

Computer Ethics & Security

Assoc. Prof. Pannipa Phaiboonnimit
and Dr. Noparut Wanichanaan

Adapted for English Section by
Kittipitch Kuptavanich
and Prakarn Unachak



Computer Ethics

Ethics

- **Code of practice adopted/ agreed upon by a profession or organizations to regulate that profession/group.**
- **AKA code of responsibility**
- **Which will**
 - ▶ **Discuss difficult issues, difficult decisions**
 - ▶ **Provide a clear account of what behavior is considered "ethical" or "correct" or "right"**

Why Ethics for Using Computer Systems?

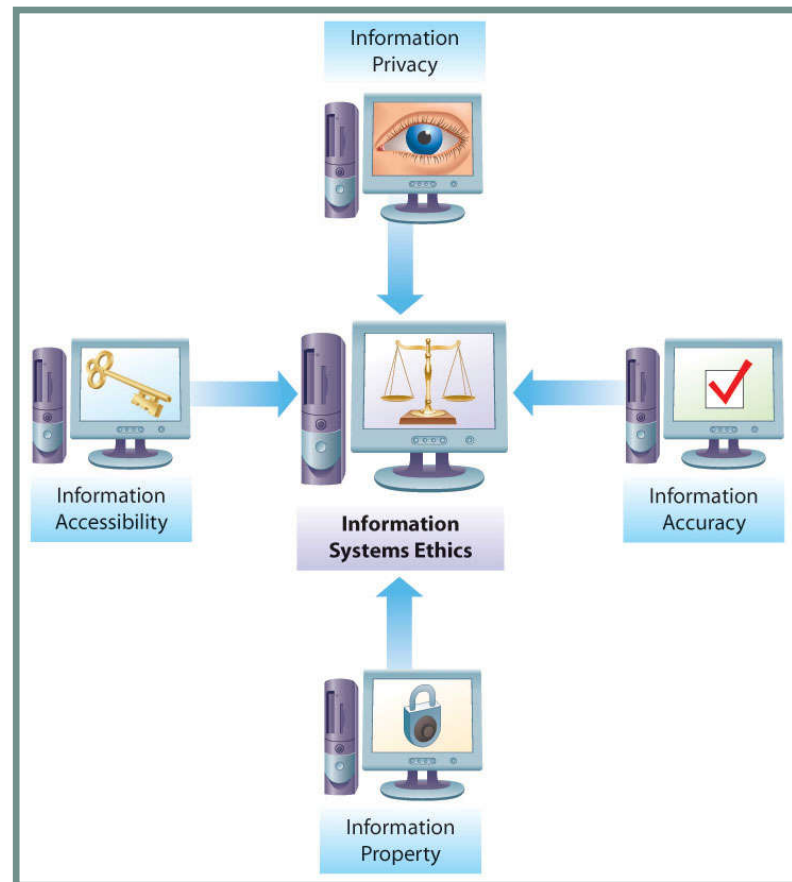
- **Computers are becoming greater part in many aspects of our lives**
 - ▶ **Banking**
 - ▶ **Medical System**
 - ▶ **Personal Information**
 - ▶ **Governmental Databases**
 - ▶ **Social Media**
- **Access and use to these information can affect the owner of such information, for good and/or for ill.**
 - ▶ **With the effect becomes larger and more widespread in modern time**
- **Hence, the need for ethics.**



4 Issues in Information System Ethics*

PAPA

- Information **P**rivacy
- Information **A**ccuracy
- Information **P**roperty
- Information **A**ccessibility



*Richard O. Mason, **Four Ethical Issues of the Information Age**, *MIS Quarterly*, Vol. 10, No. 1 (Mar., 1986), pp. 5-12



Information Privacy

➤ Which piece of information should you have to reveal?

▶ To whom?

▶ Any safeguard?

➤ Information you should keep private:

▶ Family History

▶ Medical History

▶ Identification Information (ID numbers, Birth Date)

▶ Location

▶ Account and password information



Information Privacy (cont.)

