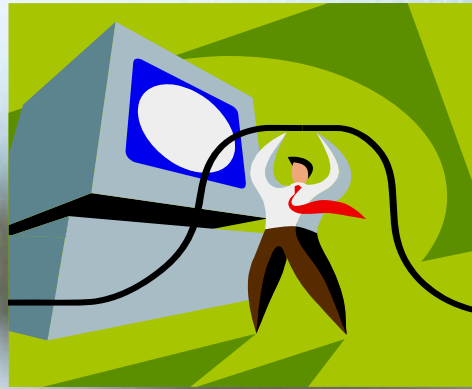


Managing Internet Annoyances on Campus



Viruses, Spyware, SPAM, and Phishing

Introduction

- Internet Use on Campus
- Presentation Breakdown
- Explanation of Handouts
- C&NS Training Materials
 - <http://www.fairfield.edu/cnstraining>

Viruses, Trojans, and Worms Oh My!



■ Definition

- A computer virus is a software program that is created by people and is “deliberately designed to interfere with computer operation, record, corrupt or delete data, or spread themselves to other computers and throughout the internet.” (Microsoft)
- **Why do people create Viruses?**
- **How do Viruses work?**



Viruses, Trojans, and Worms Oh My!

- How do you get a Virus?
- How do you know if you have a one?
 - Computer stops responding or locks up often
 - Crashes and restarts every few minutes
 - Restarts on its own and then fails to run normally
 - Applications don't work properly
 - Disks or disk drives are inaccessible
 - Printing doesn't work correctly
 - You see unusual error messages
 - You see distorted menus and dialog boxes
- **These signs can also indicate hardware or software problems and have nothing to do with a virus!**

Viruses, Trojans, and Worms Oh My!

- **Common Viruses target executable (.exe) files that contain application software or parts of the operating system.**
 - Mail spoolers, computer shutdown and restarts, loss of functionality in Office products, data/file corruption, loss of network connectivity or internet access.
- **Worms**
 - Malicious self-replicating program.
- **Trojans**
 - Malicious program that is disguised as legitimate software.

Viruses, Trojans, and Worms Oh My!

- **What kind of computers do viruses appear on?**
 - Microsoft Operating systems, of course!
 - Other Operating Systems?
- **How do you remove viruses?**
 - There is no way of knowing you have a virus unless you have virus detecting software.
- **How do we manage viruses on campus?**
 - Norton Anti-Virus



How to protect your computer against Viruses

- Keep your computer software up to date
- Adjust your web browser security settings and use other browsers
- Use antivirus software
- Regularly backup your files (Artemis)
- Be on alert while browsing (Always read before you click "OK")
- Use e-mail cautiously
- Don't use illegal file sharing programs



Spyware

■ Definition

- “**Spyware** is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent. It has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.” (wikipedia.org)
- “Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, spyware is designed to exploit infected computers for commercial gain.” (wikipedia.org)
- The Who: “Much spyware operates under the cloak of legitimate business, complete with corporate headquarters, legal department, publicists, Washington lobbyists and millions in revenues to fund the assault on your computer. Spyware is written by the very best teams of hackers and virus writers.” (Consumer Reports)

Spyware

■ Types of Spyware

(Most frequently detected)

- Adware - Delivery of unsolicited pop-up advertisements
 - Theft of personal information (including financial information such as credit card numbers)
 - Monitoring of Web-browsing activity for marketing purposes (tracking)
 - Routing of Internet Browsers to advertising sites

Spyware

- **How do you get Spyware?**
 - “Spyware gets on a system through deception of the user or through exploitation of software vulnerabilities. The most direct route by which spyware can get on a computer is for the user to install it.” (wikipedia.org)
 - E-mail attachments, files downloaded from web sites, instant messaging programs, free games, utilities, or ad-supported software.

Spyware

■ How do you know you have Spyware?

- You see pop up ads all the time.
- Your settings have changed and you can't change them back to the way they were.
- Your web browser contains additional components that I don't remember downloading. A new toolbar.
- Your computer seems sluggish.
- Computer crashes.

■ Can Spyware get on other Operating Systems?

- (Mac users Beware of Widgets!)

Spyware



■ Examples of Spyware

- Keyloggers, capture screenshots of online use, eavesdrop on you via your web cam and microphone.

■ Programs with Spyware

- Bearshare, Bonzi Buddy, Download Accelerator Pro, Internet Optimizer, Gator, Kazaa, Weather Bug, Aol Instant Messenger, Limewire, Huntbar, Webshots



Spyware

- **How do you remove Spyware?**
- **How do you protect your computer against Spyware?**
 - Keep your computer software up to date
 - Adjust your web browser security settings and use other browsers
 - Use antivirus software
 - Regularly backup your files
 - Be on alert while browsing
 - Use e-mail cautiously

Spyware

- How do we manage Spyware on campus?

Internet Annoyance Terminology

- Viruses, Worms, Trojans, Spyware -- Sounds like they all do the same thing!!!!
- Spiruses!!
- Anti-Virus software will become more multi-functional.

Spam – It ain't in a can anymore!

■ Definition

- **Spamming** is the use of any electronic communications medium to send unsolicited messages in bulk. The term "spam" can refer to any commercially oriented, unsolicited bulk e-mailing perceived as being excessive and undesired. (wikipedia.org)

SPAM



■ Why SPAM

- The Name: The Monty Python Spam sketch and Hormel Foods

■ The Purpose of SPAM

- Sending spam is a lucrative business. It costs spammers next to nothing to send out millions, even billions, of e-mail messages. Low operating costs. Barriers to entry are low.
- A tiny percentage of a hundred million people buy something in response to a junk message.



