

Computer Perils

*There is always
free cheese
in a mouse trap*

Overview

- Threats
- Consequences
- Free Cheese in a Mouse Trap
- Leaving Fingerprints
- Best Practices
- Best Practices are not Enough

Threats

- Virus
 - A virus is a type of program that can replicate itself by making (possibly modified) copies of itself. Spread by E-mail and programs. Attaches to another program
- Common Programs (interpreting code)
 - Internet Browsers, Players, Office Programs
- Worms
 - Self-contained program that spreads through the network through network services (file sharing, printing, mail, administrative, blue tooth)
- Freeware/Shareware
 - Nothing is free. Many programs contain viruses or spyware.

Consequences

Privacy

- Surveillance (programs gather information about you and give it to others).
- Keystroke logging

System Integrity

- Corrupt the H.D.
- Corrupt the OS
- Degrade performance (launching pop-ups, etc).

Become a Zombie

- launch attack on others
- Illegal activities (file server, website, etc)

Social Engineering

(free cheese)

- Wetware the weakest link
 - E-mail
 - Spoofed sender.
 - Has a virus payload.
 - Websites
 - Tricked into visiting.
 - Can compromise your computer through browser flaw.
 - Give away sensitive information.

Being Perfect is not Enough

- A fully patched and virus protected computer is still vulnerable.
- A superworm can get through your computer through a hole that has not been patched (Zero Day Vulnerability).
- A virus laden e-mail will come through before definitions exist or are updated.

Leaving Fingerprints

- Everywhere you go on the Internet your actions are logged by your IP address

Example:

- 81.80.199.105 - - [16/Feb/2006:13:34:28 -0800] "GET /labmanual/chap1/1.10.html HTTP/1.1" 200 222573
"http://www.google.it/search?q=Wright+Etchant&hl=it&lr=&start=10&sa=N" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
- 212.107.27.37 - - [16/Feb/2006:13:50:36 -0800] "GET /labmanual/chap8/8.22.html HTTP/1.1" 200 97510
"http://www.google.com/search?q=what+is+a+field+iris&hl=en&lr=&rls=GGLR,GGLR:2005-39,GGLR:en&start=10&sa=N" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
- 128.32.126.228 - fujit [21/Feb/2006:16:50:51 -0800] "GET /members/active/ningc.html HTTP/1.1" 200 392

An IP address provides the minimum amount of information needed to attack a computer over the Internet.

- DATAMINING

Cookies

Helps websites keep track of your session

- but gives away information about what you do.
- advertising companies, double click

Reduce Risk

- *Back up your data*
 - Photos, Music, Mail, Taxes,
 - Anti-Virus
 - Patches
 - Be Careful
 - Firewall

Summary

- Watch where you are going.
- There is nothing for free.
- Keep your system patched and up-to-date with virus definitions.
- Look out for suspicious behavior on your computer.
- Back up your files.