Computer Security

Assoc. Prof. Pannipa Phaiboonnimit

Adapted for English Section by
Kittipitch Kuptavanich
and Prakarn Unachak

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
- Self-replicating
  - Virus
  - Worm
- Non self-replicating
  - Trojan

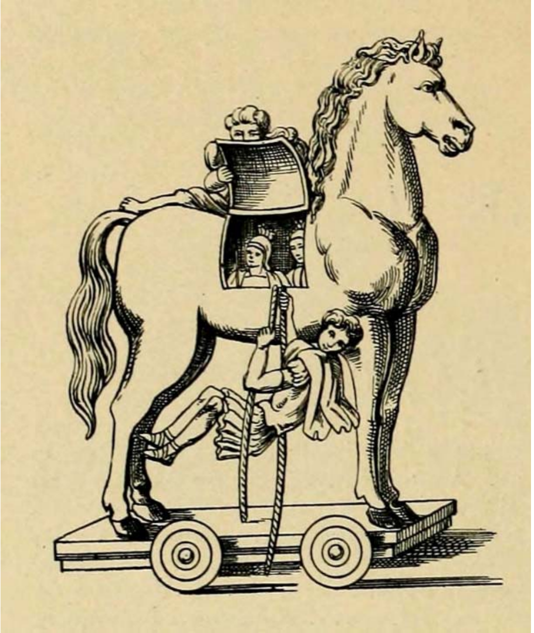
http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

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
- 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
  - 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

http://en.wikipedia.org/wiki/Hacker_(computer_security)

Hacking and Cracking (2)

- Crackers
  - Break into computers with the intention of doing harm
- Hacktivists
  - 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

http://en.wikipedia.org/wiki/Cyberstalking

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

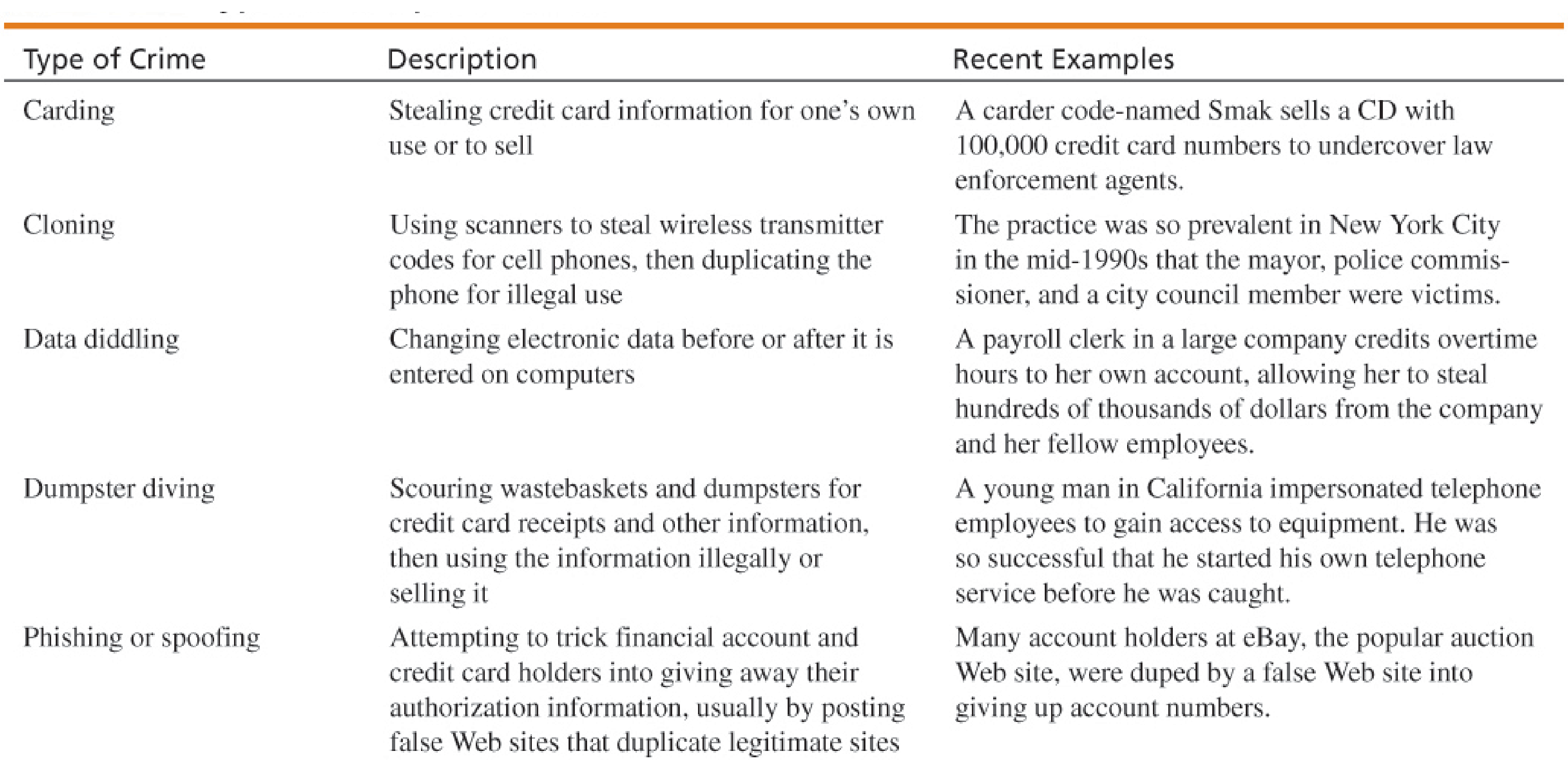
http://en.wikipedia.org/wiki/Identity_theft

