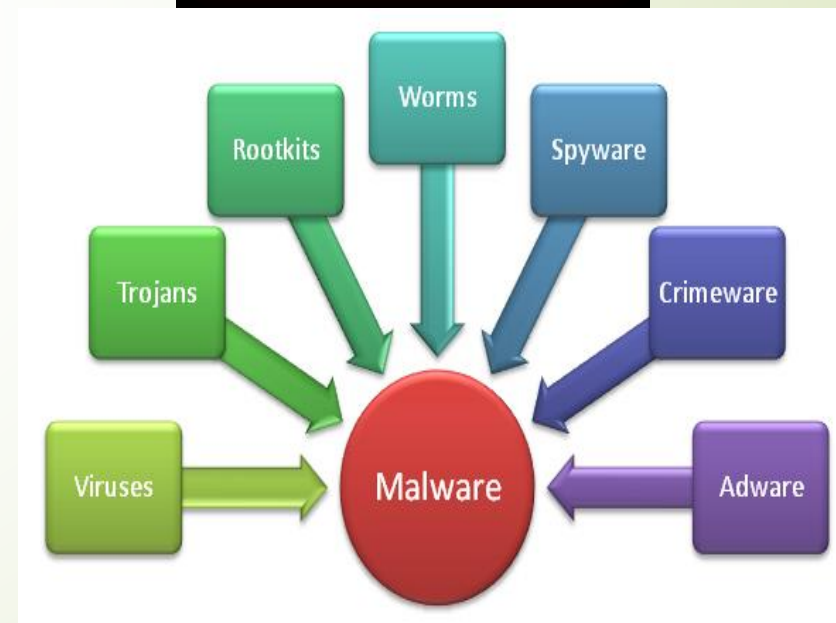


KỸ NĂNG PHÒNG CHỐNG MÃ ĐỘC

- Khái niệm mã độc, Các hành vi của mã độc
- Sử dụng thư điện tử thận trọng
- Cẩn thận khi truy cập các trang web trên mạng Internet
- Không sử dụng phần mềm bẻ khoá, không bản quyền
- Sử dụng phần mềm diệt virus

