Seven Simple Steps to Securing your Home Computer

PROFESSOR PARKS

2/5/20

Introductions

- Share:
  - Your name, and maybe
  - Why you are here

What can you do when your computer becomes infected?

- Run and hide?
- Disconnect your computer from the Internet?
- **No!** Instead be security-smart and prepared.

TRY THESE

SEVEN

SIMPLE STEPS!

Step 1: Assess Your Risks

- Years ago, people thought of the Web as well...wonderful. And safe!
- And it is even more wonderful today. But some corners of the Web are pretty wild, dangerous and weird.
- And what's "out there" can bring home unwelcome consequences to your privacy and computer security.

Assess Your Risks

- Ask yourself:
  - Who uses my computer?
    - Do visitors or friends use my computer?
    - Do young children or teenagers have unsupervised access to your computer?
  - How do I connect to the Internet?
    - Are you always connected?
      - If "Yes" then you need a firewall, etc.
  - What do people with access to my computer do on the Internet?
    - Does anyone shop, bank, pay bills, invest in stocks or mutual funds, or manage an IRA online?

Step 2: Use Anti-malware Software - I beg you!

- Virus and spyware writers are working around the clock to attack/exploit you; and antivirus vendors and companies like Microsoft are working around the clock to help protect you.
- Help protect your computer files and e-mail by using and updating your antivirus and anti-spyware software.
- *What is the difference between a Virus, Trojan Horse, Worm and Spyware?*

Use Antivirus and Anti-spyware Software

- How can you get a virus or spyware?
  - Besides picking up one from an e-mail attachment, you can acquire it from free content you download from a Web site or from a thumb drive someone shares with you.
  - If your computer is not protected, once you download and install the program, the virus or spyware can spread.

How big is the virus problem?

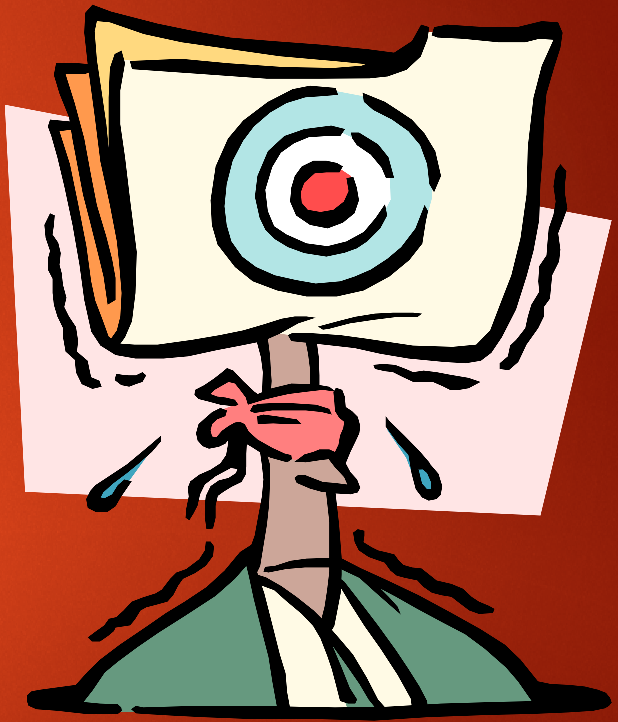
- There are at least 300,000 known malware and more are written every day.
- About 95-98% of malware come through e-mail and instant messaging.
- Often malware arrive with e-mail disguised as something entertaining, like pictures, music, or greeting cards.
  - Time to take the Sandwich test

How to know if your computer has malware?

- Stay alert for these symptoms:
  - Computer slows down.
  - Very large amount of Internet activity.
  - Unusual behavior of your computer.

What should you do if you get a Virus or Spyware?

- Don’t panic!
  - Get the latest signature file from your vendor's Web site.
  - Next, run your scan of the computer and it should find infected files automatically. It will advise whether it is able to remove them from every file or whether you should delete infected files.
  - Inform anyone you may have infected. After you eradicate the virus or spyware from your system, inform those with whom you have shared files that they may be at risk from the same infection.



