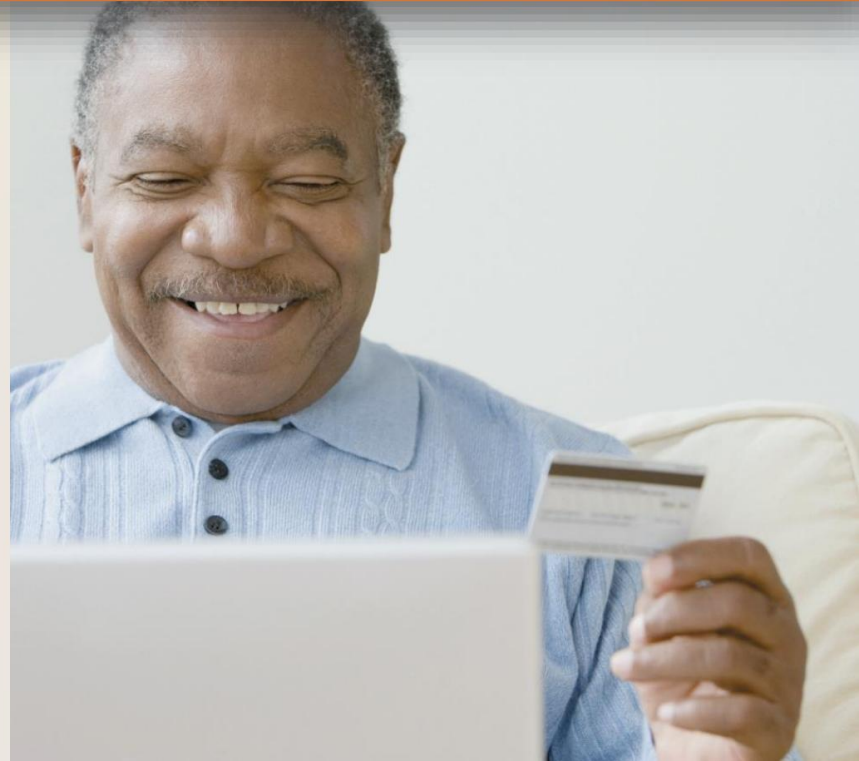


Chapter Eleven

Computer Security and Safety, Ethics, and Privacy

Khám phá Máy tính 2012

Hướng dẫn tương tác của bạn
với thế giới kỹ thuật số



Tổng quan về mục tiêu

Các loại
thủ phạm
tội phạm mạng

Các cuộc tấn
công mạng và
Internet và
các cách bảo vệ

Truy cập và
sử dụng máy tính
trái phép

Ăn cắp và phá
hoại phần cứng;
Trộm phần mềm

Mã hóa thông
tin

Mối quan tâm phi
kỹ thuật của
việc sử dụng máy tính

Rủi ro bảo mật máy tính

- Rủi ro bảo mật máy tính là bất kỳ sự kiện nào có thể gây ra hư hỏng máy tính.

Network range

- Tội phạm mạng là một hành vi bất hợp pháp trực tuyến hoặc dựa trên Internet

Tin tặc

(truy cập trái phép)

Bánh quy giòn

(truy cập trái phép và
thiệt hại)

Script Kiddies

(sử dụng các chương trình hack
được tạo sẵn do người khác thực hiện)

Công ty

Gián điệp

Những kẻ khủng bố trên mạng

(làm hỏng máy tính vì
lý do chính trị)

Cyberextorcians

(sử dụng mạng như một lực
lượng tấn công để đòi tiền)

Rủi ro bảo mật máy tính

- Thông tin được truyền qua mạng có mức độ rủi ro bảo mật cao hơn so với thông tin được lưu giữ tại cơ sở của tổ chức



Các cuộc tấn công mạng và Internet

- Phần mềm độc hại (phần mềm độc hại):

Máy vi tính Vi-rút

- Đính kèm với một chương trình, yêu cầu hành động của con người để lan tỏa.

Sâu

- Tự sao chép nhiều lần mà không có sự tác động của con người, sử dụng hết tài nguyên và có thể tắt máy tính

Ngựa thành Troy

- Độc hại chương trình trông giống như một chương trình hợp pháp

Rootkit

- Chương trình ẩn sự hiện diện của nó trong máy tính và cho phép quản trị viên truy cập cấp độ

Các cuộc tấn công mạng và Internet

- Máy tính bị nhiễm độc có một hoặc nhiều hiện tượng sau:

