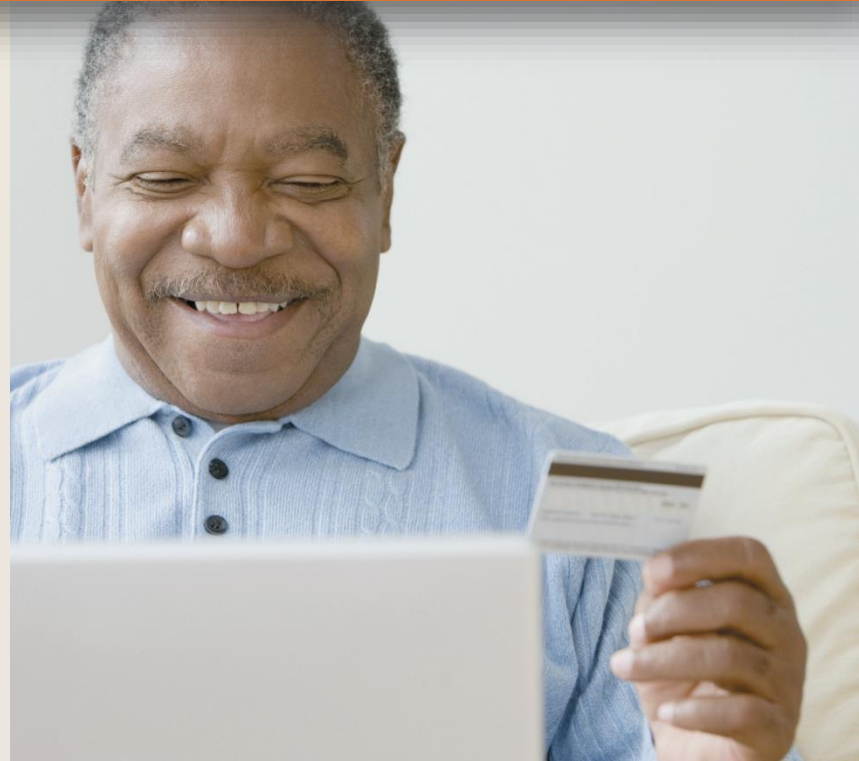


Computer Security and Safety, Ethics, and Privacy

Discovering Computers 2012

**Your Interactive Guide
to the Digital World**



Objectives Overview

Types of
cybercrime
perpetrators

Internet and
network attacks,
and ways to
safeguard

Unauthorized
computer access
and use

Hardware theft
and vandalism;
Software theft

Information
encryption

Nontechnical
concerns of
computer use

Computer Security Risks

- A computer security risk is any event that could cause a damage to computer.
- A ^{Tội phạm mạng} **cybercrime** is an online or Internet-based illegal act

Hackers

(access unauthorizedly)

Crackers

(access unauthorizedly
and damage)

Script Kiddies

(use readymade hacking
programs made by others)

Corporate Spies

Cyberterrorists
(damage computers for
political reasons)

Cyberextortionists

(use network as an offensive
force to demand money)

Computer Security Risks

- Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises



Internet and Network Attacks

- Malicious softwares (malware):

Computer Virus

- Attaches to a program, requires human action to spread.

Worm

- Copies itself repeatedly without human action, using up resources and may shut down computer

Trojan Horse

- A malicious program that looks like a legitimate program

Rootkit

- Program that hides its presence in a computer and enable administrator level access

Internet and Network Attacks

- An infected computer has one or more of the following symptoms:

Slow down

Less available
memory

Crashes

Pop-ups

New browser
homepage,
new toolbars

Unknown
programs
mysteriously
appear

System
properties
change

Operating
system shuts
down
unexpectedly

Internet and Network Attacks

Tips for Preventing Viruses and Other Malware

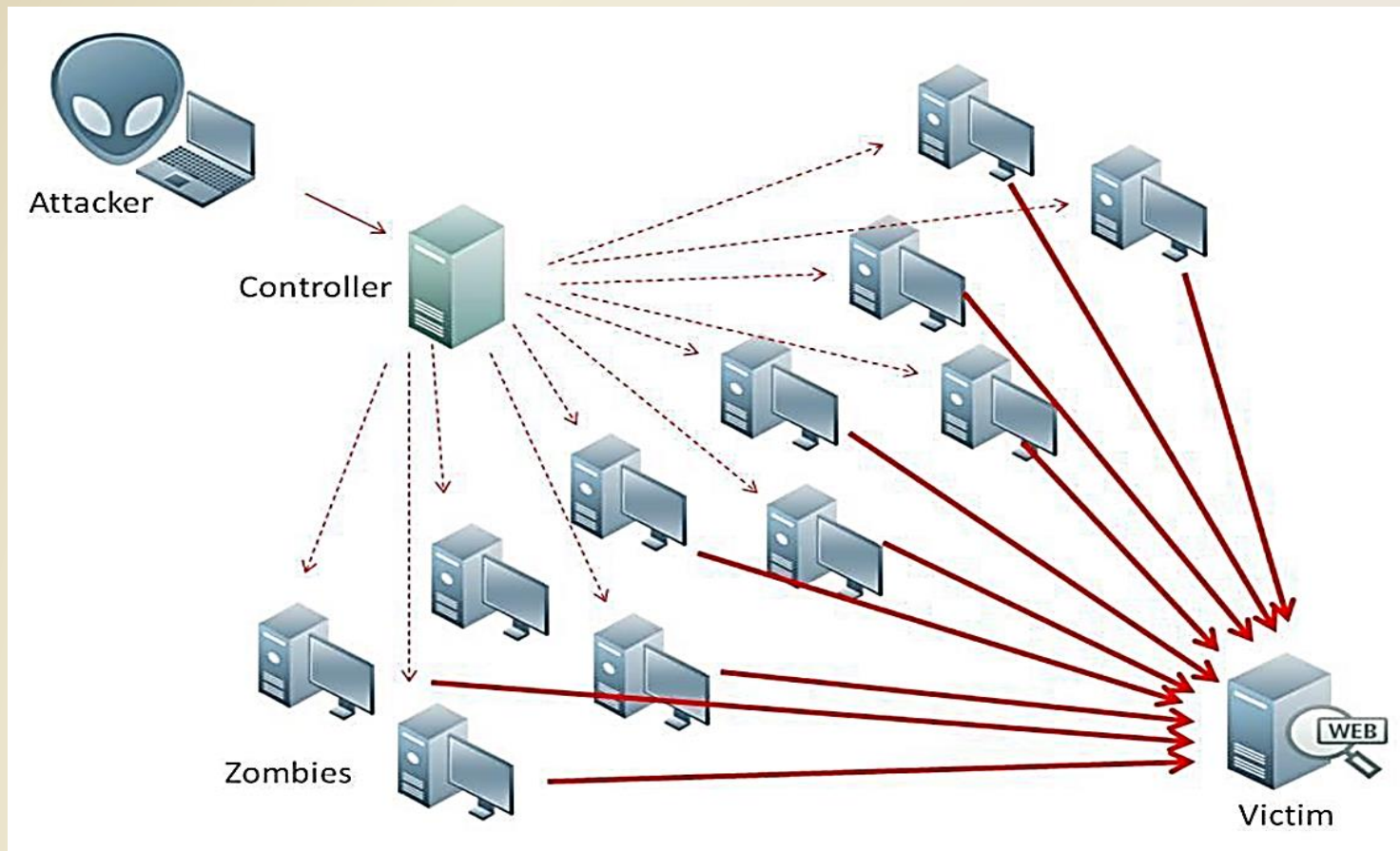
1. Never start a computer with **removable media** inserted, unless the media are uninfected.
2. Never open an **e-mail attachment** unless you expect it and it is from a trusted source.
3. Install an **antivirus program** on all of your computers. Update the software and the virus signature files regularly.
4. Scan all downloaded programs and plugged media for viruses and other malware.
5. If the antivirus program flags an e-mail attachment as infected, delete or quarantine the attachment immediately.
6. Install a personal **firewall** program.
7. Stay informed about new virus alerts and virus hoaxes.