Software Piracy

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

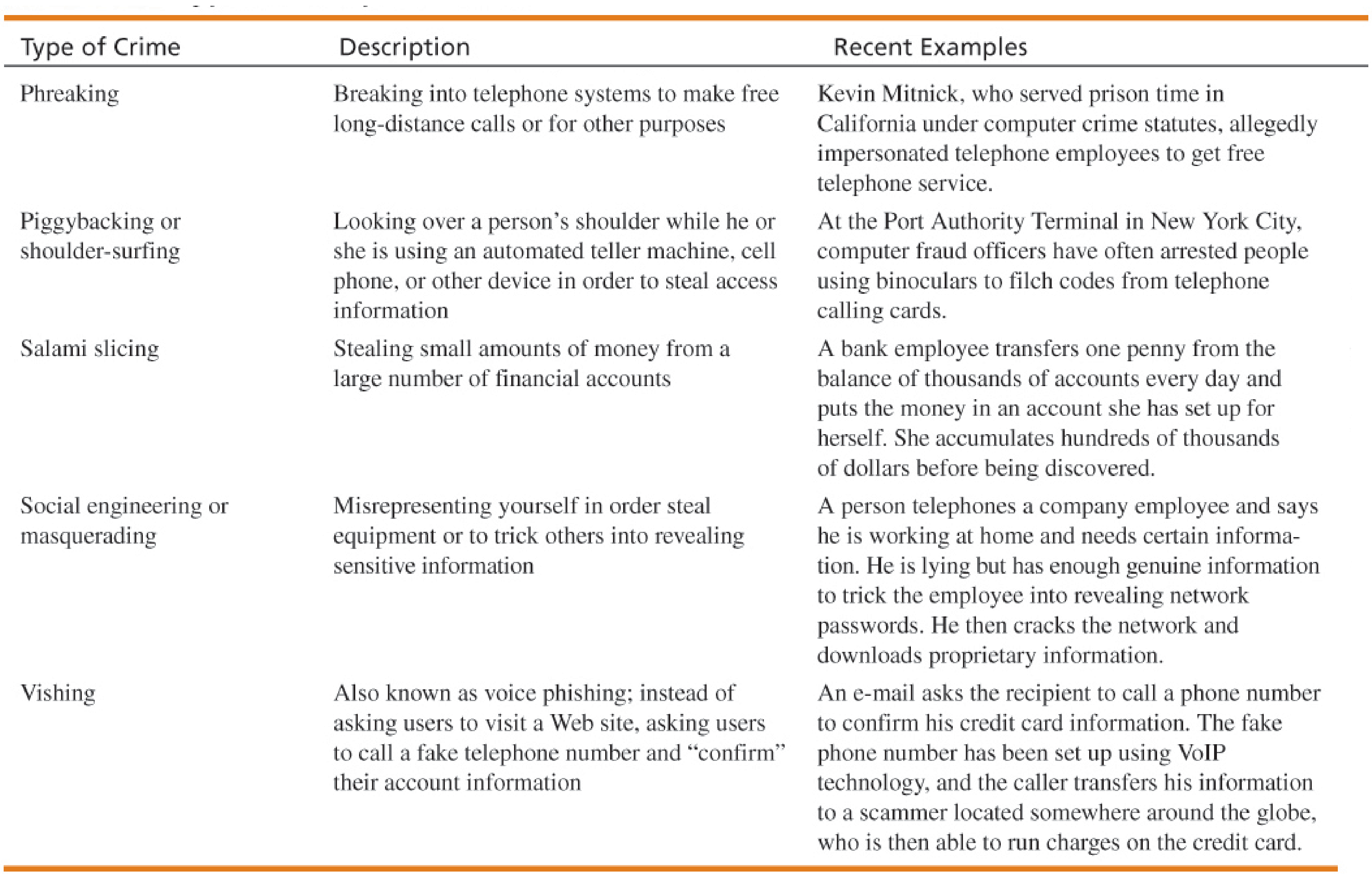
- Illegal activities
  - Making copies of purchased software for others
  - Offering stolen proprietary software (warez peddling)