Chậm lại

Ít có sẵn
ký ức

Sự cố

Cửa sổ bật lên

Trang chủ trình
duyet mới,
thanh toolbars mới

không xác định
chương trình
xuất hiện một
cách bí ẩn

Thuộc
tính hệ
thống thay đổi

Hệ điều
hành tắt đột
ngột
unexpectedly

Các cuộc tấn công mạng và Internet

Mẹo để ngăn chặn vi rút và phần mềm độc hại khác

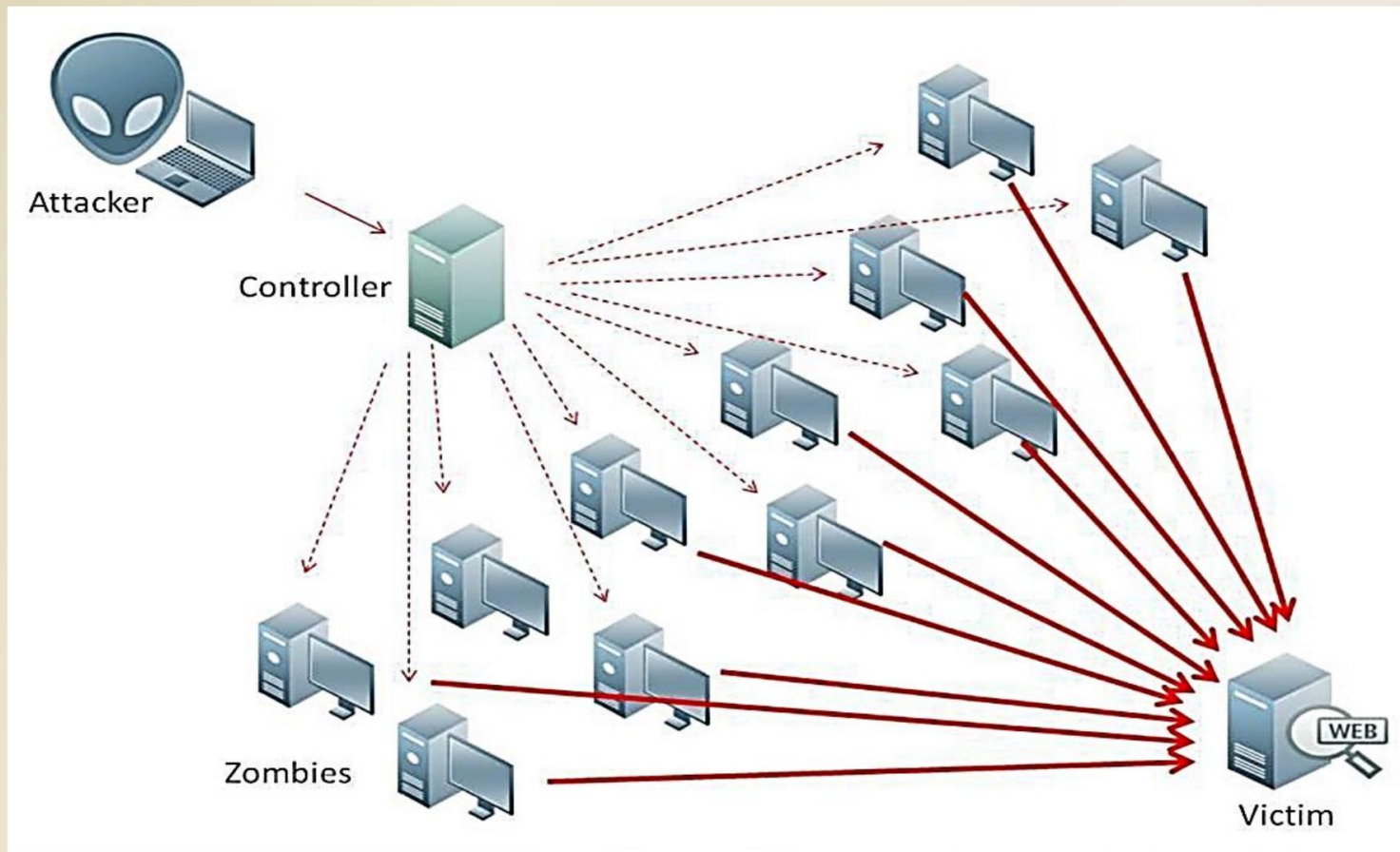
1. Không bao giờ khởi động máy tính với **phương tiện di động** được lắp vào, trừ khi phương tiện đó không bị nhiễm.
2. Không bao giờ mở **tệp đính kèm e-mail** trừ khi bạn mong đợi và nó đến từ một nguồn đáng tin cậy.
3. Cài đặt một **chương trình chống vi-rút** trên tất cả các máy tính của bạn. Cập nhật phần mềm và các tập tin chữ ký vi rút thường xuyên.
4. Quét tất cả các chương trình đã tải xuống và phương tiện được cắm để tìm vi-rút và phần mềm độc hại khác.
5. Nếu chương trình chống vi-rút gắn cờ một tệp đính kèm e-mail là bị nhiễm, hãy xóa hoặc cách ly tệp đính kèm ngay lập tức.
6. Cài đặt chương trình **tường lửa cá nhân** .
7. Cập nhật thông tin về các cảnh báo vi rút mới và các trò lừa bịp vi rút.