Internet and Network Attacks

- A **botnet** is a group of interconnected computers that are *remote-controlled* by cybercriminals *without the owner's awareness*.
 - A compromised computer is known as a **zombie**
- A **denial of service attack (DoS attack)** makes an Internet service unavailable by *flooding the target* with traffic to trigger a crash.
 - Distributed DoS (**DDoS**)

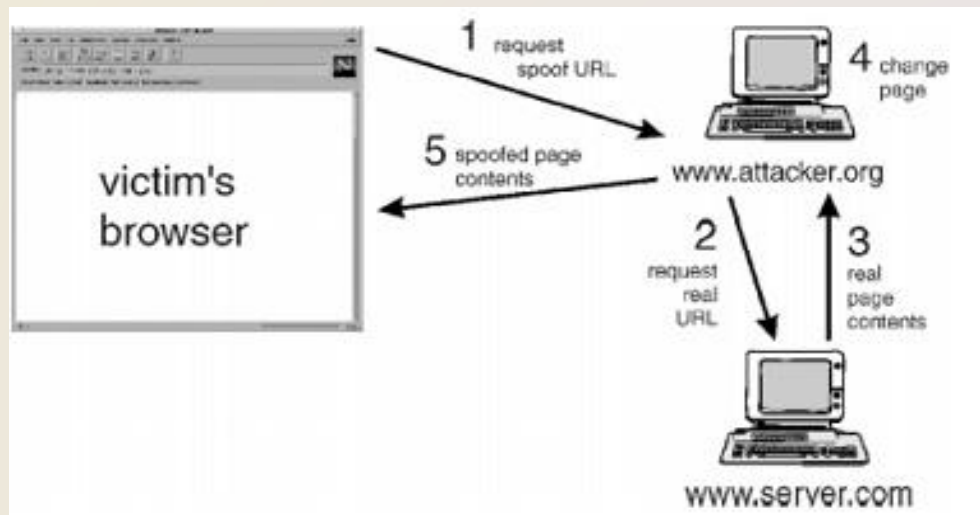
Internet and Network Attacks

- **DDoS** attacks are launched from **botnets (zombies)**:



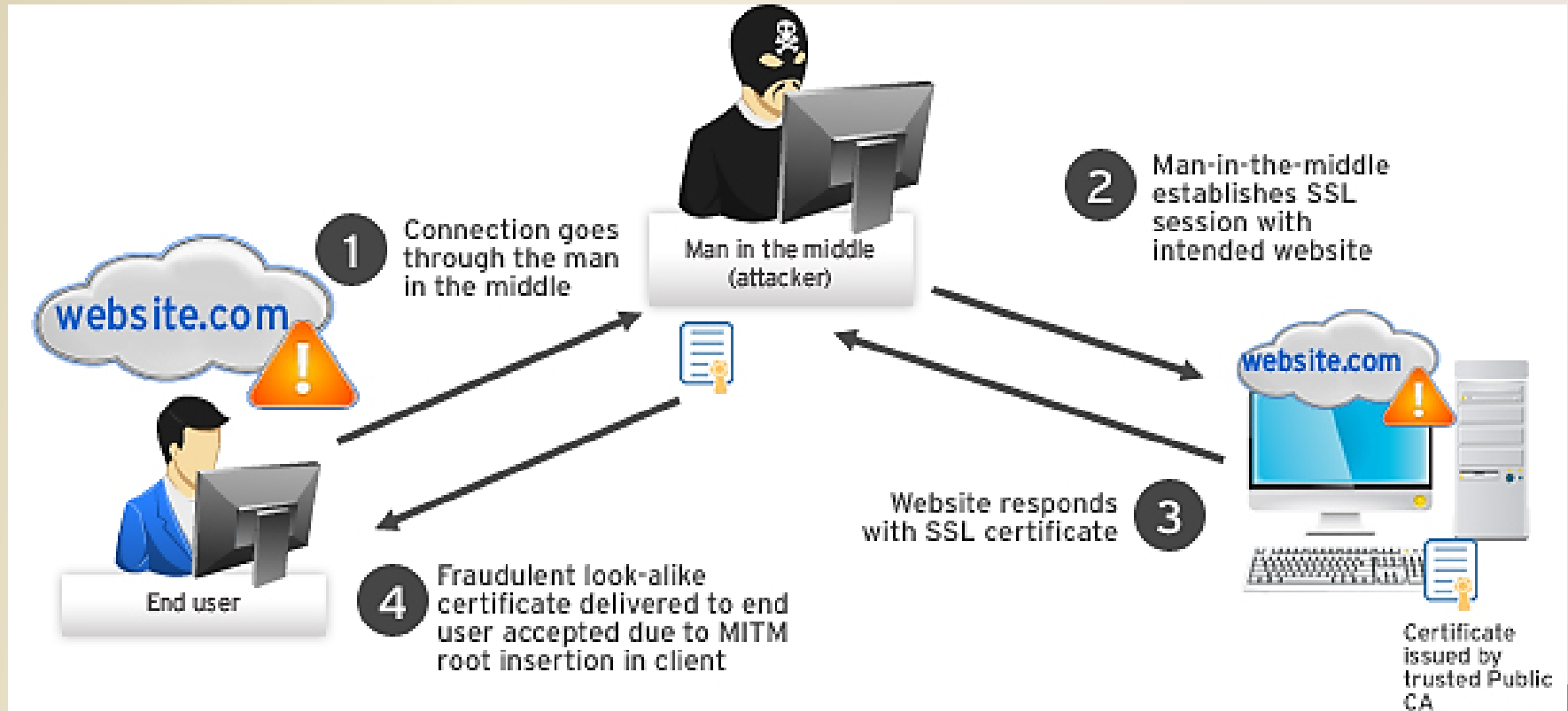
Internet and Network Attacks

- A **back door** is a program that allows users to *bypass normal authentication* and gain access.
- **Spoofing** is a technique intruders use to *make their Internet transmission appear legitimate*. E.g: email spoofing, web spoofing, IP spoofing.