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.

https://blogs.sophos.com/2015/03/03/anatomy-of-a-ransomware-attack-cryptolocker-cryptowall-and-how-to-stay-safe-infographic/

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 back/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

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

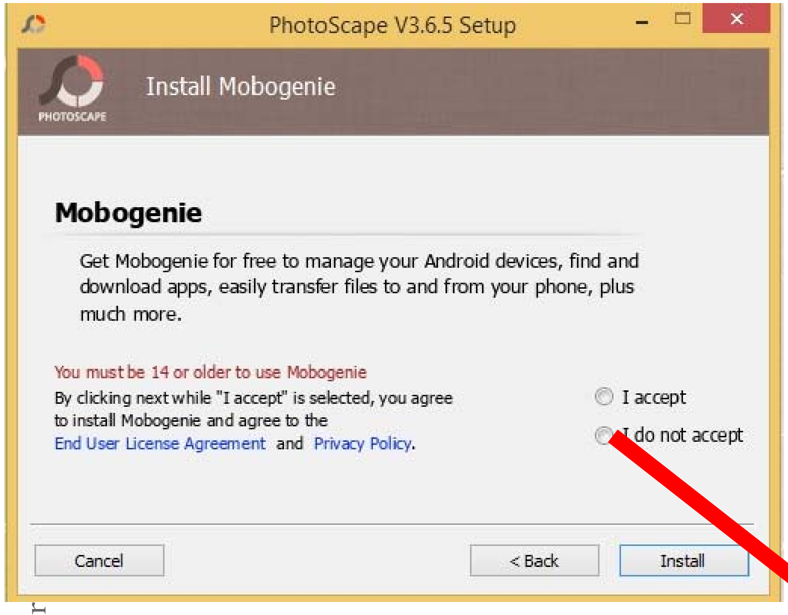
How to Stay Safe Online (2)

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

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



Mobogenie

Get Mobogenie for free to manage your Android devices, find and download apps, easily transfer files to and from your phone, plus much more.