Khái niệm mã độc

- Là một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức



Các hành vi của mã độc

Lấy cắp dữ liệu

1



Theo dõi hoạt động

2



Bị lợi dụng thực hiện tấn công đối tượng khác

3

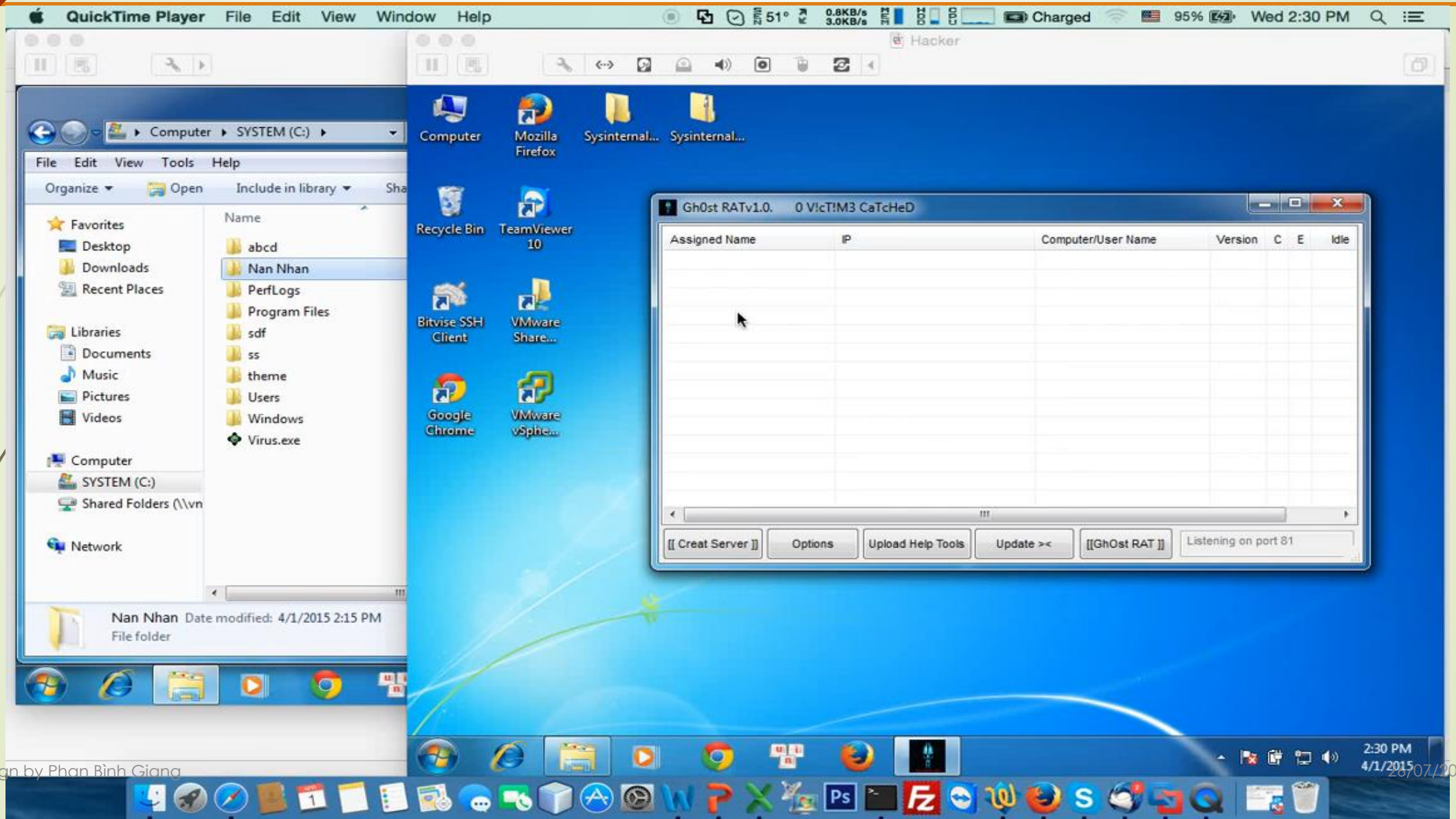


Phá hoại dữ liệu

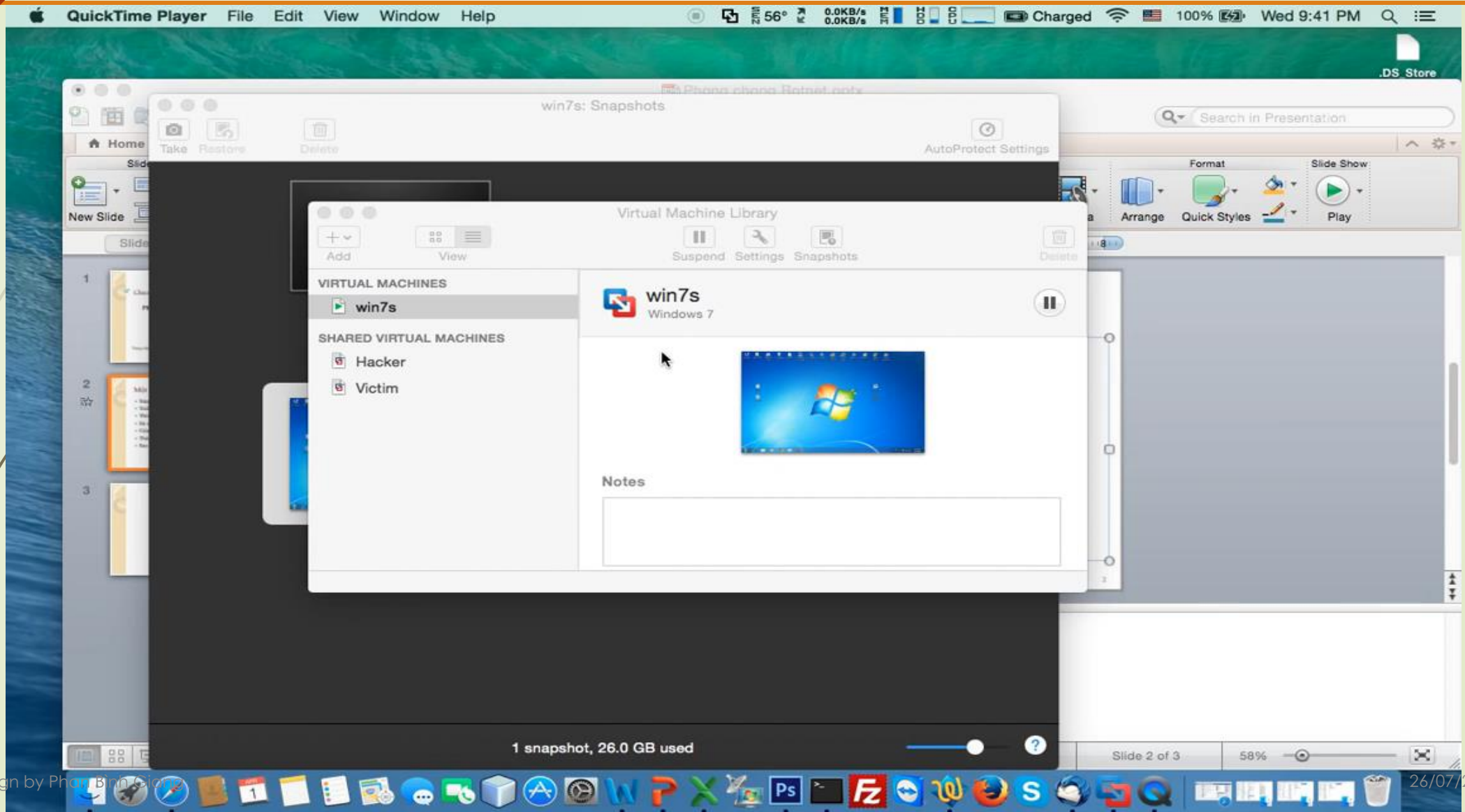
4



Clip demo lấy cắp dữ liệu



Clip demo phá hoại dữ liệu



Sử dụng thư điện tử thận trọng

- Mã độc có thể lây nhiễm vào máy tính người sử dụng thông qua các tệp tin đính kèm thư điện tử của người lạ gửi đến nạn nhân hoặc thư điện tử giả mạo một cơ quan, tổ chức
- Người sử dụng không nên mở các tệp tin đính kèm thư điện tử nhận được từ một người lạ hoặc một người có địa chỉ thư điện tử giống với những người mà mình quen biết
- Sử dụng chương trình diệt virus để dò quét tệp tin đính kèm trước khi đọc nội dung

Cẩn thận khi truy cập các trang web trên mạng Internet

- Chỉ cần truy cập vào một trang web độc hại là người dùng đã có thể bị lây nhiễm mã độc vào máy tính của mình.
- Các trang web này thường dụ dỗ người sử dụng truy cập thông qua các liên kết gửi qua mạng xã hội, thư điện tử hay tin nhắn.
- Hầu hết các trình duyệt Internet sẽ cảnh báo
- Người sử dụng cần thật cẩn trọng khi truy cập vào các trang web lạ được gửi đến từ người khác trong quá trình sử dụng các dịch vụ trên mạng

