Cyber Crime Unit

The federal government has suffered a nearly 680 percent increase in cyber security breaches in the past six years.

Computer Security Risks

- A **computer security risk** is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability
- A **cybercrime** is an online or Internet-based illegal act

Hackers

Crackers

Script Kiddies

Corporate Spies

Unethical Employees

Cyberextortionists

Cyberterrorists

HACKER

Someone who gets into another persons computer or network **ILLEGALLY**.

Say their intent is to improve **SECURITY**.

Have advanced **COMPUTER** and **NETWORK** skills.

CRACKER

Someone who gets into another persons computer or network **ILLEGALLY**.

Their intent is to:

1. **GET RID OF** data

2. **STEAL** information

3.Other **SPITEFUL** acts.

Have advanced **COMPUTER** and **NETWORK** skills.

SCRIPT KIDDIE

Not as knowledgeable as a cracker but has the **SAME** intent.

Often use **PREWRITTEN** hacking and cracking software packages to crack into computers.

CYBEREXTORTIONIST

Uses **EMAIL** as a channel for **BLACKMAIL.** If they are not paid a sum of money, they threaten to:

1. **REVEAL** confidential material
2. **TAKE ADVANTAGE OF** a safety flaw
3. **BEGIN** an attack that will compromise a organization’s network

CYBERTERRORIST

They use the **INTERNET** or **NETWORK** to destroy or damage computers for **GOVERNMENTAL** motives.

Targets may be:

1. Nation's **AIR TRAFFIC** system
2. **ELECTRICITY**-generating companies
3. **TELECOMMUNICATION** infrastructure

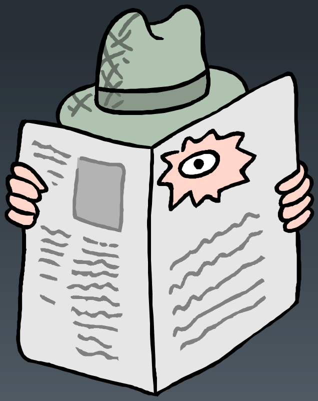
CORPORATE SPYS

Have **OUTSTANDING** computer and networking skills and are hired to break into a specific computer and **ROB** its exclusive **FILES** and information or to help identify **SAFETY** risks in their own **ORGANIZATION**.

Dishonest companies **EMPLOY** corporate spys.

CORPORATE ESPIONAGE

- When spies are hired to gain a **COMPETITIVE** advantage over other corporations.



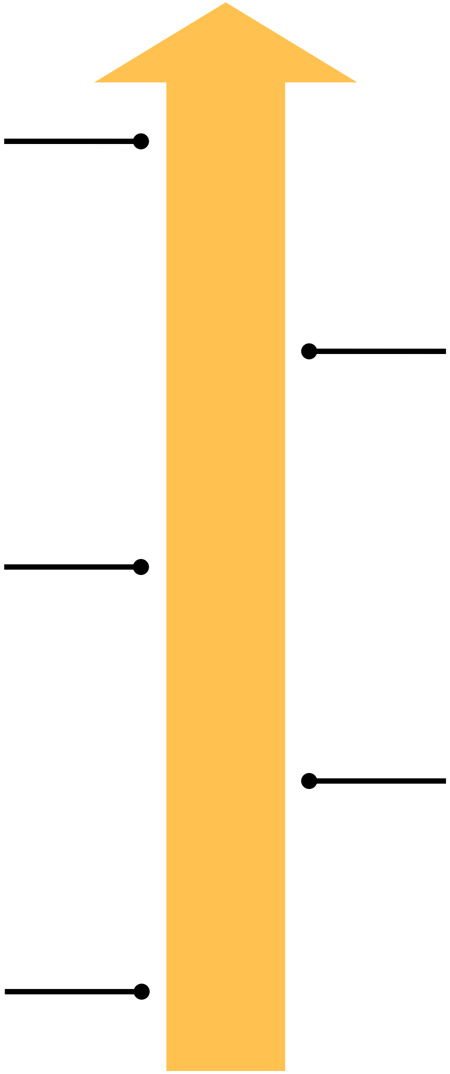
Computer Crime

Web Warriors – CBC Documentary

Link to video
http://www.youtube.com/watch?v=34cwMz3HZ8Q

Blaster Worm

1-10 minutes into film



Our most critical systems are connected to the internet through Microsoft software