Các cuộc tấn công mạng và Internet

- Mạng **botnet** là một nhóm các máy tính được kết nối với nhau được điều khiển từ xa bởi tội phạm mạng mà không có chủ sở hữu nhận thức.
 - Một máy tính bị xâm nhập được gọi là **xác sống**
- Tấn **công từ chối dịch vụ (tấn công DoS)** làm cho dịch vụ Internet không khả dụng bằng cách làm ngập mục tiêu với lưu lượng truy cập để gây ra sự cố.
 - DoS phân tán (**DDoS**)

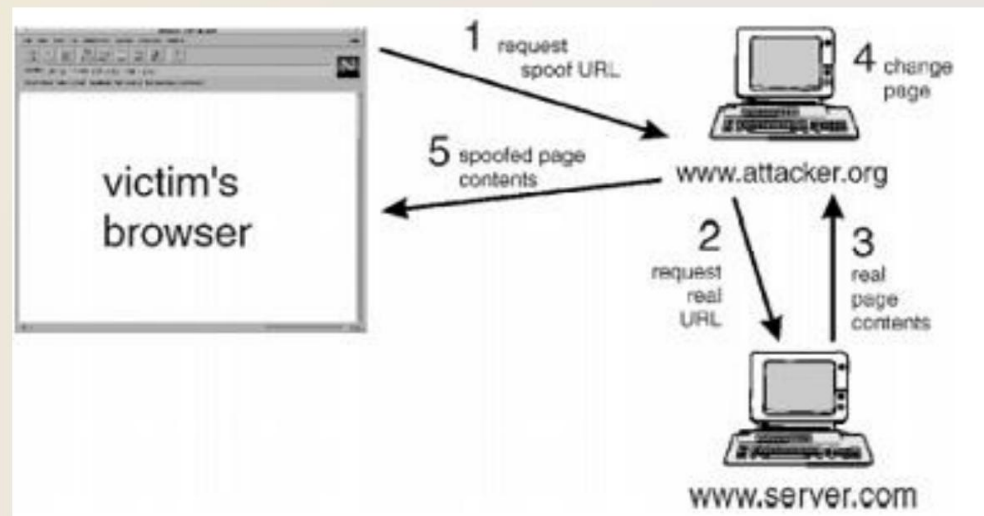
Các cuộc tấn công mạng và Internet

- Các cuộc tấn công DDoS được khởi động từ botnet (thây ma):



