

# Essentials of PC Security:

Central Library Tech Center  
Evansville Vanderburgh Public Library



# Why should you be concerned?

- There are over 10,000 known computer viruses.
- Over 200 new viruses are being discovered each month.
- “Phishing” scams have cost Americans over 1 billion dollars in just the past few years.
- An unsecured computer can be more easily infected with viruses.
- Spyware can report your computer usage to strangers.
- Having your computer slowed down or out of commission is an annoying hassle. You paid for the computer and should be able to use it.

# Microsoft Windows Security

## Administrator

- Can create and delete user accounts on the computer.
- Can create account passwords for other user accounts on the computer.
- Can change other people's account names, pictures, passwords, and account types.

## User

- Cannot install software or hardware, but can access programs that have already been installed on the computer.
- Can change his or her account picture and can also create, change, or delete his or her password.
- Cannot change his or her account name or account type. A user with a computer administrator account must make these kinds of changes.

# Administrator or User?

- Administrator accounts have very powerful abilities. Unfortunately, these abilities leave your computer more open to attack.
- Programs and viruses running in an administrator account have all the privileges of an administrator.
- User accounts should be used for day to day computing. Administrative accounts are only used when their powers are absolutely necessary.

# Windows Patches

- Microsoft periodically releases updates and patches for Windows to fix security flaws and update functionality.
- Make certain that you are receiving the latest patches through Windows Update.
- This will help to minimize new threats to your computer.

# Windows Update

How to use Windows Update:

1. Open Internet Explorer
2. Click on the Tools menu
3. Click on Windows Update
4. Follow the instructions to download and install the latest updates for your computer.

# Internet Security

- The three most common ways to connect to the Internet are Dial-up, DSL, and Cable service.
- Dial-up connects through a modem to the telephone line and is only on when that phone number is dialed.
- DSL and Cable are brought in through dedicated wiring and are always on.
- All of these connections expose your computer to the Internet. This makes it possible for other computers to communicate with your system.
- To make certain that your computer can only be accessed by computers that have permission from you, a firewall is required.
- Windows Firewall is a security program integrated into Windows. It is automatically activated and working so long as you do not turn it off.

# Anti-Virus Software

- Viruses are programs designed to harm your computer. They take many forms and are constantly increasing in number and complexity.
- Anti-virus software detects and removes these malicious programs from your computer.
- There are many Anti-virus programs to choose from. Two of the most popular ones are:
  - **Norton Anti-Virus**
  - **AVG Anti-Virus**

# Anti-Spyware Software

- Spyware compiles information about your computer such as what files are on your hard drive or where you have been on the Internet and sends it back to the programmer/user that put it on your system.
- These programs can be used to create pop-up ads on your computer, gather statistical information for companies, or they can be used for spying on you in general for whatever purpose the programmer sees fit.
- Even the programs that reputable companies use can slow down your computer because they are using your computer's resources to run their program.
- There are many anti-spyware programs but two popular ones are:
  - **Ad-aware**
  - **Spybot**

# E-Mail Safety Tips

- When you don't know who the sender is don't open the e-mail.
- Even if the e-mail is from someone you trust, be careful of suspicious links and attachments in the message.
  - The sender may be unaware that the links are harmful.
  - The sender may not be who they appear to be. Some computer viruses will mail themselves to everyone on the infected computer's mailing list!

# Avoid Phishing Attacks

- Phishing is a type of fraud particular to computing.
- Through e-mail or a website you are presented with a link that appears to be credible, but is actually only very close to the real company's web address.
- By asking for personal information or installing malicious software the fraudulent site hopes to gain access to credit cards or other identity information to get your money.
- An easy way to see if the website is valid is to go to: [www.google.com](http://www.google.com) and type in the company's name. The real website should appear in the results. The fake website should not.
- If the website wants personal information, call the real business' phone number from the phone book and ask if they need any information.
- Unless you are certain you are dealing with a reputable business, do not give out personal information.
- The website: [cups.cs.cmu.edu/antiphishing\\_phil/](http://cups.cs.cmu.edu/antiphishing_phil/) has an instructional game to help you spot phishing attacks.

# Secure Submission

- If a company is genuine, you should be careful to only submit your personal information, especially credit card numbers, through a secure website.
- Secure websites will be identified by an icon in the status bar. Internet Explorer will show a closed yellow padlock in the upper right or lower right section of the screen depending on its version.