Blaster Worm can infect your computer simply by being on-line

In the past, you had to open an attachment file to receive a virus

Self Activating

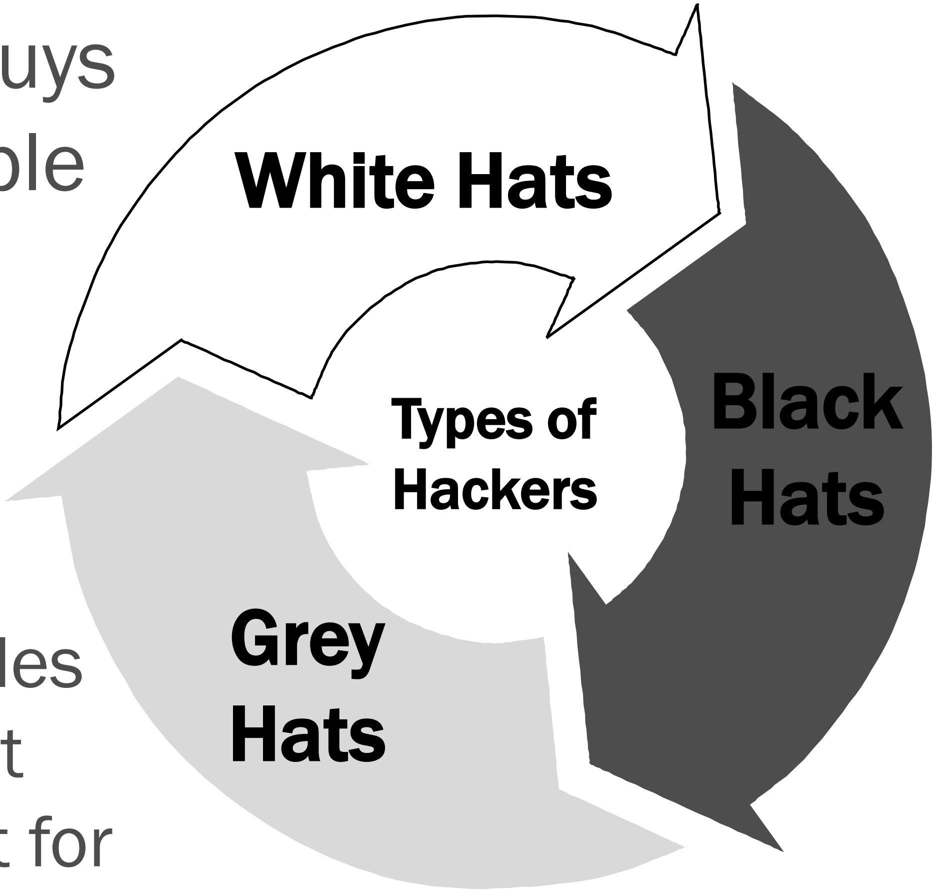
No specific target

3 Types of Hackers

The internet was not set-up to be secure
It was meant to share information between computers

White Hats

The Good Guys
The IT people



Black Hats

Bad Guys
Crooks that try to steal your credit card number etc.

Grey Hats

Work both sides of the street
Can be bought for hire

Donnie – The Hacker

- Donnie hacked into India’s critical infrastructure
- Within 5 minutes, he hacked into a major airline
- DEFCON, the largest internet convention
- The FBI go to DEFCON to learn about the newest hacking strategies

MafiaBoy

This segment of the video starts at 15:40

Mafiaboy

•Mafiaboy's real name is Michael Calce

•He was just **15** years old when he committed computer crime

•Michael took down big companies like CNN, Yahoo and eBay

•He sent a **Denial of Service** attack against the companies

- The newest type of computer virus is called **Storm Worm**
- It is always changing. Every time you disconnect you get a different copy
- **China** and **Russia** are particularly bad for creating viruses
- Warfare between countries involves sending viruses to attack banks and government offices

Denial of Service Attack

1. Describe what happens during a <u>denial of service attack</u>

- The hacker gains access to many large university computers
- Harness that power by sending many requests to a company such as yahoo.com
- The website can not handle all of those requests and it crashes

Russia

32-35 minutes into film

- **Russia** - the country of hacking
- The internet allowed the Russian mob to go global
- At the beginning of 2007, since the start of the internet, there were 250,000 viruses
- In 1 year, during 2007, it went from 250,000 viruses to 500,000 viruses

WoodPeckers and Storm Worm

36 minutes into film

- **Woodpeckers** – hammer keyboards very fast, trying to eliminate viruses

- **Storm Worm**, newest type of virus appears
- No one knows its purpose
- Doesn’t destroy anything – yet
- It’s always changing
- Every time you download it, you get a different copy

Storm Worm – continued...

- Turns a computer into a Zombie
- The author of the virus can control your computer remotely
- They harness they power of all the zombie computers together creating a Botnet

Cyber Warfare Between Nations

- Estonia is one of the most wired countries on earth
- 78% of the people bank on-line
- Within minutes hackers shut down their banks
- Many believe the attacks were politically motivated from Russia

China

Warfare Hacking

Recruiting

- The Chinese military is recruiting Hackers
- Why?

Internet

- They are using the internet rather than tanks
- How can the internet be used to attack a country?

Conclusion

- China is the country “we are most worried about.”