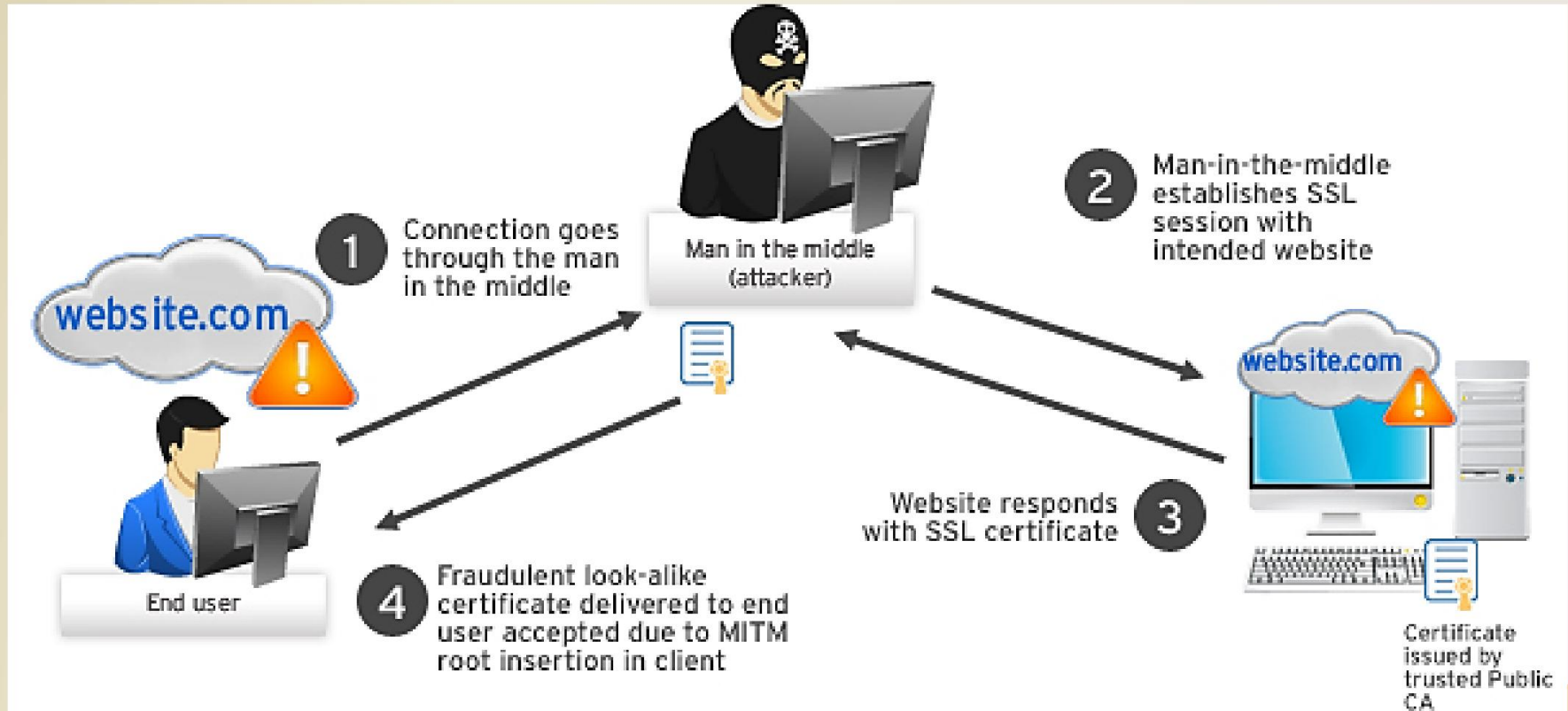
Các cuộc tấn công mạng và Internet

- Cửa **sau** là một chương trình cho phép người dùng bỏ qua xác thực thông thường và có được quyền truy cập.
- **Giả mạo** là một kỹ thuật mà những kẻ xâm nhập sử dụng để làm cho đường truyền Internet của họ có vẻ hợp pháp. Vd: giả mạo email , giả mạo web, giả mạo IP.