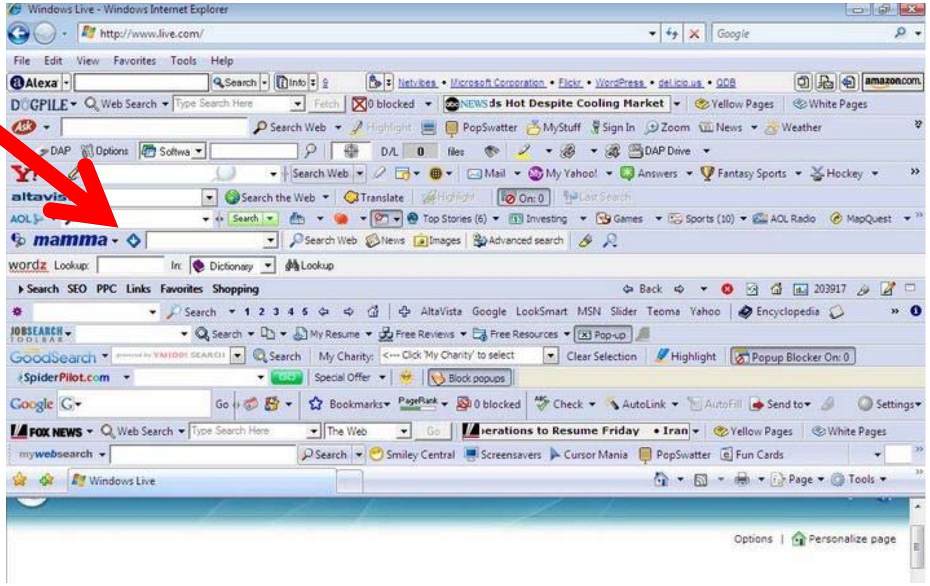
You must be 14 or older to use Mobogenie

By clicking next while "I accept" is selected, you agree to install Mobogenie and agree to the End User License Agreement and Privacy Policy.