Cyber Warfare Between Nations

Information warfare

The use of information technologies to corrupt or destroy an enemy's information and industrial infrastructure

Network Warfare

Hacker-like attacks on the nation's network infrastructure, including the electronic banking system

Structural Sabatoge

Attacks on information systems that support transportation, finance, energy and telecommunications

Cyber Wars

- Cyber Security's definition is constantly evolving/changing.
- It always relates to the protection of computers and the information stored on them.
- Since networks are constantly expanding, it's hard to combat cyber crime.

Cyber Wars

- McAfee is a provider of security products and services that help secure systems and networks.
- Current customers of internet security include: the National Security Agency, the Department of Defence and other federal defence and law enforcement agencies.

How Hackers Stole $45 Million in 2 Days

1. Describe **Phase 1**
2. Describe **Phase 2**
3. Describe **Phase 3**
4. How could this have been prevented? (Outline the 3 ways)

Link to article
http://mashable.com/2013/05/25/45-million-stolen/

5 Biggest Computer Viruses of All Time

- What are the names of the 5 viruses?
- Click on each **virus** and describe…

1. What was it
2. How it worked
3. How it spread

Link to interactive infographic

http://mashable.com/2013/11/20/5-biggest-computer-viruses-all-time/

Microsoft and FBI Take Down Global Cyber Crime Ring

1. How much damage did the **Botnet** cause?
2. Where do they think the hackers reside?
3. Do they know who is responsible for creating this Botnet?
4. How has the **Citadel malware** spread?
5. Where are botnets mainly located?

Link to article

http://mashable.com/2013/06/06/microsoft-fbi-botnets/

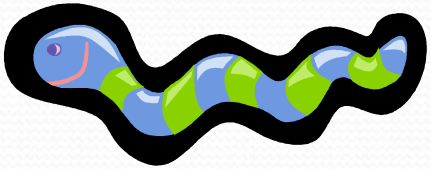
COMPUTER VIRUSES, WORMS, TROJAN HORSES, AND ROOTKITS

- A COMPUTER VIRUS IS A POTENTIALLY **DAMAGING** COMPUTER PROGRAM THAT AFFECTS, OR **INFECTS**, A COMPUTER **ADVERSELY** BY CHANGING THE WAY THE COMPUTER WORKS **WITHOUT** THE USER'S AWARENESS OR **APPROVAL.**

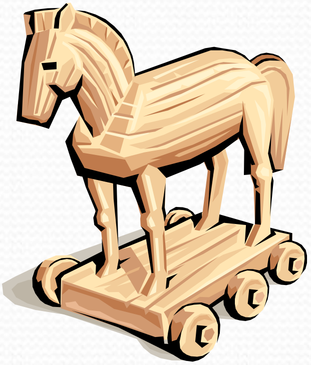
WORM

- PROGRAM THAT **COPIES** ITSELF

CONTINUALLY USING RESOURCES AND POSSIBLY **SHUTTING** DOWN THE COMPUTER OR NETWORK.



TROJAN HORSE



- NAMED AFTER THE **GREEK** MYTH.
- PROGRAM THAT **HIDES** WITHIN OR LOOKS LIKE A GENUINE PROGRAM.
- CERTAIN CONDITION OR ACTION THAT TRIGGERS THE TROJAN HORSE DOES NOT **REPEAT** ITSELF TO OTHER COMPUTERS.

ROOTKIT

- PROGRAM THAT **BURIES** IN A COMPUTER AND ALLOWS SOMEONE FROM A **DISTANT** LOCATION TO TAKE FULL **CONTROL** OF THE COMPUTER.
- CAN BE USED IN **LAW** ENFORCEMENT.
- USE IN **EVIL** AND **ILLEGAL** ACTIVITIES GROWING.

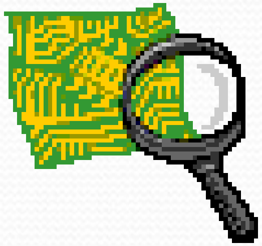
- VIRUSES, WORMS, TROJAN HORSES, AND ROOTKITS ARE CLASSIFIED AS **MALWARE.**
- MALWARE SHORT FOR **MALICIOUS** SOFTWARE.

MALWARE

- PROGRAMS THAT ACT WITHOUT A USER'S **KNOWLEDGE** AND **INTENTIONALLY** ALTER THE COMPUTER'S OPERATIONS.

OTHER CLASSES OF MALWARE:

- **BACK DOORS**
- **SPYWARE**



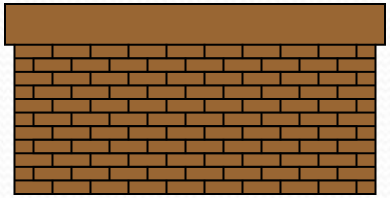
SPOOFING

- A **SYSTEM** INTRUDERS USE TO MAKE THEIR NETWORK OR INTERNET TRANSMISSION APPEAR LEGITIMATE TO A VICTIM COMPUTER OR NETWORK.