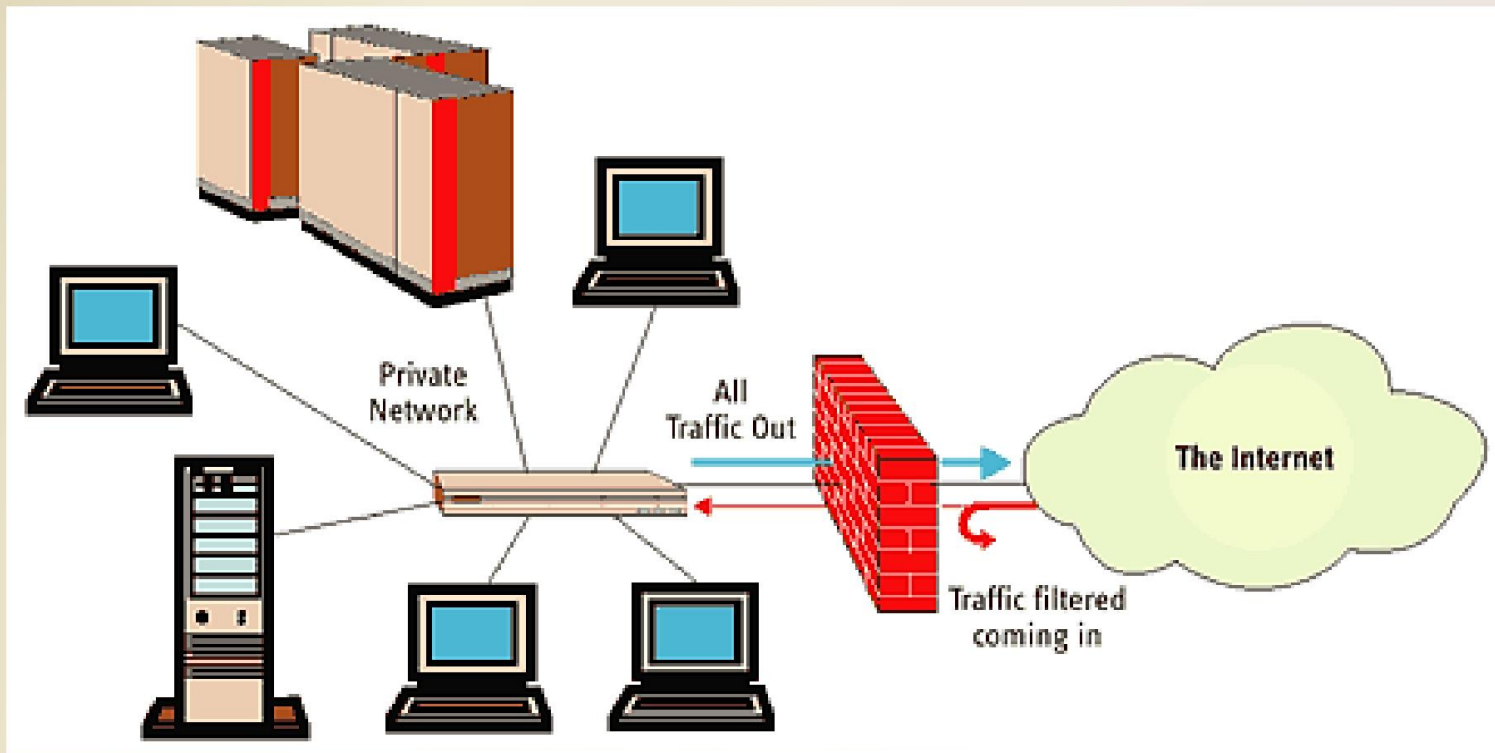
Các cuộc tấn công mạng và Internet

- **Man-in-the-Middle (MITM):** kẻ tấn công bí mật chuyển tiếp và có thể thay đổi thông điệp giữa hai bên.



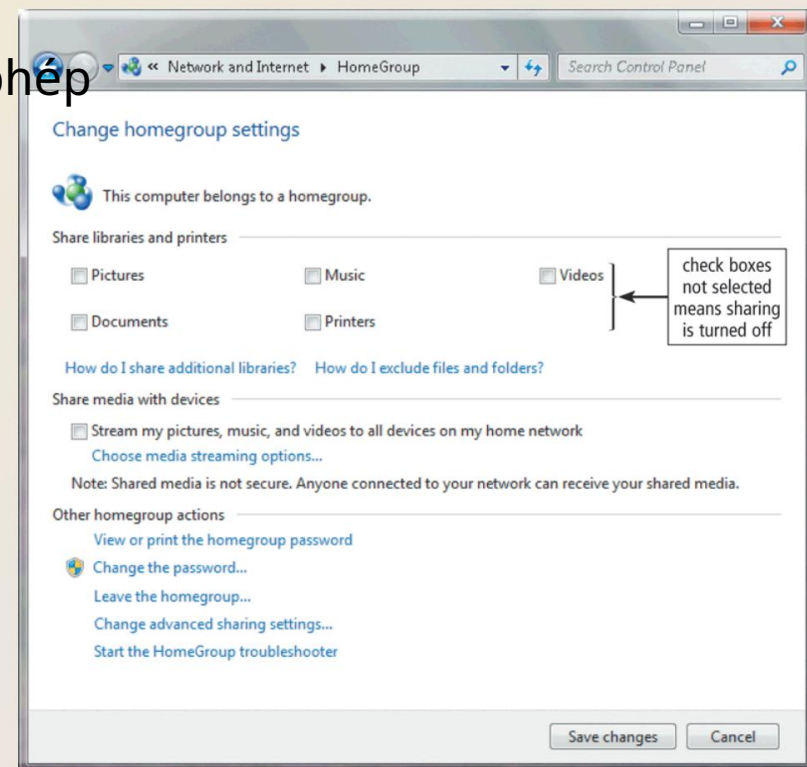
Các cuộc tấn công mạng và Internet

- **Tường lửa** là phần cứng và / hoặc phần mềm bảo vệ tài nguyên của mạng khỏi sự xâm nhập



Truy cập và sử dụng trái phép

- Các cách ngăn chặn truy cập và sử dụng trái phép
 - Chính sách sử dụng được chấp nhận (AUP)
 - Tắt chia sẻ tệp và máy in
 - Tường lửa
 - Phần mềm phát hiện xâm nhập



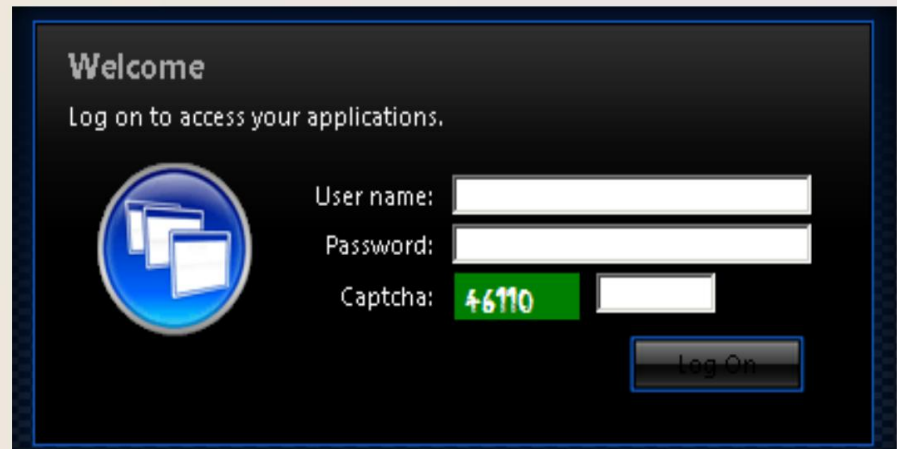
Truy cập và sử dụng trái phép

- **Kiểm soát truy cập** cho biết ai có thể truy cập máy tính, khi nào họ có thể truy cập, họ có thể thực hiện những hành động nào.
- Hai giai đoạn để truy cập hệ thống: **xác định** (định danh) và **xác thực** (xác thực)