- **Channel of Privacy Loss**
 - ▶ Automatic System such as Trojan/Spyware
 - ▶ Privacy Setting on Social Network
- **Result of Privacy Loss**
 - ▶ Cyberstalking
 - ▶ Exhortions
 - ▶ Identity Theft
 - ❖ Fastest growing “information” crime
 - ▶ Other use/misuse of personal information
 - ❖ Employer might use your Social Media information to not hire you



Information Accuracy

- **Ensuring of the authenticity and fidelity of information**
 - ▶ **“Does this information make sense?”**
 - ▶ **“Is this information correct?”**
 - ▶ **“Is this information from credible source?”**
- **High costs of incorrect information**
 - ▶ **Banks**
 - ▶ **Hospitals**
- **Difficult to track down the person who made the mistake**



Credibility of Information



Information Property

- **Who owns information about individuals/ products?**
- **How can this information be sold and exchanged?**
- **Data Ownership**
- **Intellectual Property**



Information Accessibility

- Who has the right to access a piece of information?
 - ▶ Under what condition?
 - ▶ At what level (e-mail subject, contents, etc.)
 - ▶ What can be done with the information?
 - ▶ Any Safeguard?
- **Example: system administrators can access users' data in the system, but need to be limited by code of conducts**
- Who has to right to block access to a piece of information?
- When can data be monitored?



Consent Form & Data Privacy Statements

- Cover data access and data property
- **Consent form** is a statement allowing company access and use of customers' data as dictated by **data privacy statements** (or **term & conditions**)
- **Data privacy statements** entails what company can do with collected data (still has to be legal use!)
- Company maintaining the database with customer information legally owns it
 - ▶ Is free to sell it
 - ▶ Cannot sell information it agreed not to share
 - ▶ Must ensure proper data handling practices

IT Laws in Thailand

- **Electronic Transactions Law**
- **Electronic Signatures Law**
- **National Information Infrastructure Law**
- **Data Protection Law**
- **Computer Crime Law (updated 2017)**
- **Electronic Funds Transfer Law**



Computer Crime Law of 2017

What is illegal?

- **Unauthorized access**
- **Unauthorized publication of security measures**
- **Unauthorized “snooping” of computer traffic**
- **Unauthorized alteration or destruction or other’s people’s system or data**
- **Unauthorized obstruction of other’s legitimate use of computer**
- **Sending information (or e-mail) pretending to be from other sources.**



Computer Crime Law of 2017

What else is illegal?

- **Uploading of lewd materials**
- **Creating/sharing false information that can damage other's reputation or wellbeing**
- **Defamation via technological channel**
- **Sending/starting e-mail chains**
- **Posting or other action that defames royal institution (possibly, very long jail time)**



Posting and Sharing in Thailand

- You should not share/upload contents that
 - ▶ Are false/ partially false and intend to harm others
 - ▶ Are false/ partially false and threaten national security or intend to cause panic
 - ▶ Violate national security or related to terrorism
 - ▶ Consists of obscene materials
- Violator can be jailed up to 5 years, and/or fined for up to 100,000 baht.



Responsible Computer Use

Responsible computer use* (based on work of the Computer Ethics Institute) prohibits:

- 1. Using a computer to harm others**
- 2. Interfering with other people's computer work**
- 3. Snooping in other people's files**
- 4. Using a computer to steal**
- 5. Use a computer to bear false witness
(impersonation/spread lies)**
- 6. Copying or using proprietary software without paying for it**
- 7. Using other people's computer resources without authorization**
- 8. Appropriating other people's intellectual output**

* <http://computerethicsinstitute.org/publications/tencommandments.html>



Responsible Computer Use (cont.)

And encourage:

- 1. Thinking about the social consequences of what you are/will be doing.**
- 2. Using a computer in ways that insure consideration and respect of your fellow human.**



Intellectual Properties

- **Legally recognized exclusive right to creations of the mind**
 - ▶ **Intangible assets**

- **Laws can vary**
 - ▶ **Limited time**
 - ▶ **Limited to exclusivity**
 - ❖ **Fair use**
 - ▶ **Need to defend/ maintain**



Types of Intellectual Property

- **Copyrights**
 - ▶ **Creative works, including software**
- **Patents**
 - ▶ **Inventions**
- **Trademark**
 - ▶ **Recognizable sign, design or expression which identifies products or services of a particular source from those of others**
 - ▶ **Something that define a brand**
 - ▶ **Name, Logo, Slogan**
 - ▶ **Trademark holder needs to defend**