○ I accept

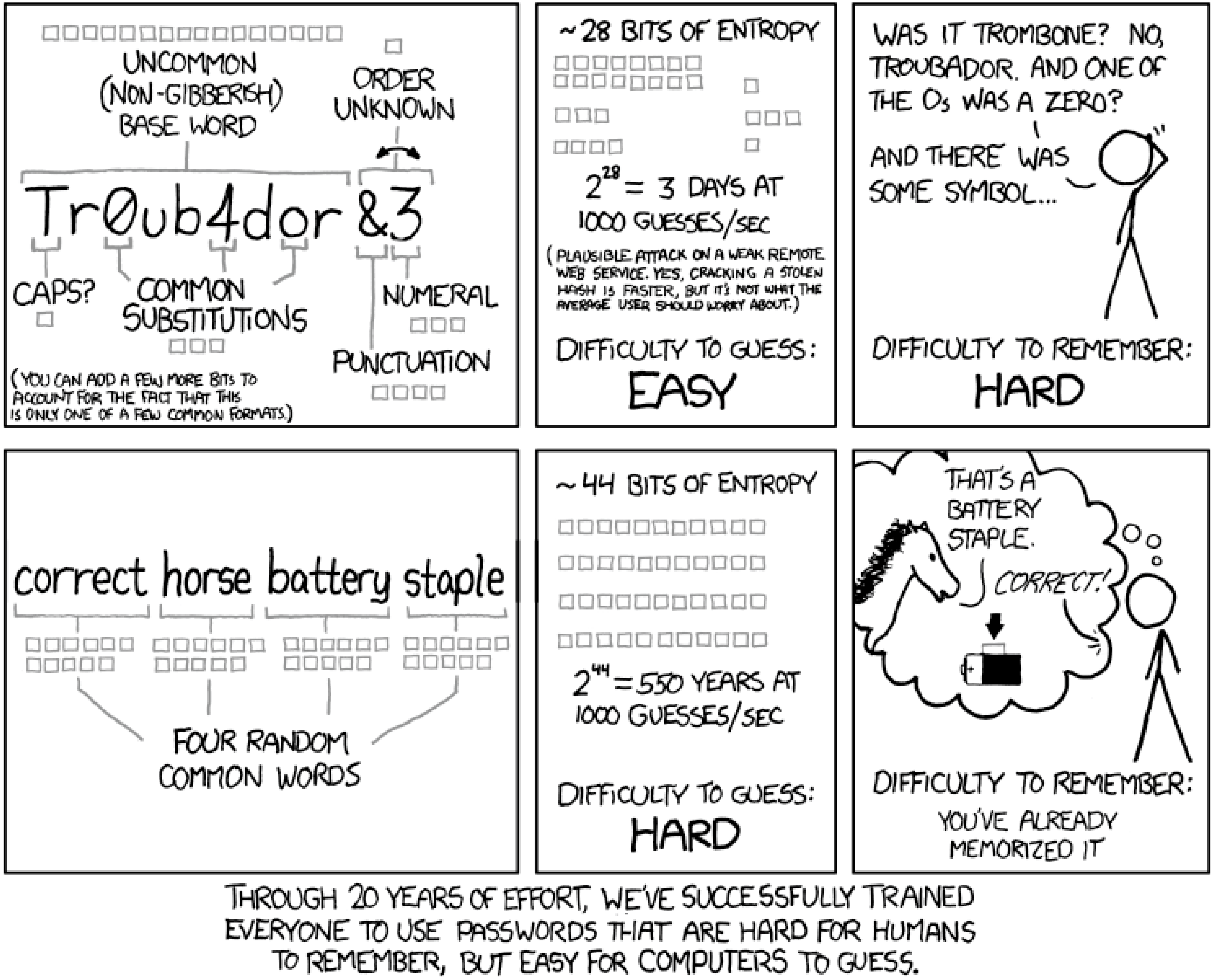
○ I do not accept

Cancel | < Back | Install



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?


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

source:xkcd.com

Other Security Measure

- Biometrics
  - Use human characteristic and traits
  - Example: fingerprint, voice, face
  - Might not be practical
- Two-factor Authentication
  - Two components
    - Password + smart phone
    - Password + fingerprint
  - 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

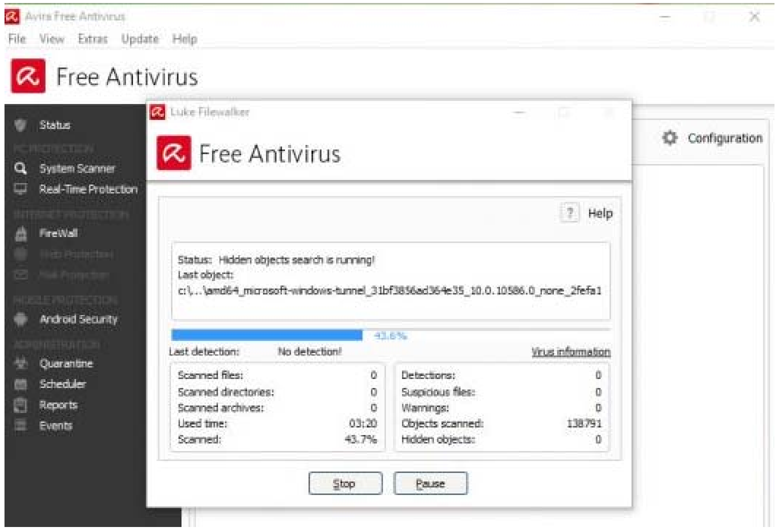
- Encryption
  - In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it
  - An authorized party, however, is able to decode the messages using a **decryption** algorithm.
- Firewall System
  - Firewalls impose restrictions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

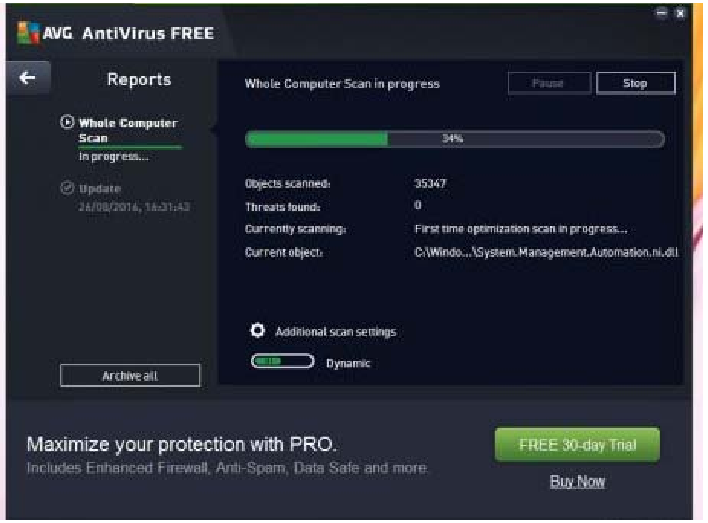
- Avira Free Antivirus
- AVG AntiVirus Free
- Panda Free Antivirus 2016
- Comodo Free Antivirus
- Avast Free Antivirus
- ZoneAlarm Free Antivirus + Firewall
- Immunet AntiVirus
- Bitdefender Antivirus Free Edition
- Microsoft Windows Defender



Status: Hidden objects search is running!
Last object:
c:\...\amd64_microsoft-windows-tunnel_31bf3856ad364e35_10.0.10586.0_none_2fefa1

Last detection: No detection!