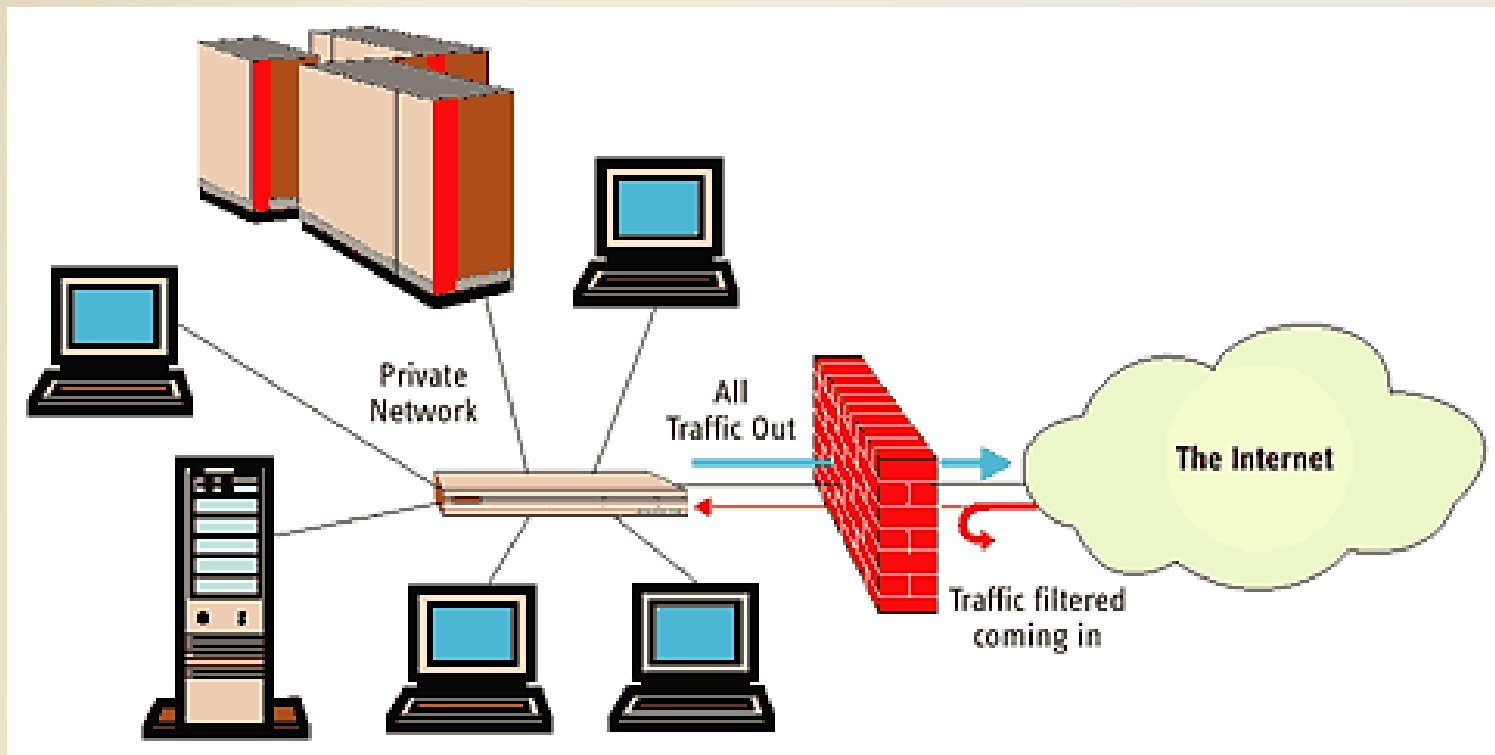
Internet and Network Attacks

- **Man-in-the-Middle (MITM):** attacker secretly relays and possibly alters the message between two parties.



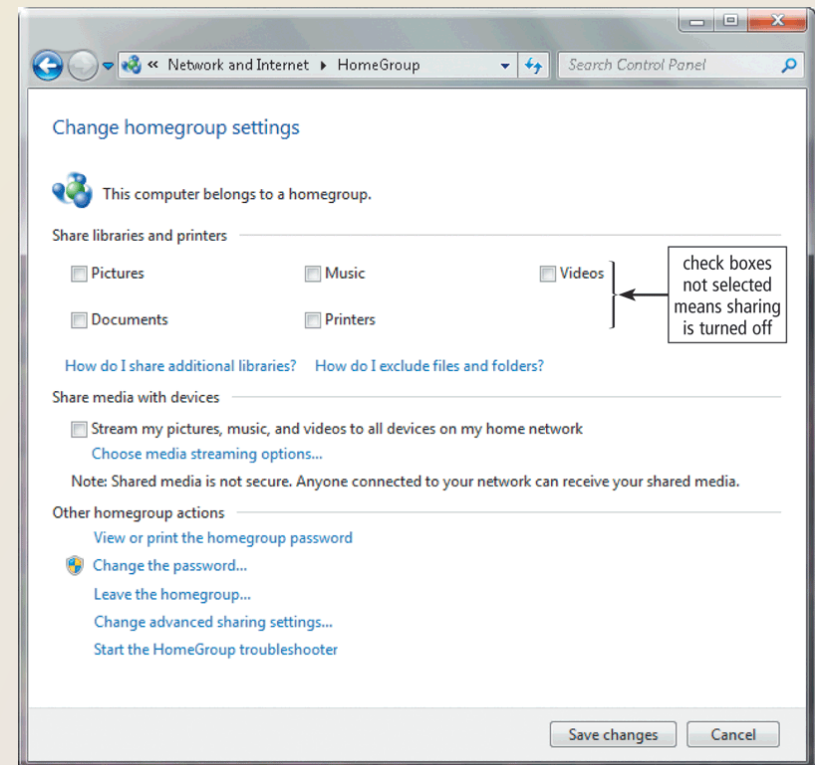
Internet and Network Attacks

- A **firewall** is hardware and/or software that protects a network's resources from intrusion