FIREWALLS

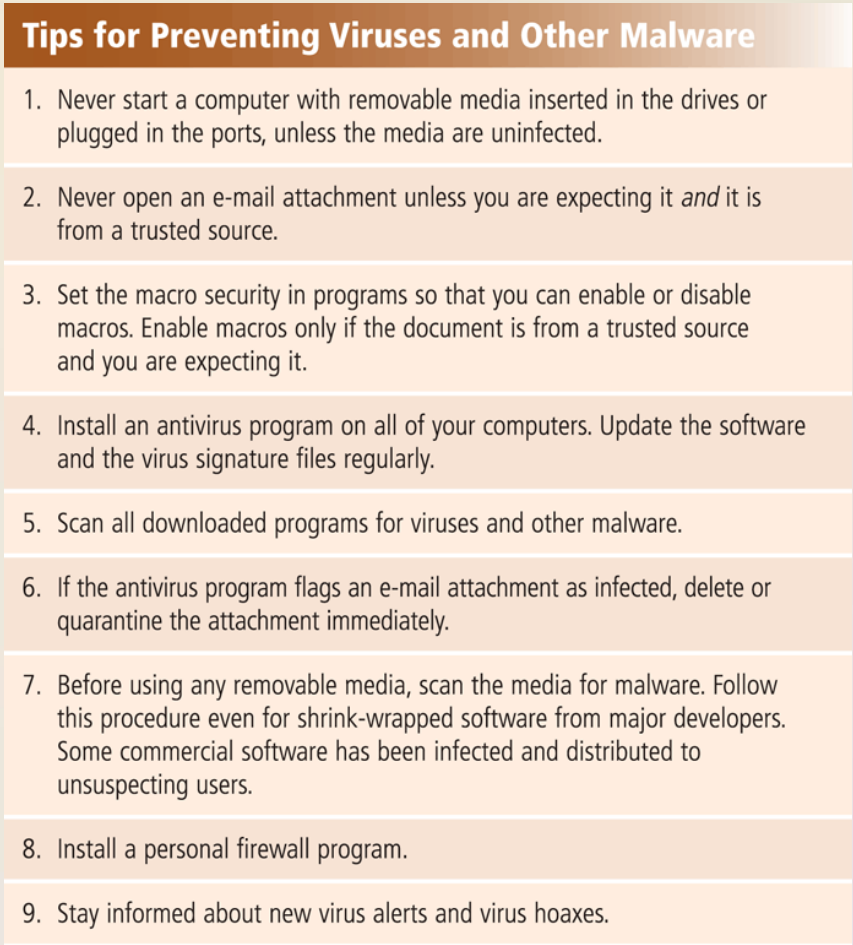
- **HARDWARE** AND/OR **SOFTWARE** THAT PROTECTS A NETWORK'S RESOURCES FROM

INTRUSION BY USERS ON ANOTHER NETWORK.



Internet and Network Attacks

- Users can take several precautions to protect their home and work computers and mobile devices from these malicious infections