SPAM

■ How to you get spam?

- Spammers steal, swap, or buy lists of valid e-mail addresses.
- Some spammers also gather or harvest addresses from Web sites where people sign up for free offers, enter contests, and so on.

SPAM

- **Why SPAM is bad (its effects on your e-mail and computer)**
 - Costs which are borne by the public (in terms of lost productivity and fraud)
 - Spam is certainly annoying and disruptive, even disturbing. But spam can also potentially be dangerous to your computer, to your bank account, and to your privacy.

SPAM

■ Types of Spam

- The most common form of spam is that delivered in e-mail as a form of commercial advertising. (junk-mail)
- Spammers have developed a variety of spamming techniques, which vary by media: e-mail spam, instant messaging spam (**SPIM**), Usenet newsgroup spam, Web search engines spam, weblogs spam, and mobile phone messaging spam (**SPIT**).
- Non-commercial – Denial of Service Attacks, spread viruses.

■ How “they” are managing Spam

- Microsoft
 - Better security built into their OS's and e-mail programs.
- The Federal Government
 - Legislation

SPAM

- **How can you manage SPAM on campus?**
 - Microsoft Outlook
 - Spam Filtering from the Exchange Server
 - The <<spam>> subject line
 - Using “Rules” to manage spam
 - Don’t use the “Preview Pane”
 - Use “Message with Preview” instead
 - The future of SPAM filtering on Campus
 - University SPAM software

SPAM

■ How you can manage Spam

- Delete junk e-mail messages without opening them.
- Don't reply to spam, even if it gives you the option to unsubscribe to the list.
- Don't give personal information in an e-mail or instant message. AOL keeps records of you messages!!
- Think twice before opening attachments or clicking links in e-mails or instant messages.
- Don't buy anything or give to any charity promoted through spam.
- Don't forward chain e-mail messages.
- Report abusive, harassing, or threatening e-mail messages.
- Report phishing scams and other fraudulent e-mail.
- File a complaint with the FTC. (Federal Trade Commission)
- Forward your complaints to system administrators who can act on them.
- Use multiple e-mail addresses. Separate work and personal e-mail.
- Follow "How to protect your computer against viruses and spyware."



Phishing

■ Definition

- “Phishing is a type of deception designed to steal your identity.” (microsoft.com)
- “In phishing scams, scam artists try to get you to disclose valuable personal data—like credit card numbers, passwords, account data, or other information—by convincing you to provide it under false pretenses.” (microsoft.com)
- “Phishing schemes can be carried out in person or over the phone, and are delivered online through spam e-mail or pop-up windows.” (microsoft.com)



Phishing

- **How does Phishing work and how do you get it?**
 - "A phishing scam sent by e-mail may start with con artists who send millions of e-mail messages that appear to come from popular Web sites or sites that you trust, like your bank or credit card company." (microsoft.com)
 - "The e-mail messages, pop-up windows, and the Web sites they link to appear official enough that they deceive many people into believing that they are legitimate. Unsuspecting people too often respond to these requests for their credit card numbers, passwords, account information, or other personal data." (microsoft.com)

Phishing

- **What does a phishing scam look like?**
 - They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites.
 - To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site, but it actually takes you to a phony scam site or possibly a pop-up window that looks exactly like the official site.
 - These copycat sites are also called "spoofed" Web sites. Once you're at one of these spoofed sites, you might unwittingly send personal information to the con artists. They then often use your information to purchase goods, apply for a new credit card, or otherwise steal your identity.



Phishing

■ Recent Phishing attempts

- Customers of banks and online payment services.
- Some examples.

■ How do you spot Phishing?

- "Verify your account"
- "If you don't respond within 48 hours, your account will be closed." or something related.
- "Dear valued customer" or "member"
- "Click the link below to gain access to your account."
- IP numbers for addresses, not regular name addresses.
- The yellow Lock on the bottom right of your browser.
- HTTPS (<https://owa.fairfield.edu/exchange>)
- You are not a member!!, general salutations –not specific.
- Call the company or business to find out.

Phishing

■ Spotting Phishing continued...

- You don't know the person who has sent you the message.
- You are promised untold sums of money for little or no effort on your part.
- You are asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process.
- You are asked to provide your bank account number or other personal financial information, even if the sender offers to deposit money into it.
- The request contains a sense of urgency.
- The sender repeatedly requests confidentiality.
- The sender offers to send you photocopies of government certificates, banking information, or other "evidence" that their activity is legitimate (these are fake!).

Phishing

- **What “they” are doing to control Phishing?**
 - Training the user
 - Legislation
 - Anti-Phishing Organizations
 - Software

Phishing

- **How you can manage phishing**
 - Follow, “How you can manage SPAM” steps
 - Do report suspicious e-mail
 - Do be wary of clicking on links in e-mail messages.
 - Do type addresses directly into your browser or use your personal bookmark.
 - Do check the security certificate when you are entering personal or financial information into a website.
 - Don't enter personal or financial information into pop-up windows.

Phishing

- **What to do if you think you responded to a Phishing scam**
 - **Step 1: Report the incident**
 - Your credit card company, if you have given your credit card information.
 - The company that you believe was forged.
 - The IFCC. The Internet Fraud Complaint Center (IFCC)
 - The Federal Trade Commission.
 - **Step 2: Change the passwords on all your accounts**
 - **Step 3: Routinely review your credit card and bank statements**
 - **Step 4: Use up-to-date antivirus and anti-spyware software, update your computer software**

Managing Internet Annoyances on Campus

Questions???

and

THANK YOU!!