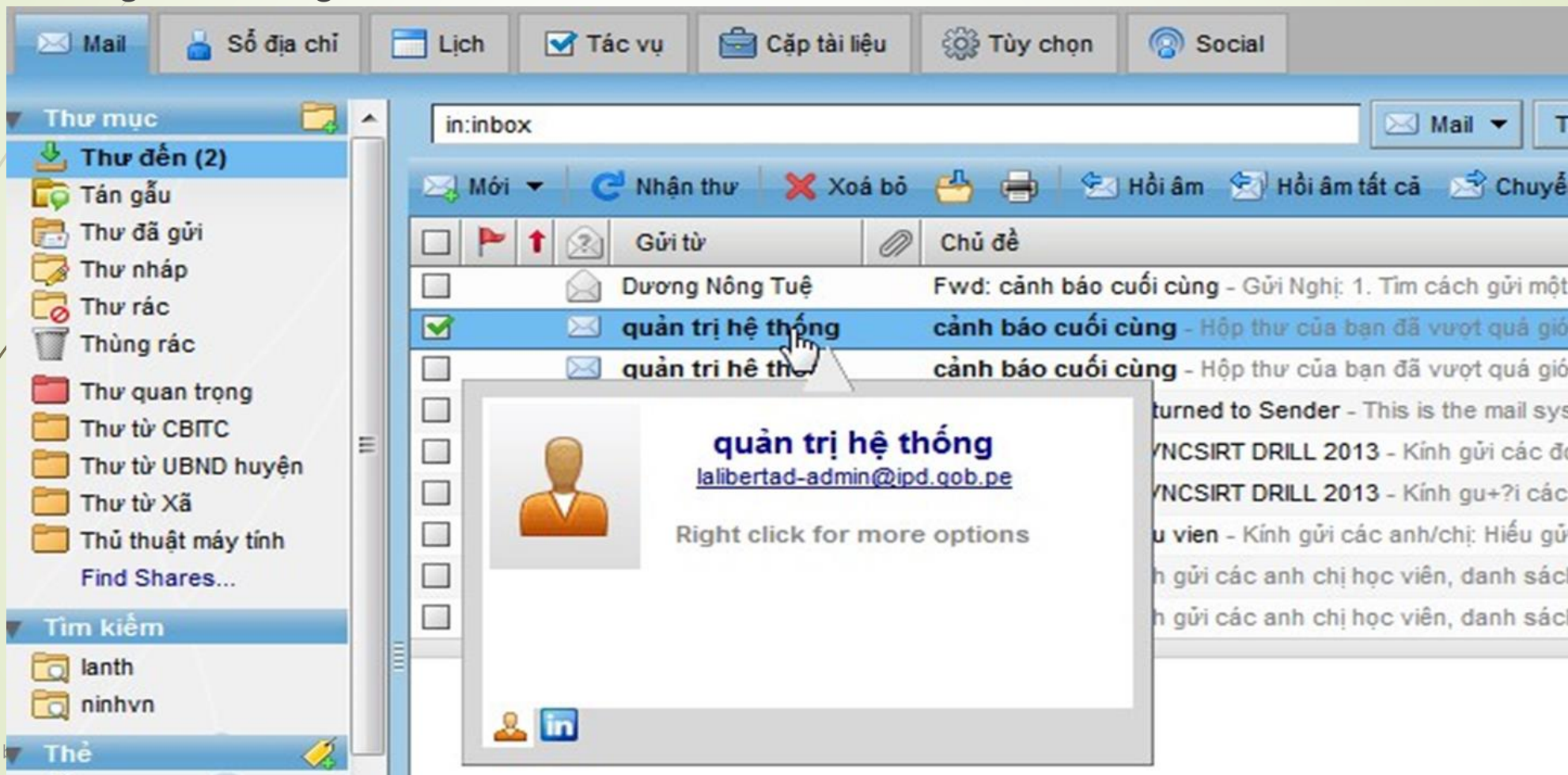
- Các phần mềm độc hại có thể tồn tại trong các phần mềm bẻ khoá, phần mềm miễn phí hay có trả phí nhưng không được tải từ chính trang web của nhà phát triển.
- Không nên tải, sử dụng hay cài đặt các phần mềm bẻ khoá hoặc các phần mềm được chia sẻ trên các diễn đàn, mạng xã hội mà người dùng không rõ nguồn gốc
- Cách tốt nhất để phòng chống mã độc là tải phần mềm tại ngay chính trang web của nhà sản xuất

Sử dụng phần mềm diệt virus

- Có nhiều chương trình diệt virus miễn phí và có trả phí. Các chương trình miễn phí có ít chức năng hơn nhưng cũng có thể giúp người dùng cơ bản chống lại các mã độc thông dụng
- Một số mã độc giả mạo chính phần mềm diệt virus. Do đó, người dùng cần tải các chương trình diệt virus tại chính trang web của nhà sản xuất
- Cần cẩn trọng với việc sử dụng USB để sao lưu dữ liệu giữa các máy tính

Không nên tin tưởng tên hiển thị trong mail

- Giả mạo tên hiển thị của một email để đánh lừa như: tên của các Công ty, tổ chức, hãng lớn; Người quen của bạn; Người nổi tiếng