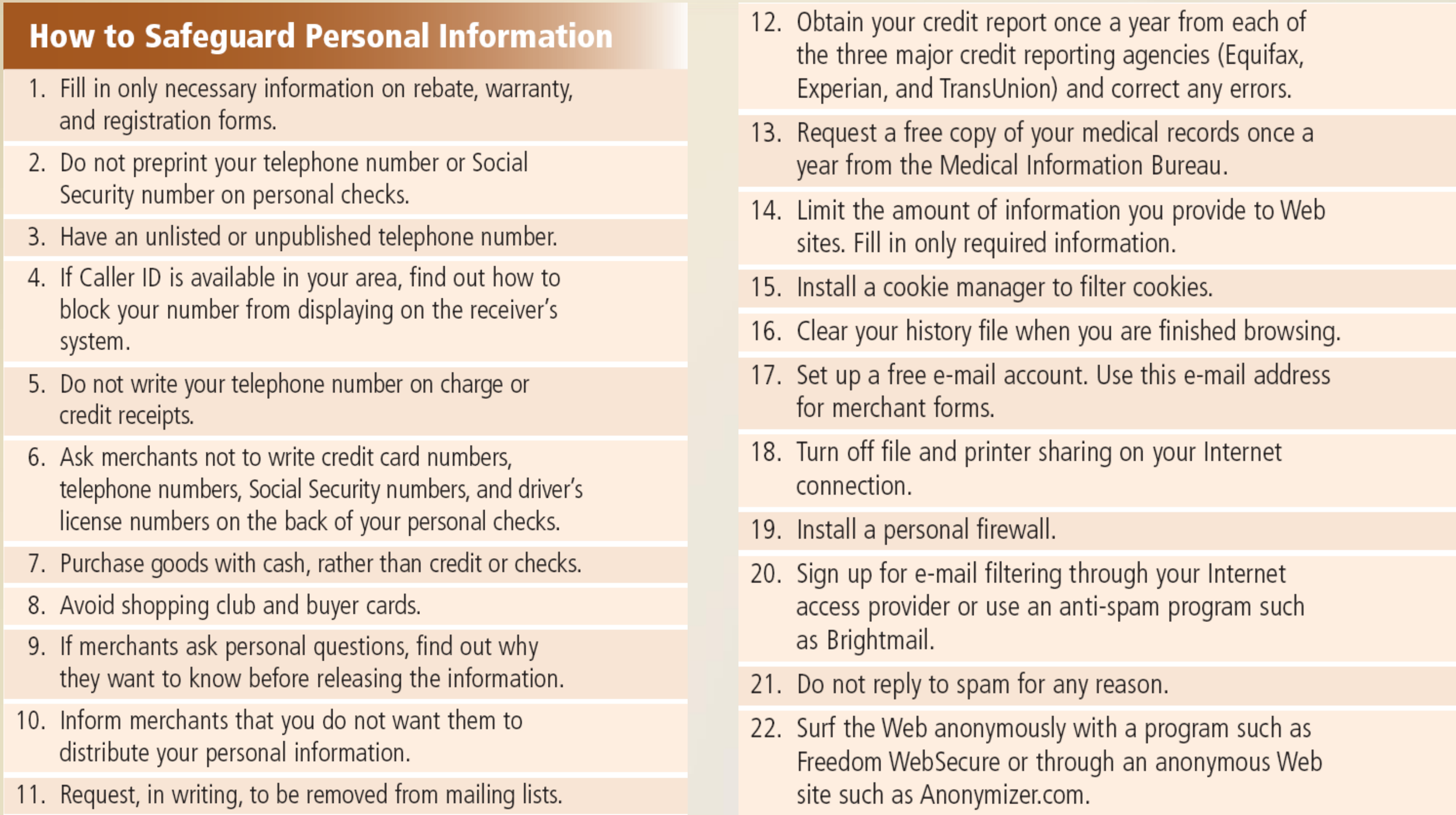


Tips for Preventing Viruses and Other Malware

1. Never start a computer with removable media inserted in the drives or plugged in the ports, unless the media are uninfected.
2. Never open an e-mail attachment unless you are expecting it *and* it is from a trusted source.
3. Set the macro security in programs so that you can enable or disable macros. Enable macros only if the document is from a trusted source and you are expecting it.
4. Install an antivirus program on all of your computers. Update the software and the virus signature files regularly.
5. Scan all downloaded programs for viruses and other malware.
6. If the antivirus program flags an e-mail attachment as infected, delete or quarantine the attachment immediately.
7. Before using any removable media, scan the media for malware. Follow this procedure even for shrink-wrapped software from major developers. Some commercial software has been infected and distributed to unsuspecting users.
8. Install a personal firewall program.
9. Stay informed about new virus alerts and virus hoaxes.

Page 560 – 561
Figure 11-7

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.

Page 584
Figure 11-31

Ethics and Society

- A **cookie** is a small text file that a Web server stores on your computer
- Web sites use cookies for a variety of reasons:

Allow for personalization

Store users' passwords

Assist with online shopping

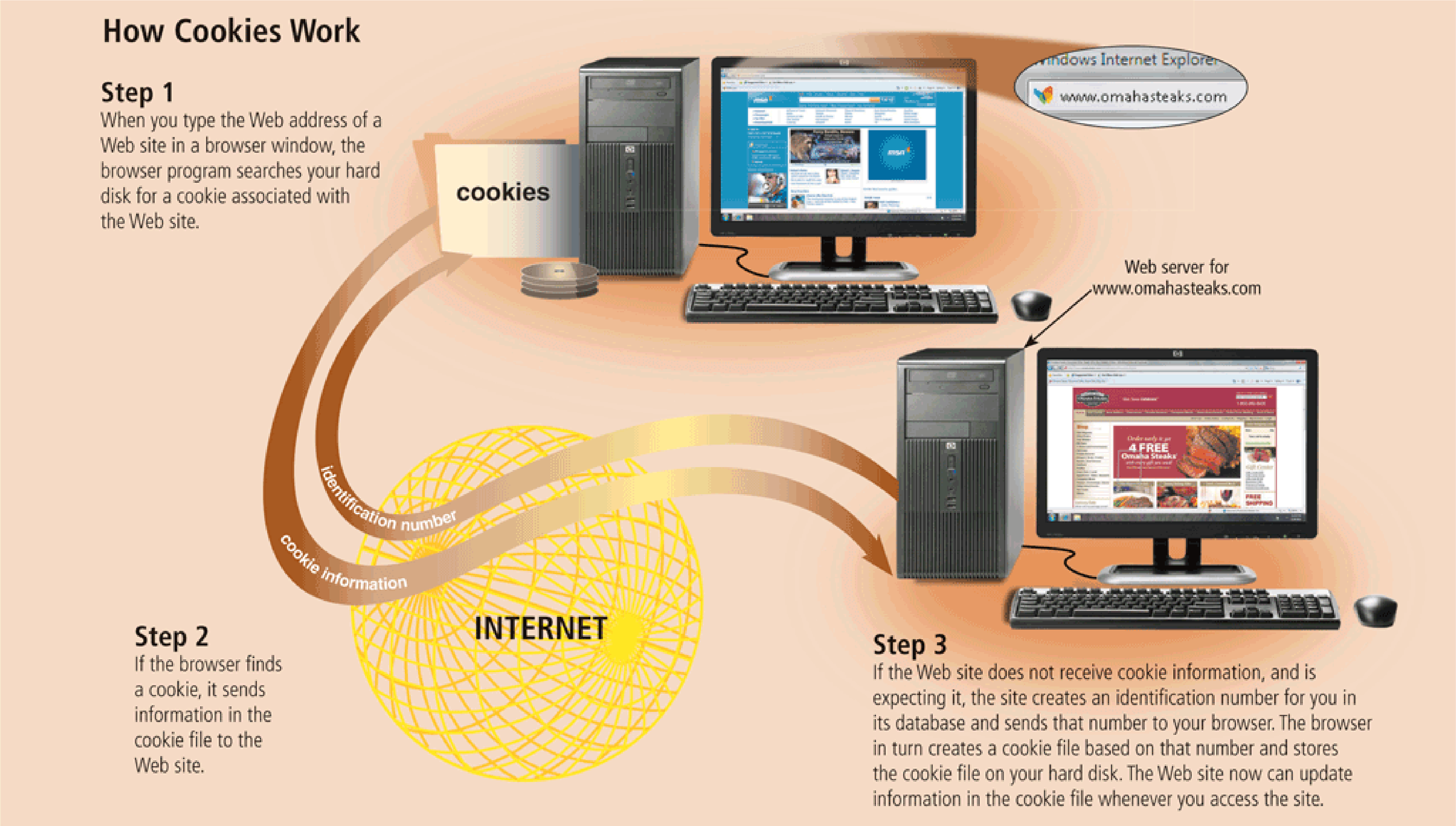
Track how often users visit a site

Target advertisements

Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Cookies below Chapter 11

Pages 585 – 586

Ethics and Society



How Cookies Work

Step 1
When you type the Web address of a Web site in a browser window, the browser program searches your hard disk for a cookie associated with the Web site.

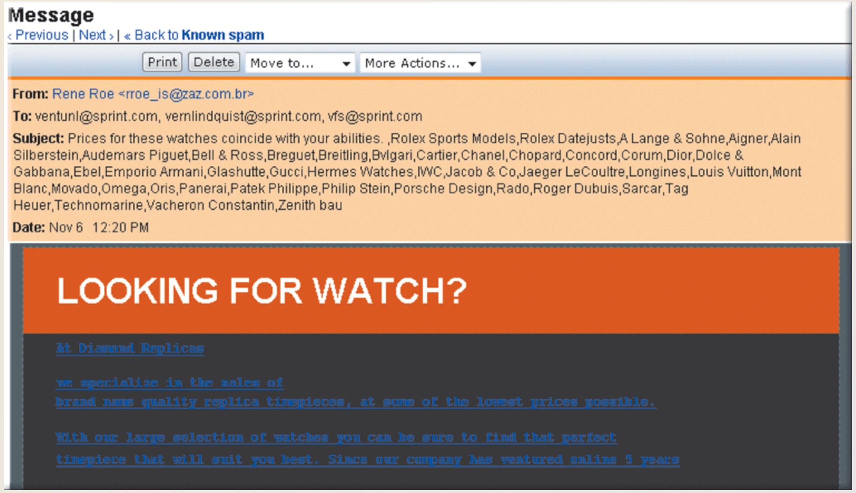
Step 2
If the browser finds a cookie, it sends information in the cookie file to the Web site.

Step 3
If the Web site does not receive cookie information, and is expecting it, the site creates an identification number for you in its database and sends that number to your browser. The browser in turn creates a cookie file based on that number and stores the cookie file on your hard disk. The Web site now can update information in the cookie file whenever you access the site.