Tên người dùng và mật khẩu

Passphrase

CAPTCHA



The image shows a Windows XP login screen. At the top, it says "Welcome" and "Log on to access your applications." Below this is a circular icon representing a user profile. To the right of the icon are three input fields: "User name:", "Password:", and "Captcha:". The "Captcha:" field contains the text "46110" in green. Below the input fields is a "Log On" button.

Truy cập và sử dụng trái phép

- Thiết bị **sinh trắc học** xác thực danh tính của một người bằng cách dịch đặc điểm cá nhân thành mã kỹ thuật số được so sánh với mã kỹ thuật số trong máy tính



Trộm cắp và phá hoại phần cứng

Ăn cắp phần cứng là hành
vi ăn cắp thiết bị
máy tính

Phá hoại phần cứng
là hành động làm xấu hoặc
phá hủy thiết bị máy
tính

Trộm cắp thông tin

- **Đánh cắp thông tin** xảy ra khi ai đó đánh cắp thông tin cá nhân hoặc bí mật
- **Mã hóa** là một quá trình chuyển đổi dữ liệu có thể đọc được thành các ký tự không thể đọc được để ngăn truy cập trái phép

Simple Encryption Algorithms			
Name	Algorithm	Plaintext	Ciphertext
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL
Expansion	Insert characters between existing characters	USER	UYSYEYRY
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN

Trộm cắp thông tin

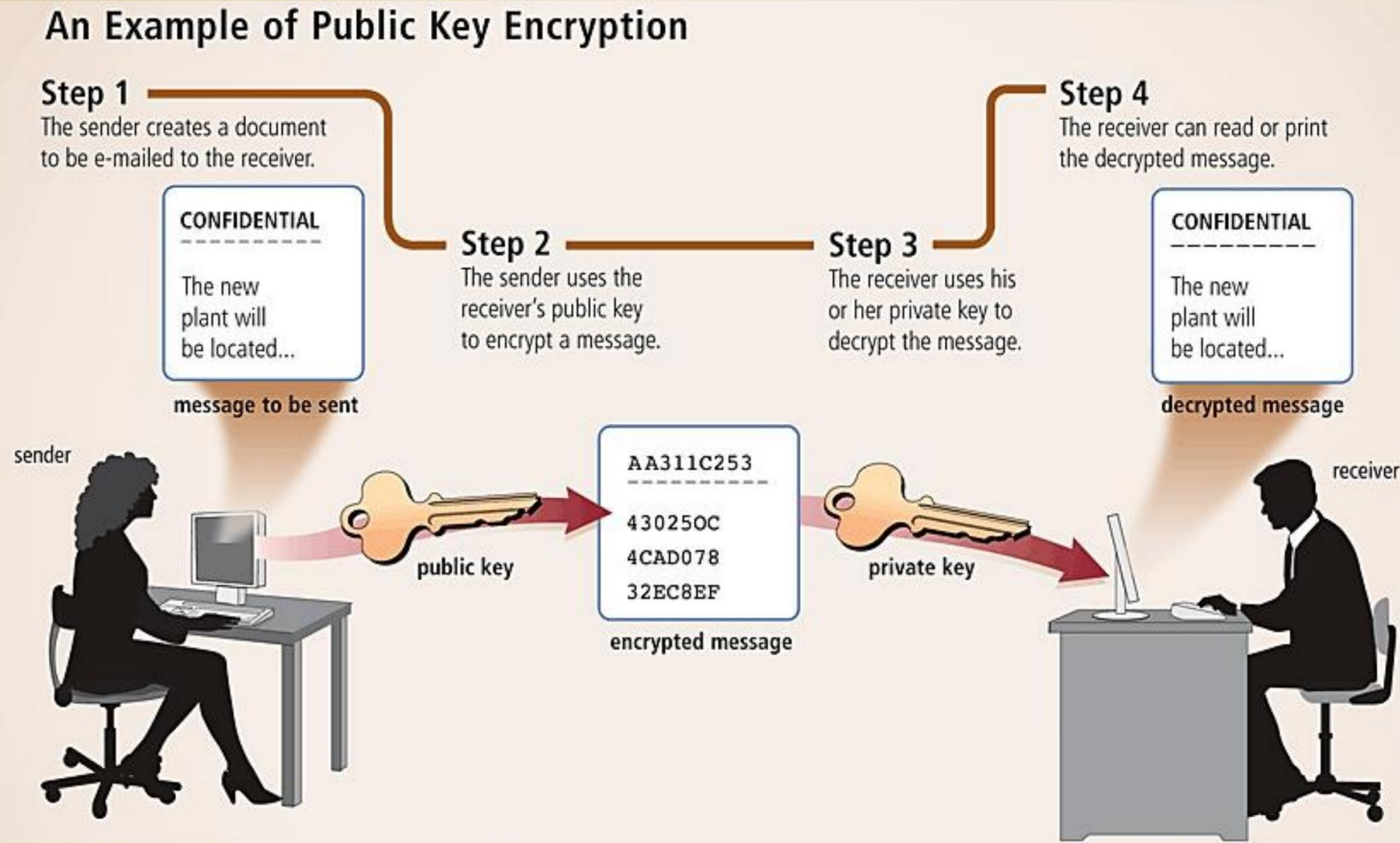
- **Mật mã đối xứng:** sử dụng cùng một khóa cho mã hóa và giải mã.