Cần nhắc kỹ lưỡng khi bấm vào liên kết trong email



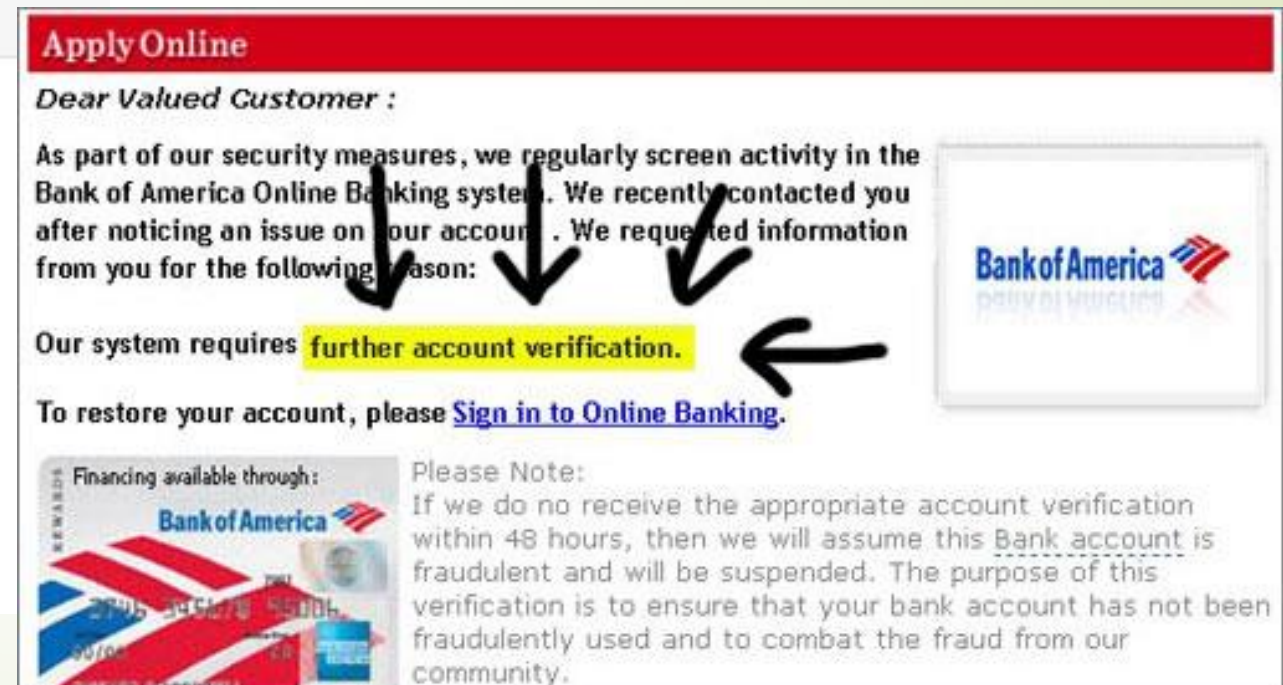
HSBC  **The world's local bank**

Our Valued Customer,
You Have 1 New Security Message Alert !
[Click here to resolve the problem](#)
Sincerely,
HSBC Bank Plc
Security Department Team



Bỏ qua các email yêu cầu cung cấp thông tin cá nhân

- Một tổ chức, công ty, ngân hàng,... sẽ không bao giờ yêu cầu người sử dụng cung cấp thông tin cá nhân



Cẩn trọng email có tiêu đề Hấp dẫn - Nhạy cảm - Khẩn cấp

cảnh báo cuối cùng

▼ Gửi từ:  quản trị hệ thống

Hộp thư của bạn đã vượt quá giới hạn lưu trữ của 2.GB
Được thành lập bởi người quản trị hiện nay là 2.30GB, có thể không
gửi hoặc nhận tin nhắn mới cho đến khi bạn xác nhận e-mail của bạn

Nhấp vào liên kết dưới đây để xác nhận e-mail của bạn

<http://dichvuemail001.webs.com/>

cảm ơn bạn
quản trị hệ thống



Thông Báo Tvoo, 47

🏠 Sống ở Hà Nội

💍 Đã kết hôn

•Chúc Mừng Tài Khoản Twoo Của Bạn Mang Mã Số Dự Thưởng (TBY92A) Đã May Mắn Nhận Được Giải Nhất Của Chương Trình Trùng : "Sự Kiện Tuần Lễ Vàng-Trí An Khách HÀNG Quý II Là :----->> 🎉 1 Xe Liberty 150 I.E & 50 Triệu Đồng Tiền Mặt 🎉 <<----- Bây Giờ Bạn Vui Lòng Liên Hệ Hotline ☎ (0084) 905 870165

Hoặc Truy Cập Vào <http://HoSoCaNhanTwoo.Com> Để Làm Hồ Sơ Nhận Giải Nhất Về Địa Chỉ Của Bạn.Hệ Thống Thông Báo Ngày (29/08/2014)

• Lưu Ý: Chỉ Áp Dụng Cho Tài Khoản Nhận Được Thông Báo Ngày Từ Hệ Thống.