Trademark

- Usually, trademark needs to be defended/keep using.
- Can become abandoned, or generic: common name for that types of products.
- Examples:
 - ▶ Aspirin
 - ▶ Dry ice
 - ▶ Trampoline
 - ▶ Videotape



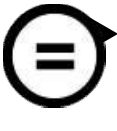



Fair Use

- **Any copying of copyrighted material done for a limited and “transformative” purpose.**
 - ▶ **Comment upon/ criticize**
 - ▶ **Parody**
- **Can be done without permission from the copyright owner**
- **Examples:**
 - ▶ **A news report regarding a product**
 - ▶ **A music review quoting a few line from the lyrics**
 - ▶ **Fan-made parody of a TV show**



Free Use License — Creative Commons

- **Creative Commons (CC) licenses facilitates legal sharing**
 - ▶ Customizable — owner can specify terms
 - ▶ Standardize — Easy to understand
- **Based on (mainly) 4 terms**
 -  **Attribution (BY)**
 - ❖ Must credit the original creator
 -  **ShareAlike (SA)**
 - ❖ Must license under identical terms
 -  **NoDerivers (ND)**
 - ❖ No derivatives — No modification
 -  **NonCommercial (NC)**
 - ❖ Can't use for commercial purpose



Creative Commons Licenses



1. Attribution (CC BY)



2. Attribution-ShareAlike (CC BY-SA)



3. Attribution-NonCommercial (CC BY-NC)



4. Attribution-NoDerivs (CC BY-ND)



5. Attribution-NonCommercial-ShareAlike (CC BY-NC-SA)



6. Attribution-NonCommercial-NoDerivs (CC BY-NC-ND)





Free software

- **Available for use at no monetary cost**
- **Free-to-use, but with restriction**
 - ▶ **Ads/ solicitation for donation**
 - ▶ **Limited types of use**
 - ❖ **Non-commercial**
 - ▶ **Limited time trial (shareware)**
 - ▶ **With upgradable version, for a price (freemium)**
- **May collect user's data**
- **Might not be safe**
 - ▶ **Only use free software from credible sources**



Computer Security

Classification of Threats

- **Computer Attack**
 - ▶ Intend to damage files, computers and/or networks
- **Computer Crimes**
 - ▶ Use of computer or network technology in criminal activities
- https://www.youtube.com/watch?v=AuYNXgO_f3Y
 - ▶ Source: code.org



Computer Attacks

- **Malwares — Trojan, Worm, and Virus**
- **Denial of Service (DoS)**

Malicious Software (Malware)

- **Automated programs and/or actions that intend to cause damage to computers and network, or stealing your data**
- **Self-replicating**
 - ▶ **Virus**
 - ▶ **Worm**
- **Non self-replicating**
 - ▶ **Trojan**



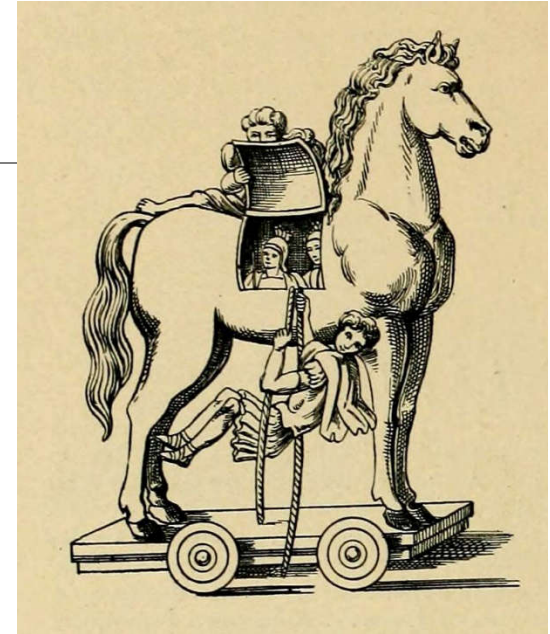
Virus/Worm

- **Self-replicating**
- **Virus**
 - ▶ **Usually damage files**
 - ▶ **Can reside in important part of hard drive, such as boot sector**
 - ▶ **Can spread through e-mail attachment or USB drive**
- **Worm**
 - ▶ **Does not destroy files**
 - ▶ **Designed to copy and send itself through networks**
 - ▶ **Brings computers down by clogging memory**



