Phishing, Viruses, Pop ups and Worms

Protect Yourself From Cyber Security Threats
What are these threats?

How do I protect my computer?
Social engineering attacks occur when an attacker uses human interaction and expected, traditional social skills to obtain or compromise information.

• Attacks may be done in stages, using information obtained in a first contact to gain credibility for the second contact.

Phishing is a social engineering attack that uses credible looking email or web sites to solicit personal, often financial information.

• Often uses official looking logos and addresses.

• Financial information gathered in this way is used to gain account access or steal identity.
Avoid Being a Victim

- Be suspicious of unsolicited email, phone calls, or visits asking you to provide internal, private or financial information.

- Read greetings carefully; official greetings usually use your full first and last name, not “Dear PayPal Member.”

- Never provide account numbers without verifying the request.

- Do not share PIN numbers or passwords; even problem solvers do not need this information to help you.
Privacy Statements

- Privacy Statements and User Agreements explain how data that you provide on a website will be used, distributed or shared.

- Read Privacy Statements and User Agreements carefully before providing information on any website.
Avoid Being a Victim

- Double-check URLs
- Retype links in browsers instead of point/click from email
- Check for encryption (https: and a lock icon)
- Check for email fraud notices on valid websites
Spoofed URLs may be long, making only the first part visible in the address bar.

The following procedure can be used to ensure that the site you are visiting is not being spoofed.

• Position your mouse over the link and right click to “Copy”
• Paste the URL into Notepad (or any other text editor). Initiate the URL link and bring up the web page.
• Once on the site, double-click on the padlock icon and check that it is “Issued to” a URL that ends in company.com
Most companies take cyber security threats seriously. Don’t just ignore phishing incidents – Report them to the company whose site is being spoofed.

If you have been scammed or detect any suspicious activity or email, report it to the Federal Trade Commission (FTC)

- File a complaint at ftc.gov
- Visit the FTC’s Identity Theft Website ftc.gov/idtheft to learn how to minimize your risk of damage
- By phone: 1-877-ID-THEFT
- Online Complaint Form: www.ftc.gov/idtheft
IM and Chat

- Do not trust identities in instant messaging (IM) or chat – identities are not verifiable
- Attackers use the “comfortable” space of IM and chat to introduce malicious software
- Communication is public through archived logs of conversations
- Software settings of IM and chat programs are often open and unprotected
Viruses

- Viruses -
Small malicious programs loaded onto your computer without your knowledge, which execute and run by themselves, replicating and spreading outside your control

- Viruses require the spread of an infected host file

- Most viruses quickly use all available memory and hard drive space, causing slow systems and networks
- Worms -

Small programs that replicate from system to system without a host file

- They often spread automatically by taking control of standard computer features that transport files or information
  - They spread quickly, clogging and slowing down networks and may spread private information that was stored on the computers it reaches
- Trojans -

Imposter files that claim to be important or useful, but when triggered cause malicious damage or theft

- They are often spread by files attached to emails with inviting subject lines

- They may destroy files or compromise security.
Anti-Virus Software

- Scans computer or email for specific patterns that identify known viral, worm and trojan infections

- Anti-Virus only works after a new virus has been identified and definitions have been created and loaded onto the computer
OU’s Protection

- **Symantec Campus Anti-Virus Software**
  - Desktops and servers can be protected from a central “push” server

- **Sophos at the email gateway**
  - Scans email for known viruses

- **Stripping email attachments**
  - OU email automatically deletes attachments with specific known carrier extensions (see Helpdesk documents for details)
Often used by the advertising industry

May send pop-up ads, redirect browser to specific websites, or monitor websites you visit

May decrease a computer’s performance

Introduces privacy concerns
How do I know if they are there?

- Common Symptoms of Pop-ups, Adware, Spyware
  - Endless pop-up windows
  - Redirected to websites unrelated to the URL you typed into the browser
  - Changed homepage
  - Unexpected tool-bars or icons
  - Search click results in unknown display
  - Slow computer
  - Banner errors when trying to log-on
Protect Yourself

- Don’t click on links in pop-up windows
- Close the window or click on X when asked unexpected questions
- Be wary of free downloadable software
- Don’t follow email links offering anti-spyware software
Cookies

- Cookies store information to support identity-customized web sites.
- They collect demographic information, website navigation paths, length of time on the site, etc.
- They may monitor what ads you see and how often you see the ads.
Protect with Software

- Adjust your browser preferences to limit pop-ups and cookies

- Make sure cookies are disabled on public computers before you use them

- Use products such as Ad-Aware or Spybot Search and Destroy to scan and delete unwanted files
Conclusion

- Be alert and aware
- Don’t share personal information without checking the request
- Check currency of anti-virus software and definitions
- Know where you are surfing and check out privacy statements
- If you have questions, call the UTS Helpdesk at ext. 4357 or email helpdesk@oakland.edu