• Chúc Mừng Bạn.
hôm nay lúc 08:44



★ Thông Báo ★

•Chúc Mừng Tài Khoản Twoo Của Bạn Mang Mã Số Dự Thưởng (TBY92A) Đã May Mắn Nhận Được Giải Nhất Của Chương Trình Trùng : "Sự Kiện Tuần Lễ Vàng-Trí An Khách HÀNG Quý II Là :----->> 🎉 1 Xe Liberty 150 I.E & 50 Triệu Đồng Tiền Mặt 🎉 <<----- Bây Giờ Bạn Vui Lòng Liên Hệ Hotline ☎ (0084) 905 870165

Hoặc Truy Cập Vào <http://HoSoCaNhanTwoo.Com> Để Làm Hồ Sơ Nhận Giải Nhất Về Địa Chỉ Của Bạn.Hệ Thống Thông Báo Ngày (29/08/2014)

• Lưu Ý: Chỉ Áp Dụng Cho Tài Khoản Nhận Được Thông Báo Ngày Từ Hệ Thống.

• Chúc Mừng Bạn.
hôm nay lúc 08:44

Cẩn thận, cân nhắc khi tải về các File đính kèm

Nguy cơ

- Là phương thức tấn công phổ biến và nguy hiểm nhất

Không nên

- Tải và mở chạy file ngay khi nhận được các email có file đính kèm

Chú ý

- Định dạng file và tạo thói quen quét virus với các file đính kèm trước khi mở chúng

Nhận diện các email spam – email quảng cáo

Hãy nhìn vào tên của bạn trong phần địa chỉ

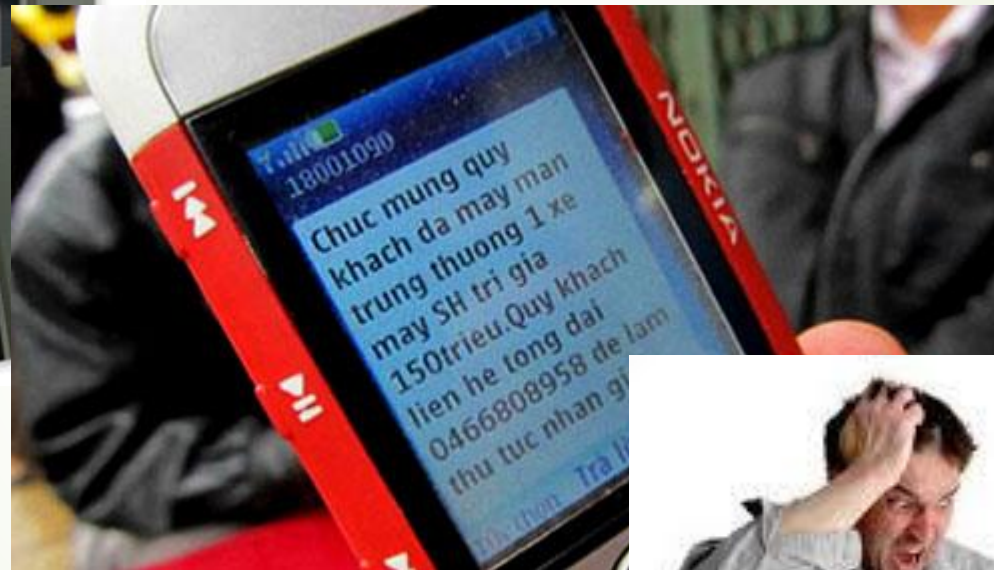
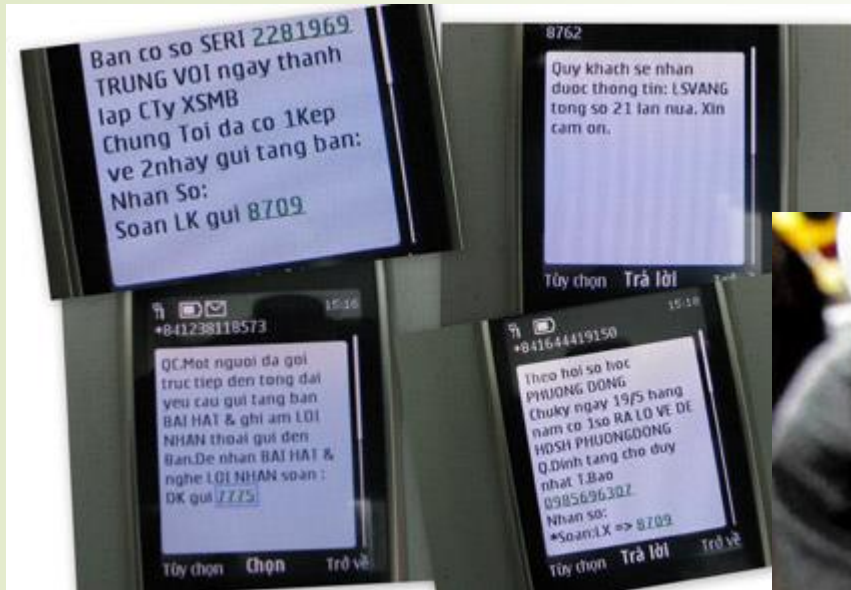
Xem xét lời chào hỏi.