- **Mật mã không đối xứng:** sử dụng khóa công khai để mã hóa và khóa riêng để giải mã.



Trộm cắp thông tin



Trộm cắp thông tin

- Chữ **ký điện tử** là một mã được mã hóa được gắn vào một tin nhắn điện tử để xác minh danh tính của người gửi
- Các trình duyệt web và các trang Web sử dụng các kỹ thuật mã hóa (HTTPS) và chứng chỉ số.



Trộm cắp thông tin

- Trang web có HTTPS và chứng chỉ kỹ thuật số:



Trộm cắp thông tin

- Các kỹ thuật bảo mật phổ biến bao gồm

Điện tử
Chứng chỉ

Lớp vận chuyển
Bảo mật (TLS)

HTTP an toàn

VPN

Lỗi hệ thống

- Lỗi hệ thống là sự cố kéo dài của một máy vi tính
- Nhiều yếu tố có thể dẫn đến lỗi hệ thống, bao gồm:
 - Phần cứng lão hóa
 - Thiên tai
 - Sự cố về điện
 - Tiếng ồn, điện áp thấp và quá áp
 - Các lỗi trong chương trình máy tính

Lỗi hệ thống

- Hai cách để bảo vệ khỏi sự cố hệ thống do sự thay đổi nguồn điện bao gồm thiết bị **bảo vệ chống sét lan truyền** và **nguồn cung cấp điện liên tục**

(Bộ lưu điện)



Sao lưu - Biện pháp bảo vệ tối ưu

- Bản **sao lưu** là bản sao của tệp, chương trình hoặc dữ liệu có thể được sử dụng nếu bản gốc bị mất, bị hỏng hoặc bị phá hủy
 - Để **sao lưu** một tệp có nghĩa là tạo một bản sao của nó
- Các **bản sao lưu ngoại** tuyến được lưu trữ ở một vị trí tách biệt với trang máy tính



Bảo mật không dây

- Ngoài việc sử dụng tường lửa, một số biện pháp bảo vệ cải thiện tính bảo mật của mạng không dây:

Điểm truy cập không
dây không được phát
SSID

Thay đổi mặc định
SSID

Định cấu hình WAP để
chỉ một số thiết
bị nhất định có thể
truy cập nó

Sử dụng các tiêu chuẩn
bảo mật WPA hoặc WPA2

Health Concerns of Computer Use

- **Computer addiction** occurs when the computer consumes someone's entire social life
- Symptoms of users include:

Craves
computer
time

Overjoyed
when at the
computer

Unable to stop
computer
activity

Irritable when
not at the
computer

Neglects
family and
friends

Problems at
work or
school

Đạo đức và Xã hội

- Đạo đức máy tính là các nguyên tắc đạo đức chi phối việc sử dụng máy tính và hệ thống thông tin
- Độ chính xác của thông tin là một mối quan tâm
 - Không phải tất cả thông tin trên web là chính xác



Đạo đức và Xã hội

Quyền sở hữu trí tuệ là quyền mà người sáng tạo được hưởng đối với tác phẩm của họ

- Bản quyền bảo vệ mọi hình thức diễn đạt hữu hình

Quy tắc ứng xử CNTT là một hướng dẫn bằng văn bản giúp xác định xem một hành động cụ thể trên máy tính là hợp đạo đức hay phi đạo đức