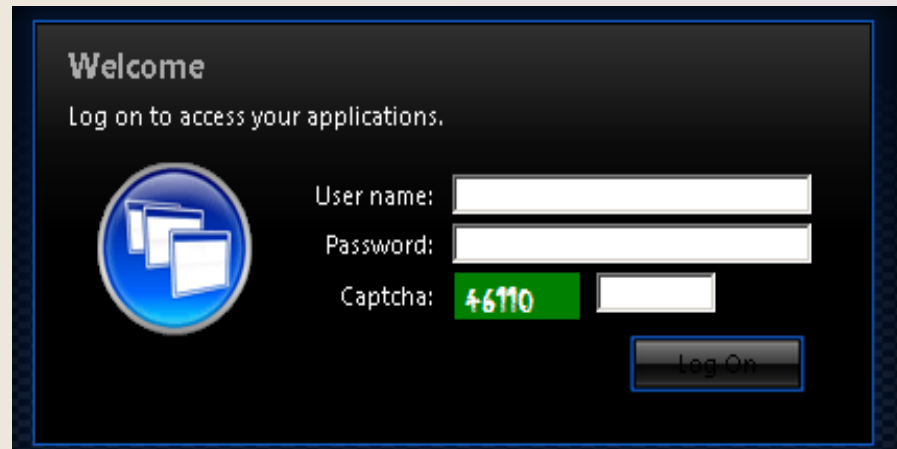
Unauthorized Access and Use

- Ways to **prevent unauthorized access and use**
 - Acceptable use policy (AUP)
 - Disable file and printer sharing
 - Firewalls
 - Intrusion detection software



Unauthorized Access and Use

- **Access controls** tell who can access a computer, when they can access, what actions they can take.
- Two-phases for accessing a system: **identification** (định danh) and **authentication** (xác thực)
 - ✓ User name & Password
 - ✓ Passphrase
 - ✓ CAPTCHA



Welcome
Log on to access your applications.

User name:

Password:

Captcha: 46110

Log On

Unauthorized Access and Use

- A **biometric device** authenticates a person's identity by translating a personal characteristic into a digital code that is compared with a digital code in a computer



Hardware Theft and Vandalism

Hardware theft is the act of stealing computer equipment

Hardware vandalism is the act of defacing or destroying computer equipment

Information Theft

- **Information theft** occurs when someone steals personal or confidential information
- **Encryption** is a process of converting readable data into unreadable characters to prevent unauthorized access

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	UYSYERYRY
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN

Information Theft

- **Symmetric cryptography:** use the same key for encryption and decryption.