Trojan

- Trojan Horse
- Look like legitimate program
 - ▶ Trick user to install/ execute it
- Multiple possible actions
 - ▶ Annoying popup ads
 - ▶ Create backdoor and give access/control to the attacker
 - ▶ Damaging files/ systems
 - ▶ Hold computers/ files ransom



source: wikipedia



Denial of Service

- In computing, a **denial-of-service** attack (DoS attack) or **distributed denial-of-service** attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users.
- Generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
- For DDoS, attackers usually have computers under their control (bot/zombies) repeatedly connect to the target, disrupting it.



Computer Crimes

- **Unauthorized Access**
- **Hackers**
- **Cyber Stalking**
- **Fraud and Identity Theft**
- **Phishing, Scan and Hoax**

Unauthorized Access

- **Using computer systems with no authority to gain such access**
- **Other examples from the media**
 - ▶ **Employees steal time on company computers to do personal business**
 - ▶ **Intruders break into government Web sites and change information displayed (**defacing**)**
 - ▶ **Thieves steal credit card numbers and buy merchandise**



Hacking and Cracking

➤ Hackers

- ▶ Someone who seeks and exploits weaknesses in a computer system or computer network.
- ▶ **Black Hat**
 - ❖ Hack for criminal/malicious purpose
 - ❖ Blackmail/ Data theft/ Extortion
 - ❖ Damage systems for fun
- ▶ **White Hat**
 - ❖ Hack for non-malicious reason (curiosity/ job/ security concern)
 - ❖ Test the systems, then alert authority/publish vulnerabilities
- ▶ **Grey Hat**
 - ❖ Mix of Black and White



Hacking and Cracking (2)

➤ Crackers

- ▶ Break into computers with the intention of doing harm

➤ Hacktivists (sometime cyber terrorist)

- ▶ Break into computer systems to promote political or ideological goals

➤ Script kiddies

- ▶ Non-expert using tools (script) made by others



Bug Bounty

The other way being white hat can benefit.

- Company offers reward (financial/recognition) for person reporting bugs of their software to them.
- Better than selling the information to black market.
- Example:
 - ▶ <https://www.facebook.com/whitehat>
 - ▶ <https://www.google.com/about/appsecurity/reward-program/>
 - ▶ <https://technet.microsoft.com/en-us/library/dn425036.aspx>



Cyber Stalking

- **Use of computer/network technologies to stalk or harass one or more persons**
- **Activities**
 - ▶ **Defamation**
 - ▶ **Gathering information**
 - ▶ **Identity theft**
 - ▶ **Monitoring (esp. on Social Network)**
 - ▶ **Threats**



Identity Theft

- **Pretending to be someone else, for malicious purpose**
 - ▶ **Criminal Identity Theft**
 - ❖ Pretend to be someone else when arrested
 - ▶ **Financial Identity Theft**
 - ❖ Credit card, loans, etc
 - ▶ **Identity cloning**
 - ❖ Living as someone else
 - ▶ **Medical Identity Theft**
 - ❖ Using other's ID to obtain drug
 - ▶ **Child Identity Theft**
 - ❖ Using Child's ID
- **Use information gather (partially) from the web**



Software Piracy

➤ Legal activities

- ▶ Making one backup copy for personal use
- ▶ Sharing free software (shareware or public domain software)

➤ Illegal activities

- ▶ Making copies of purchased software for others
- ▶ Offering stolen proprietary software (warez peddling)