Step 3: Keep Your Software Up-to-Date

- Updates—known as "fixes," "patches," "service packs," and "security rollup packages"—help to protect your computer and your personal data.
- Updates address exploitable flaws or introduce additional security features.

Why Are There So Many Updates and Advisories?

- Modern software systems involve incredibly complex engineering, but because they are made by human hands there will always be imperfections.
- Software "crackers" sometimes exploit those flaws.

Checklist for Keeping Software Up-to-Date

- The easiest way to keep up with patches is to take advantage of automatic update and notification services that many software publishers provide.
- Windows has a built-in update feature (called, "Windows Update") that will update the operating system automatically for you.

Step 4: Check Your Settings

- There are settings in software that govern how the program handles certain tasks, such as allowing or blocking downloads, screening Web sites, or accepting cookies.
- You can change the privacy and security settings to suit the levels of protection you prefer.
- Let’s learn how to secure Chrome.

Checklist for Checking Your Settings

- Is your software up-to-date?
  - Before making changes to your settings, always make sure your software patches are up-to-date.
- Check your Internet browser settings
  - Check the Security Tab settings.
    - Internet Explorer divides your online world into four zones: Intranet, Trusted, Restricted, and Internet.
  - Check the Privacy Tab settings.
    - Define your preferences for handling cookies and your standards for releasing personal information. See how to in Internet Explorer and Web Privacy.
  - Activate the Content Advisor in Internet Explorer if you have children using the web brower.

Step 5: Install a Firewall

- They say, “good fences make good neighbors.”
- You can add an important layer of protection between your computer and the Internet by using a firewall system.
  - Potential intruders scan computers on the Internet probing for a "port" where they can break and enter.
  - A firewall can help block unauthorized entry into your computer, as well as restrict outbound traffic.

Choose a Firewall

- Personal (or software) firewalls cost $ to $$$ per PC.
- Vendors
  - Microsoft
  - Symantec
  - McAfee
  - ZoneAlarm Pro
  - Sygate Personal Firewall PRO
  - Zero-Knowledge Systems Freedom Personal Firewall
  - Internet Security Systems Black Ice Defender

Manage your Firewall

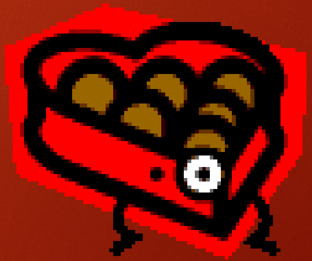
- Check for software updates. Go to your firewall vendor's Web site, and sign up to be notified of updates.
- Review the logs. Ascertain how much probing traffic your firewall is repelling.
- Turn off "always on." If you have DSL or cable modem, turn off your connection when you don't need to be online.

Step 6: Create Strong Passwords

- If you've ever lost your wallet, you know the sense of vulnerability—that someone else could be walking around with your identification, pretending to be you.
- Well, if someone were to get your passwords—log on to your computer or your online accounts—they could ultimately assume your digital identity, pass themselves off as you, and have fun at your expense.

“Security crumbles in the face of sweet bribes”

- According to one study more than 70% of people would reveal their computer password in exchange for a bar of chocolate.
- It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.
- Would You?



Fun for Bad Guys: Bad News for You

- What could someone do if they have your passwords?
  - Access information on your computer, such as your financial records, e-mail messages, stored lists of passwords, and private information.
  - Open new accounts and buy, buy, buy.
  - Change your mailing address, and have items they purchase (and bills) sent to them.
  - Withdraw money from your bank.
- ***Think of your password as if it were a key to your home and everything you own, including your reputation.***

What makes a password STRONG?

- Make sure you create a password that:
  - Is at least seven characters in length, and the longer the better.
  - Includes upper and lower case letters, numerals, symbols
  - Has at least one symbol character in the second through sixth position
  - Has at least four different characters in your password (no repeats)
  - Looks like a sequence of random letters and numbers

Make sure you:

- Don't use ANY PART of your logon name for your password
- Don't use any actual word or name in ANY language
- Don't use numbers in place of similar letters
- Don't reuse any portion of your old password
- Don't use consecutive letters or numbers like "abcdefg" or "234567"
- ***Let's create a good one together.***