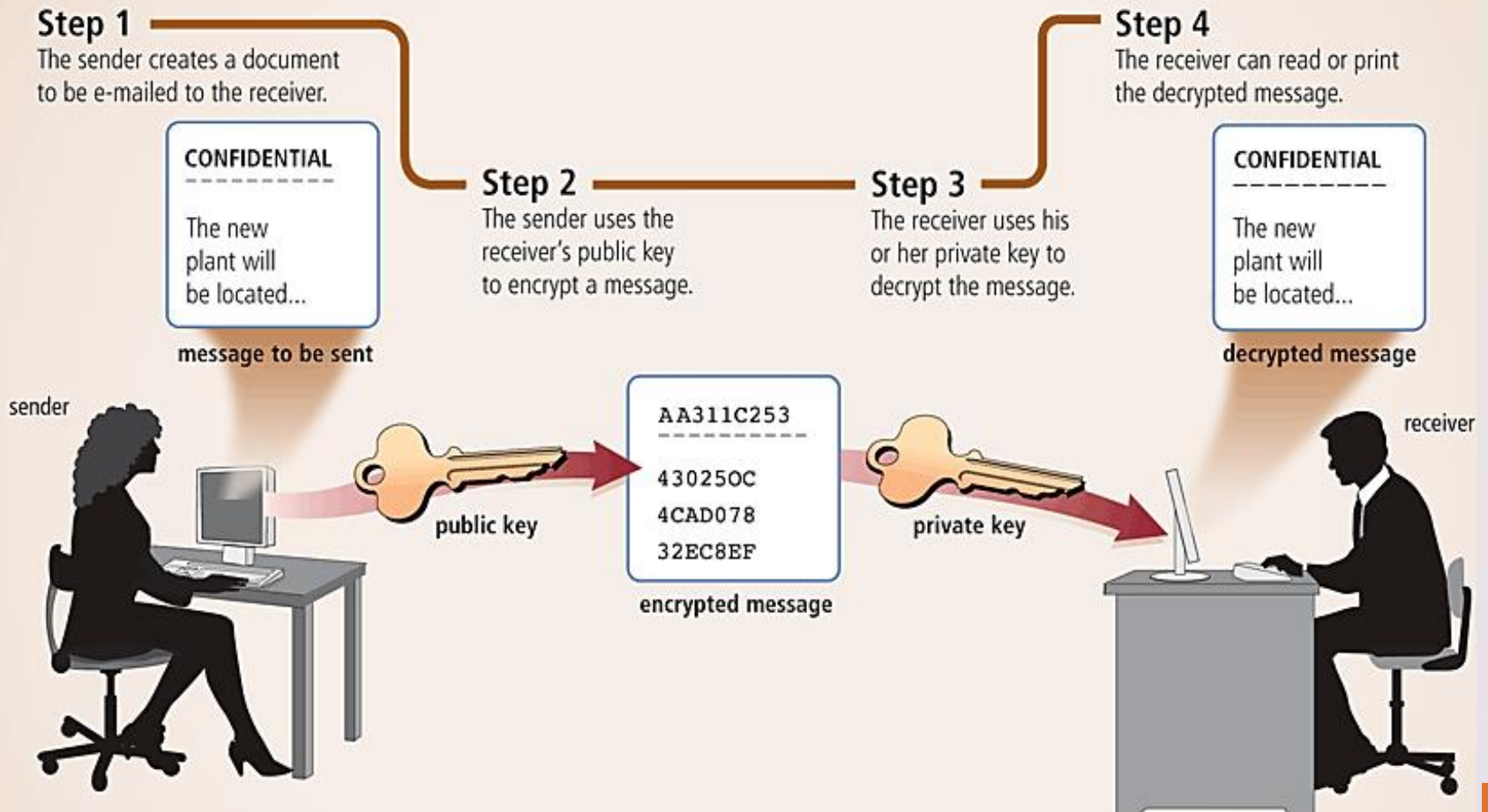


- **Asymmetric cryptography:** uses *public key* for encryption and *private key* for decryption.



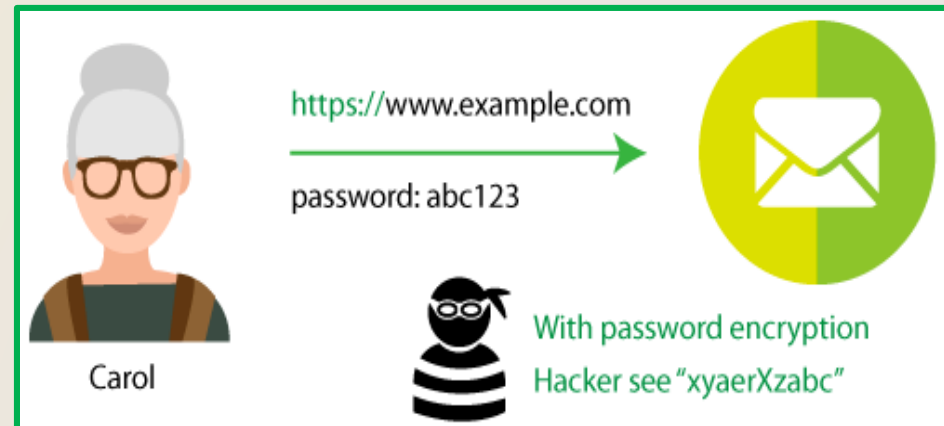
Information Theft

An Example of Public Key Encryption



Information Theft

- A **digital signature** is an *encrypted code* that is attaches to an electronic message *to verify the sender's identity*
- Web browsers and Web sites use encryption techniques (HTTPS) and digital certificate.



Information Theft

- Website with HTTPS and digital certificate:



Information Theft

- Popular security techniques include

**Digital
Certificates**

**Transport Layer
Security (TLS)**

Secure HTTP

VPN

System Failure

- A system failure is the prolonged malfunction of a computer
- A variety of factors can lead to system failure, including:
 - Aging hardware
 - Natural disasters
 - Electrical power problems
 - **Noise, undervoltages, and overvoltages**
 - Errors in computer programs

System Failure

- Two ways to protect from system failures caused by electrical power variations include **surge protectors** and **uninterruptible power supplies (UPS)**



Backing Up – The Ultimate Safeguard

- A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed
 - To **back up** a file means to make a copy of it
- **Offsite backups** are stored in a location separate from the computer site



Wireless Security

- In addition to using firewalls, some safeguards improve security of wireless networks:

A wireless access point should not broadcast an SSID

Change the default SSID

Configure a WAP so that only certain devices can access it

Use WPA or WPA2 security standards

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

Ethics and Society

- **Computer ethics** are the moral guidelines that govern the use of computers and information systems
- Information accuracy is a concern
 - Not all information on the Web is correct