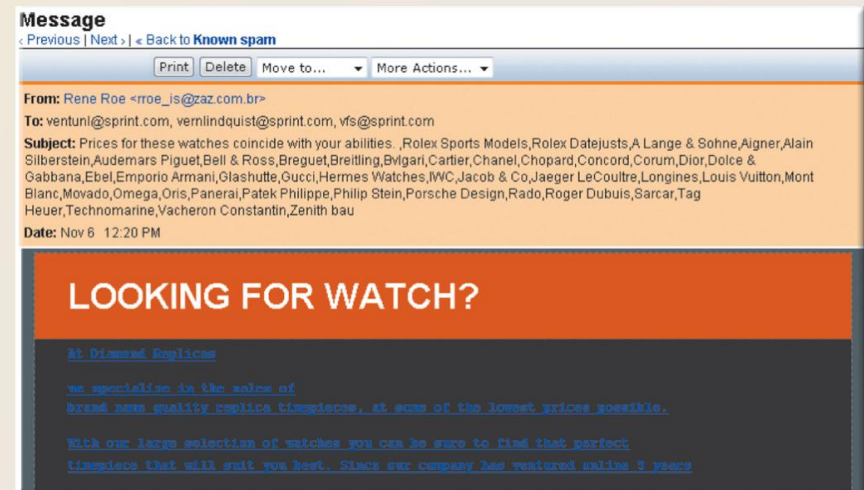
Đạo đức và Xã hội

How to Safeguard Personal Information

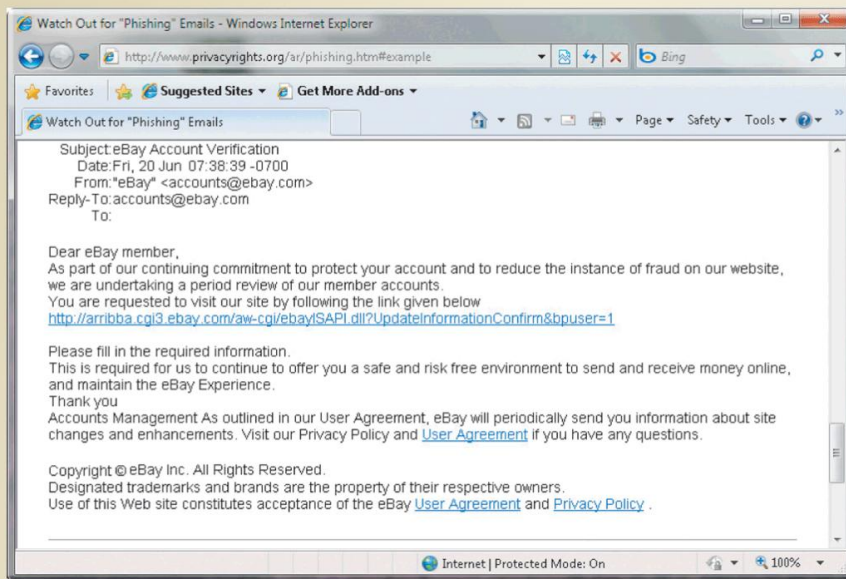
1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your telephone number or Social Security number on personal checks.
3. Have an unlisted or unpublished telephone number.
4. If Caller ID is available in your area, find out how to block your number from displaying on the receiver's system.
5. Do not write your telephone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, telephone numbers, Social Security numbers, and driver's license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping club and buyer cards.
9. If merchants ask personal questions, find out why they want to know before releasing the information.
10. Inform merchants that you do not want them to distribute your personal information.
11. Request, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to Web sites. Fill in only required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free e-mail account. Use this e-mail address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for e-mail filtering through your Internet access provider or use an anti-spam program such as Brightmail.
21. Do not reply to spam for any reason.
22. Surf the Web anonymously with a program such as Freedom WebSecure or through an anonymous Web site such as Anonymizer.com.

Đạo đức và Xã hội

- Spam là một tin nhắn e-mail không được yêu cầu hoặc bài đăng trong nhóm tin
- Các khối lọc e-mail tin nhắn e-mail từ các nguồn được chỉ định
- Các chương trình chống thư rác cố gắng loại bỏ thư rác trước khi nó đến hộp thư đến của bạn



Đạo đức và Xã hội



- **Lừa đảo** là một trò lừa đảo trong đó thủ phạm gửi một tin nhắn e-mail chính thức để cố gắng lấy thông tin cá nhân và tài chính của bạn
- **Dược phẩm** là một trò lừa đảo trong đó thủ phạm cố gắng lấy thông tin cá nhân và tài chính của bạn bằng cách giả mạo

Chapter Eleven

Computer Security and Safety, Ethics, and Privacy

Khám phá Máy tính 2012

Hướng dẫn tương tác của bạn
với thế giới kỹ thuật số

Chương 11 Hoàn thành