Manage your passwords

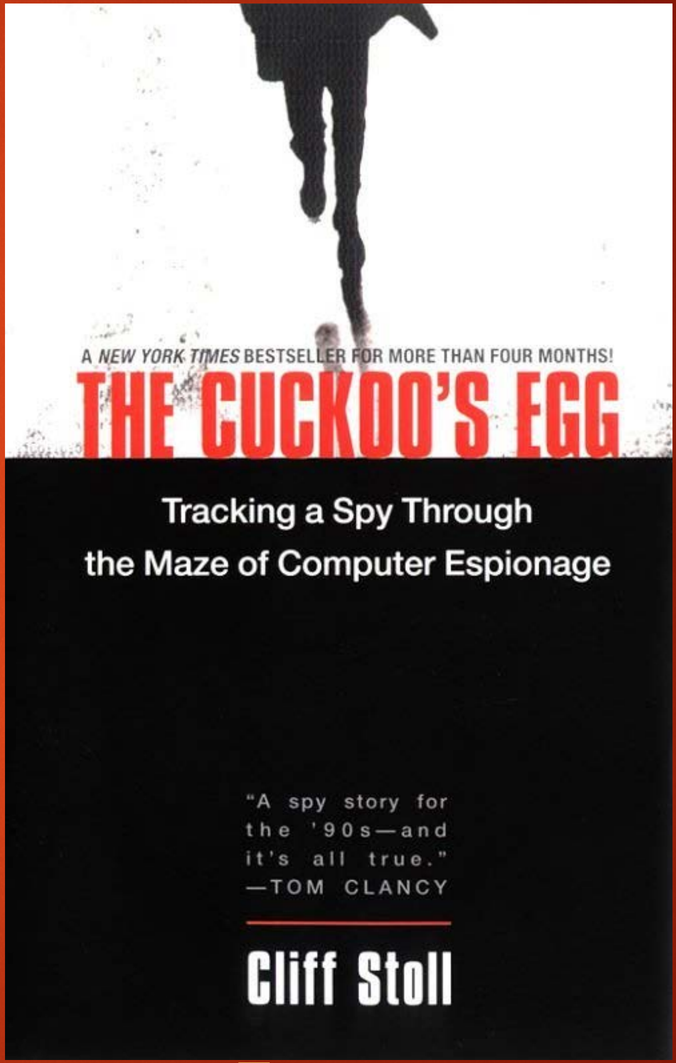
- Keep it to yourself.
- Do not write it down, if possible.
- Do not share it with anyone.
- Do not check the "remember my password" feature, without considering the value of the data the password protects.
- If you had reason to tell someone your password, then create a new one at your earliest opportunity.

Step 7: Conduct Routine Security Maintenance

- When you buy a new vehicle—whether it's the car of your dreams, a new bike, or a boat—you know you're going to have to maintain it.
- The oil needs to be changed, the air filter replaced, the tires rotated—all on a regular schedule—so you can trust your vehicle will be available when you need it to get you safely where you want to go.
- Keeping your computer updated to help protect your privacy is much the same; it involves ongoing maintenance, not a "one shot" fix.

Suggested Reading

- Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
  - by Clifford Stoll
  - At Amazon



A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!

THE CUCKOO'S EGG

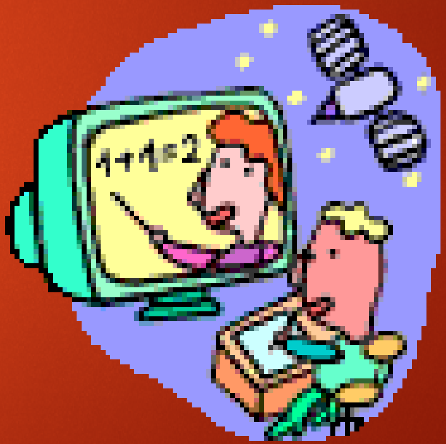
Tracking a Spy Through the Maze of Computer Espionage

"A spy story for the '90s—and it's all true."
—TOM CLANCY

Cliff Stoll

Suggested Course

- CISS 300 – Introduction to Information Systems Security (one unit, no prerequisite)



??? Questions ???

- You can reach me at parksl@crc.losrios.edu