Page 586
Figure 11-33

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



From: Rene Roe <rroe_is@zaz.com.br>

To: ventunl@sprint.com, vernlindquist@sprint.com, vfs@sprint.com

Subject: Prices for these watches coincide with your abilities. ,Rolex Sports Models,Rolex Datejusts,A Lange & Sohne,Aigner,Alain Silberstein,Audemars Piguet,Bell & Ross,Breguet,Breitling,Bvlgari,Cartier,Chanel,Chopard,Concord,Corum,Dior,Dolce & Gabbana,Ebel,Emporio Armani,Glashutte,Gucci,Hermes Watches,IWC,Jacob & Co,Jaeger LeCoultre,Longines,Louis Vuitton,Mont Blanc,Movado,Omega,Oris,Panerai,Patek Philippe,Philip Stein,Porsche Design,Rado,Roger Dubuis,Sarcar,Tag Heuer,Technomarine,Vacheron Constantin,Zenith bau

Date: Nov 6 12:20 PM

LOOKING FOR WATCH?

At Diamond Replicas

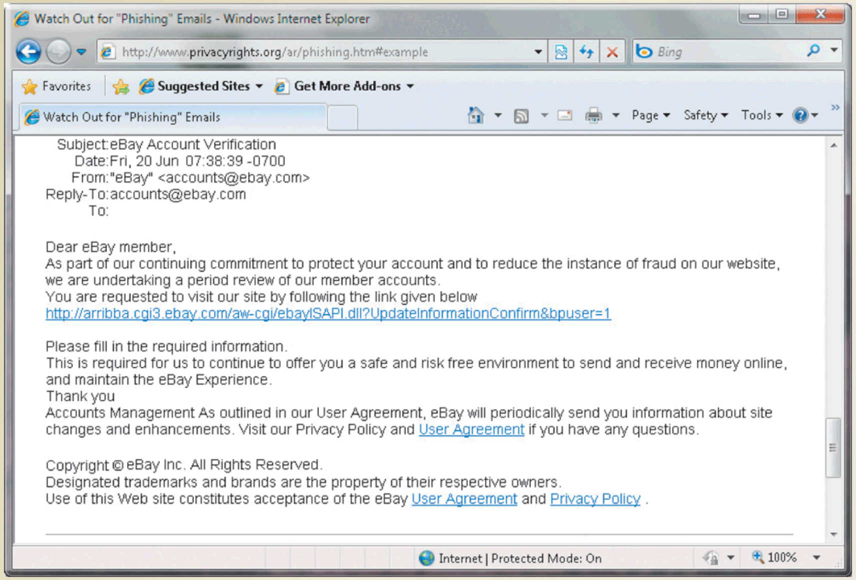
we specialize in the sales of
brand name quality replica timepieces, at some of the lowest prices possible.

With our large selection of watches you can be sure to find that perfect
timepiece that will suit you best. Since our company has ventured online 5 years

Page 587
Figure 11-34

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


Watch Out for "Phishing" Emails - Windows Internet Explorer
http://www.privacyrights.org/ar/phishing.htm#example
Bing
Favorites
Suggested Sites
Get More Add-ons
Watch Out for "Phishing" Emails
Page
Safety
Tools
Internet | Protected Mode: On
100%

Subject:eBay Account Verification
Date:Fri, 20 Jun 07:38:39 -0700
From:"eBay" <accounts@ebay.com>
Reply-To:accounts@ebay.com
To:

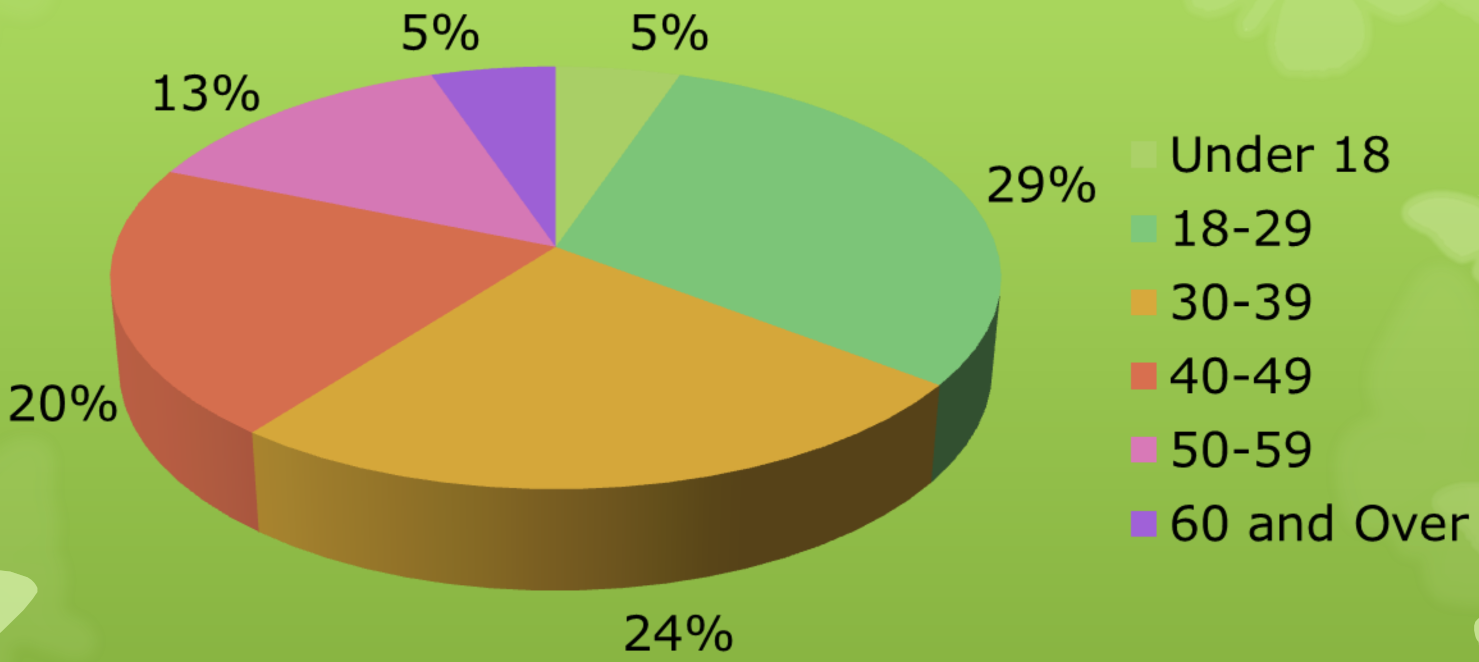
Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
You are requested to visit our site by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1

Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy .

Pages 587 - 588
Figure 11-35

IDENTITY THEFT
Complaints by Victims Age



Passwords

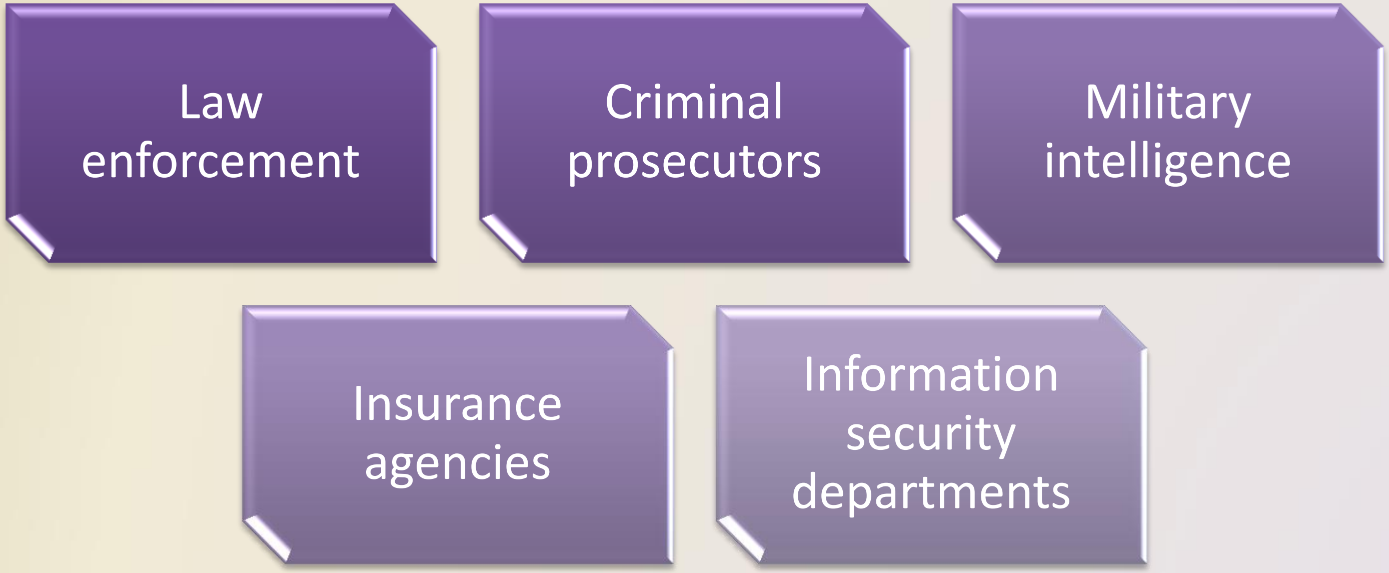
- Change every couple months
- Make all different for different accounts
- At least 7 characters
- Use capitals, numbers, symbols, etc.
- Don’t tell people!

Link to article: Russians Steal 1.2 Billion Internet Passwords!

http://mashable.com/2013/05/25/45-million-stolen/

Unauthorized Access and Use

- **Digital forensics** is the discovery, collection, and analysis of evidence found on computers and networks
- Many areas use digital forensics



Law enforcement

Criminal prosecutors

Military intelligence

Insurance agencies

Information security departments