Xem các URL xuất hiện trong email và so với
thanh trạng thái của trình duyệt

Sử dụng Copy & Paste

Sử dụng tính năng chặn email spam

Cẩn trọng với các tin nhắn rác



SỬ DỤNG MẠNG XÃ HỘI AN TOÀN

- Lợi ích, Mạng xã hội có an toàn không?
- Tác hại, Các rủi ro khi sử dụng mạng xã hội
- Bảo vệ bản thân trên mạng xã hội?
- Bảo mật thông tin cá nhân trên mạng

Lợi ích?

**Giới
thiệu
bản
thân
mình
với mọi
người**

**Kết nối
bạn bè**

**Tiếp
nhận
thông
tin, học
hỏi kiến
thức và
kỹ
năng**

**Kinh
doanh**

**Bày tỏ
quan
niệm
cá
nhân**

**Mang
đến lợi
ích về
sức
khỏe**



Mạng xã hội có an toàn không?



Lợi ích?



Tác hại

Giảm tương tác giữa người với người

Lãng phí thời gian và xao lãng mục tiêu thực của cá nhân

Nguy cơ mắc bệnh trầm cảm

Giết chết sự sáng tạo

Không trung thực và bạo lực trên mạng

Thường xuyên so sánh bản thân với người khác

Mất ngủ

Các rủi ro khi sử dụng mạng xã hội

- ➡ Làm ảnh hưởng tới hình ảnh, uy tín của bản thân.
- ➡ Các thông tin đưa lên mạng xã hội như: vị trí địa lý, sở thích cá nhân, danh sách bạn bè, kẻ xấu có thể khai thác thêm các thông tin cá nhân khác hoặc dò tìm dữ liệu tài chính, ngân hàng
- ➡ Luôn luôn phải đối mặt với nguy cơ bị tấn công, bị cài phần mềm gián điệp làm lộ các thông tin mật của cá nhân hoặc cơ quan, tổ chức.
- ➡ Có thể gây nghiện, ảnh hưởng đến công việc và gia đình

Bảo vệ bản thân trên mạng xã hội?

01

Chỉ đưa những
thông tin lên
mạng khi mình
thấy thoải mái

02

Cần hạn chế cung cấp thông
tin cá nhân

03

Những thành viên khác trên mạng xã
hội và Internet đều có thể lấy được
thông tin, kể cả trường hợp đã xoá,
chỉnh sửa

Bảo mật thông tin cá nhân trên mạng

- Không tiết lộ số điện thoại, địa chỉ thực tế, lịch công tác, thông tin liên quan tới công việc của mình tại cơ quan...
- Đặt chế độ cá nhân hoặc chỉ bạn bè thân thiết và tin cậy mới có thể xem để tránh trường hợp kẻ xấu có thể lợi dụng
- Sử dụng mật khẩu khó dò tìm, khó đoán và luôn giữ bí mật mật khẩu, tuyệt đối không chia sẻ cho ai khác.
- Sử dụng các trình duyệt web phổ biến và đã được cập nhật

“

XIN CẢM ƠN!

”