Other Computer Crimes

Type of Crime	Description	Recent Examples
Carding	Stealing credit card information for one's own use or to sell	A carder code-named Smak sells a CD with 100,000 credit card numbers to undercover law enforcement agents.
Cloning	Using scanners to steal wireless transmitter codes for cell phones, then duplicating the phone for illegal use	The practice was so prevalent in New York City in the mid-1990s that the mayor, police commissioner, and a city council member were victims.
Data diddling	Changing electronic data before or after it is entered on computers	A payroll clerk in a large company credits overtime hours to her own account, allowing her to steal hundreds of thousands of dollars from the company and her fellow employees.
Dumpster diving	Scouring wastebaskets and dumpsters for credit card receipts and other information, then using the information illegally or selling it	A young man in California impersonated telephone employees to gain access to equipment. He was so successful that he started his own telephone service before he was caught.
Phishing or spoofing	Attempting to trick financial account and credit card holders into giving away their authorization information, usually by posting false Web sites that duplicate legitimate sites	Many account holders at eBay, the popular auction Web site, were duped by a false Web site into giving up account numbers.



Other Computer Crimes (2)

Type of Crime	Description	Recent Examples
Phreaking	Breaking into telephone systems to make free long-distance calls or for other purposes	Kevin Mitnick, who served prison time in California under computer crime statutes, allegedly impersonated telephone employees to get free telephone service.
Piggybacking or shoulder-surfing	Looking over a person's shoulder while he or she is using an automated teller machine, cell phone, or other device in order to steal access information	At the Port Authority Terminal in New York City, computer fraud officers have often arrested people using binoculars to filch codes from telephone calling cards.
Salami slicing	Stealing small amounts of money from a large number of financial accounts	A bank employee transfers one penny from the balance of thousands of accounts every day and puts the money in an account she has set up for herself. She accumulates hundreds of thousands of dollars before being discovered.
Social engineering or masquerading	Misrepresenting yourself in order steal equipment or to trick others into revealing sensitive information	A person telephones a company employee and says he is working at home and needs certain information. He is lying but has enough genuine information to trick the employee into revealing network passwords. He then cracks the network and downloads proprietary information.
Vishing	Also known as voice phishing; instead of asking users to visit a Web site, asking users to call a fake telephone number and "confirm" their account information	An e-mail asks the recipient to call a phone number to confirm his credit card information. The fake phone number has been set up using VoIP technology, and the caller transfers his information to a scammer located somewhere around the globe, who is then able to run charges on the credit card.



Example: Cryptowall

- **Malware that uses encryption:**
<https://www.youtube.com/watch?v=ZghMPWGXexs>
Source: code.org
- Usually disguised as harmless attachments on e-mails, tricking you to open them.
- Once activated, the cryptowall encrypts files on your computers (and sometime those in the same network)
- Usually, cryptowall works as **ransomware**: a ransom note if left on your computer, detailing how to pay the ransom to get your files decrypted.



Example: Phishing

- **Attempt to obtain sensitive information, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.**
- **Sensitive Information**
 - ▶ **username/password**
 - ▶ **Credit card details**
 - ▶ **National ID number**
 - ▶ **Even money**
- **Usually comes in the form of e-mail pretending to be from bank/government agency/school/etc.**
 - ▶ **Usually ask you to “log in”/ provide personal information on the website with the URL provided in the e-mail.**
 - ▶ **Website is fake, created to collect your personal information.**



Hoax

- **Deliberately fabricated falsehood made to masquerade as truth.**
- **Distinguishable from:**
 - ▶ **Errors in observation or judgment**
 - ▶ **Rumors**
 - ▶ **Urban legends**
 - ▶ **Pseudoscience**
 - ▶ **April Fools' Day events that are passed along in good faith by believers or as jokes.**
- **Above is official definition, can also mean just unsubstantiated rumor spreading around the web.**



How to Stay Safe Online

1. Take cautions before clicking any attachment/ link
2. Take EXTRA cautions before sharing any personal information
3. Set privacy setting on social network properly
 - ▶ Location
 - ▶ Personal post/information
4. Install (trustworthy) security programs
 - ▶ Antivirus
 - ▶ Antispyware
 - ▶ Backup
 - ▶ Firewall

How to Stay Safe Online (2)

5. Practice Password Discipline

- ▶ Change password often
- ▶ Use different passwords for different sites
- ▶ Use strong password
- ▶ Never, ever, share password.