Scanned files:	0	Detections:	0
Scanned directories:	0	Suspicious files:	0
Scanned archives:	0	Warnings:	0
Used time:	03:20	Objects scanned:	138791
Scanned:	43.7%	Hidden objects:	0



Whole Computer Scan in progress

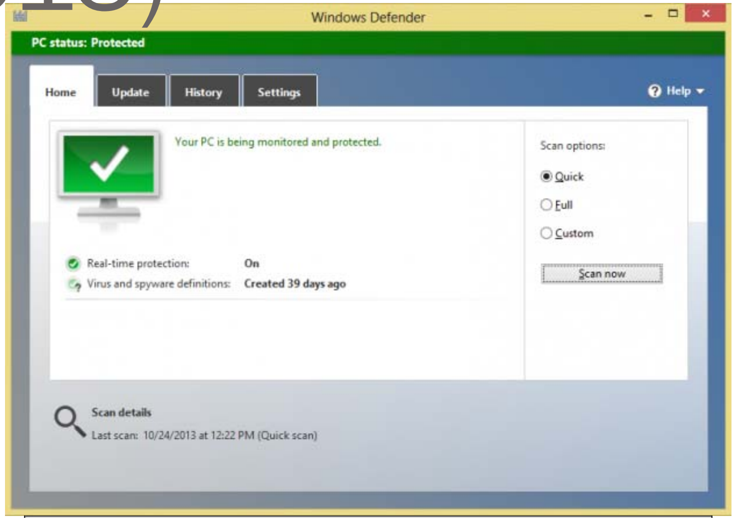
Objects scanned:	35347
Threats found:	0
Currently scanning:	First time optimization scan in progress...
Current object:	C:\Windo...\System.Management.Automation.ni.dll

Maximize your protection with PRO.
Includes Enhanced Firewall, Anti-Spam, Data Safe and more.

http://www.techradar.com/news/software/applications/best-free-antivirus-1321277

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



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Created 39 days ago

Scan options:

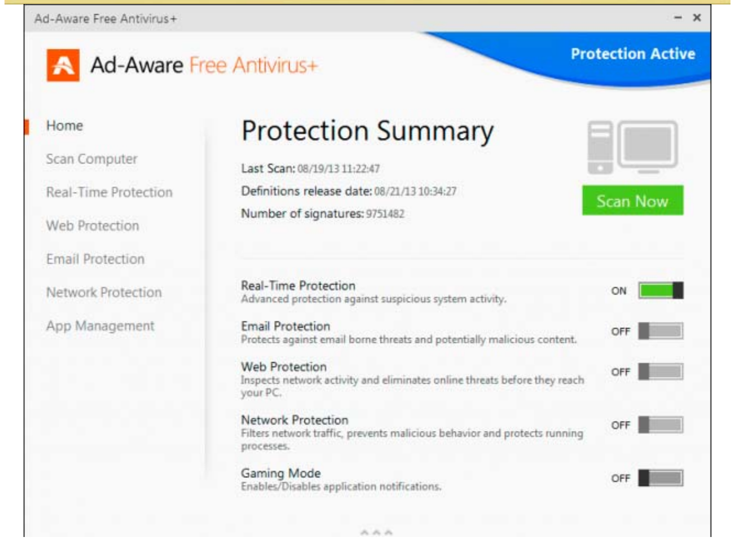
● Quick

○ Full

○ Custom

Scan details

Last scan: 10/24/2013 at 12:22 PM (Quick scan)



Protection Active

Protection Summary

Last Scan: 08/19/13 11:22:47

Definitions release date: 08/21/13 10:34:27

Number of signatures: 9751482

Real-Time Protection — Advanced protection against suspicious system activity. — ON

Email Protection — Protects against email borne threats and potentially malicious content. — OFF

Web Protection — Inspects network activity and eliminates online threats before they reach your PC. — OFF

Network Protection — Filters network traffic, prevents malicious behavior and protects running processes. — OFF

Gaming Mode — Enables/Disables application notifications. — OFF

http://netforbeginners.about.com/od/lockdownyourpc/a/antispyware.htm