Ethics and Society

Intellectual property rights are the rights to which creators are entitled for their work

- A **copyright** protects any tangible form of expression

An **IT code of conduct** is a written guideline that helps determine whether a specific computer action is ethical or unethical

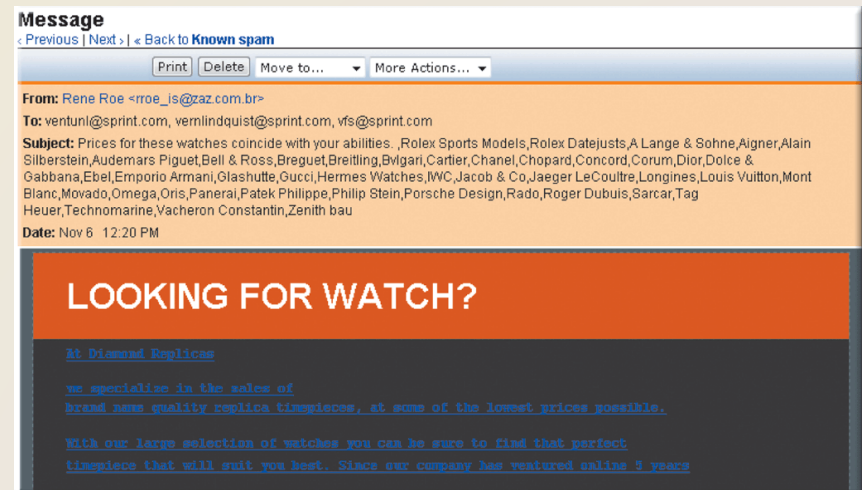
Ethics and Society

How to Safeguard Personal Information

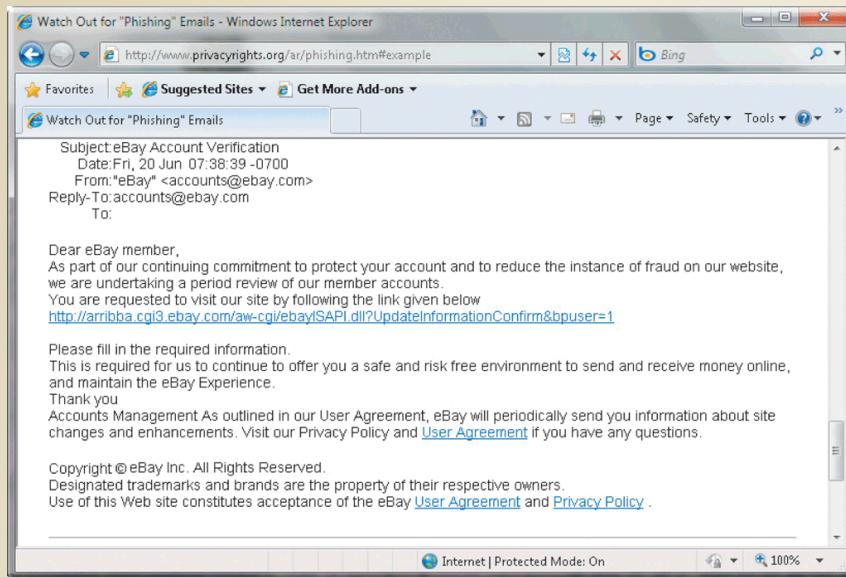
1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your telephone number or Social Security number on personal checks.
3. Have an unlisted or unpublished telephone number.
4. If Caller ID is available in your area, find out how to block your number from 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.

Ethics and Society

- **Spam** is an unsolicited e-mail message or newsgroup posting
- **E-mail filtering** blocks e-mail messages from designated sources
- **Anti-spam programs** attempt to remove spam before it reaches your inbox



Ethics and Society



- **Phishing** is a scam in which a perpetrator sends an official looking e-mail message that attempts to obtain your personal and financial information
- **Pharming** is a scam where a perpetrator attempts to obtain your personal and financial information via spoofing

Computer Security and Safety, Ethics, and Privacy

Discovering Computers 2012

**Your Interactive Guide
to the Digital World**

Chapter 11 Complete