6. Logout from Facebook/Google/etc. after you're done using public computer

7. Set password for lockout screen for your PC/Phone/Tablet


Facebook Privacy Settings

Work and Education







Where have you worked?

 Chiang Mai University

Where did you go to college?

 Faculty of Engineering, CMU

Done Editing

- ✓  Public
-  Friends
-  Only Me
-  Custom
-  Close Friends
-  Chiang Mai University
- See all lists...

Privacy Settings and Tools

/ho can see my stuff?	Who can see your future posts?	Friends
Review all your posts and things you're tagged in		
Limit the audience for posts you've shared with friends of friends or Public?		
/ho can contact me?	Who can send you friend requests?	Everyone
Whose messages do I want filtered into my Inbox?		
Basic Filtering		
/ho can look me up?	Who can look you up using the email address you provided?	Everyone
Who can look you up using the phone number you provided?		
Everyone		
Do you want other search engines to link to your timeline?		
Off		

➤ Also, try to avoid checking-in as public post.

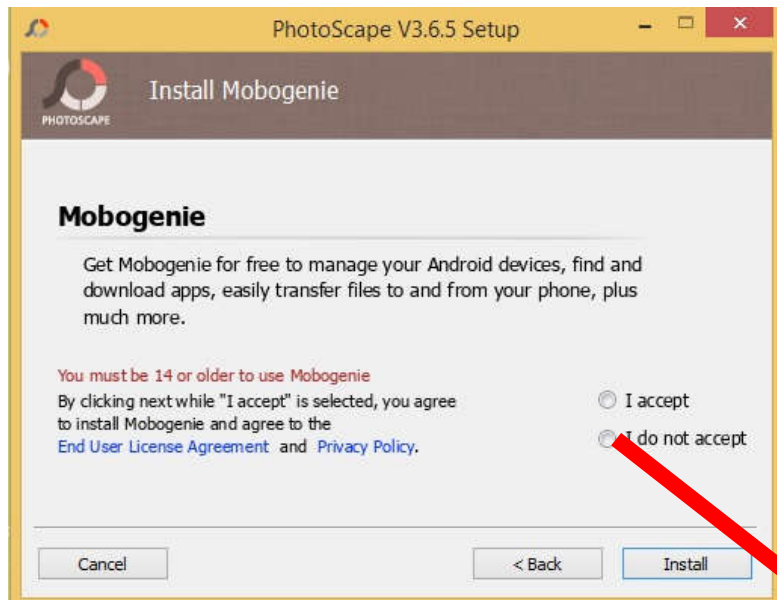


Securing Your System

- **As long as you have a computer and connect it to a network, you are vulnerable**
 - ▶ **Lock your computer when you are away**
 - ❖ **And set password to lockout screen**
 - ▶ **Disconnect your computer from the Internet when not being used.**
 - ▶ **Evaluate your security settings**
 - ❖ **Security Patches**
 - ❖ **Safeguarding your data**
 - **Anti-virus, password and encryptions, backups, separate user accounts**



Be Careful of What You Click



Password Security

- Change password often
- Use different password for different sites
 - ▶ In case one got hacked
- Use strong password
 - ▶ Hard to guess, even if the attacker know your personal information
 - ▶ (Should not be so hard that you can't remember it)
 - ▶ Avoid: 123456, *password*, *admin*, pet's name
- Secret Question
 - ▶ Option to recover your account
 - ▶ Should you use correct answer?



Authentication

- **How computer systems make sure that the user is actually who he or she is.**
- **Authentication can be:**
 - ▶ **Memorization: something you know (ex. password)**
 - ▶ **Physicality: a part of you (ex. fingerprint, face, voice)**
 - ▶ **Possession: something you own (ex. your phone)**
- **Biometrics**
 - ▶ **Use human characteristic and traits**
 - ▶ **Example: fingerprint, voice, face**
 - ▶ **Might not be practical**
- **Two-factor Authentication**
 - ▶ **Two components of above**
 - ▶ **<https://www.google.com/landing/2step/#tab=how-it-works>**



Backup

- **A backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.**
- **Backups have two distinct purposes.**
 - ▶ **recover data after its loss**
 - ▶ **recover data from an earlier time**
- **Backup conditions**
 - ▶ **Periodically**
 - ▶ **Every change**



Encryption/ Firewall

➤ Encryption

- ▶ In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it
- ▶ An authorized party, however, is able to decode the messages using a **decryption** algorithm.

➤ Firewall System

- ▶ Firewalls impose restrictions on incoming and outgoing packets to and from private networks.
- ▶ Only authorized traffic is allowed to pass through it.



Spam, Cookies and Spyware

➤ Spam

- ▶ Unsolicited e-mail promoting products or services
- ▶ Little protection available

➤ Cookies

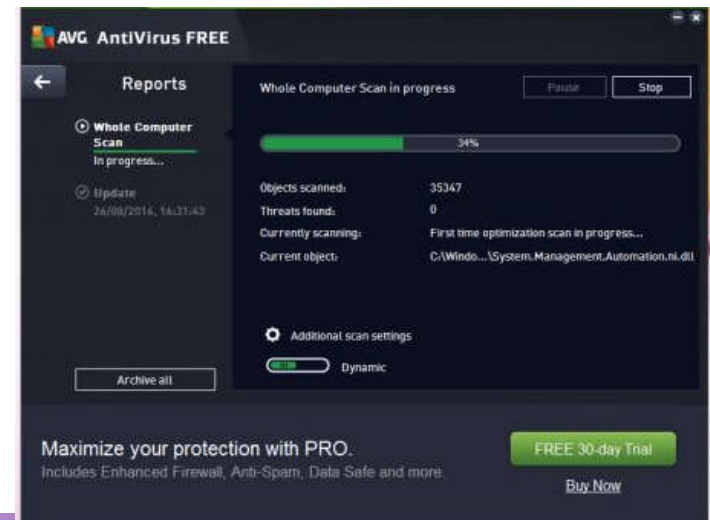
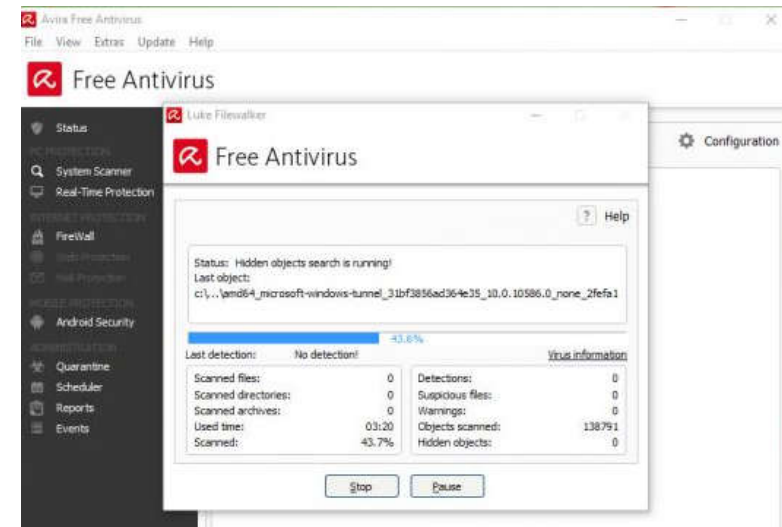
- ▶ Text file storing Web browsing activity
- ▶ Help a website “remember” you
- ▶ Can opt for cookies not to be stored
- ▶ Web sites might not function properly without cookies

➤ Spyware

- ▶ Software used for data collection without the users' knowledge
- ▶ Unlikely this activity will become illegal anytime soon

Top Free Antivirus (2016)

- **Avira Free Antivirus**
- **AVG AntiVirus Free**
- **Panda Free Antivirus 2016**
- **Comodo Free Antivirus**
- **Avast Free Antivirus**
- **ZoneAlarm Free Antivirus + Firewall**
- **Immunet AntiVirus**
- **Bitdefender Antivirus Free Edition**
- **Microsoft Windows Defender**



Top Antispyware (2013)

- **McAfee Virus Scan and Anti Spyware (not free)**
- **Navarre Webroot Spy Sweeper (not free)**
- **Lavasoft's Ad-Aware SE, Personal Edition**
- **Microsoft Windows Defender**
- **Spybot Search & Destroy**

