Security for Your PC

October 10, 2019

Festival bytes Computer Club

Presented by Harvey Missan

What is Security?

- Security: “The state of being free from danger or harm”

How can we protect our PC from harm”

- Use an Anti-Virus program
- Use strong passwords
- Email smarts
- Smart web browsing
- Backup

Anti-Virus

- Use one
  - Free
    - Avast
    - Defender
  - Pay for
    - Norton
    - McAffee

Passwords

- Use Strong Passwords
  - Select a word or phrase you will remember (8-12+ characters)
    - Make substitutions
      - a - @
      - o – 0
      - e – 3
      - l – 1
      - The quick brown fox
      - Th3 qu1ck br0wn f0x
  - Use a Password Manager
    - One is part of Avast Anti-Virus
    - Dashline
    - Sticky Password
    - Roboform
    - Password Boss
  - Some Websites disable password managers

Email Smarts

- NEVER OPEN attachments from senders you do not know
- NEVER CLICK on links from senders you do not know
- Remove all email address from emails before forwarding them
- Use BCC not CC when sending emails to many people, especially if they do not know each other

Smart Web Browsing

- **Install and use antivirus software**
  - Security experts agree across the board that a good first line of defense is to make use of antivirus software. Antivirus software will detect and remove viruses as well as prevent any new infections. Do your research, choose a software program that fits your needs, and use it.
- **Use a firewall**
  - A firewall is an application that protects your computer from hackers gaining unauthorized access to your computer. Setting up a personal firewall will dramatically reduce the possibility of your computer being attacked by Internet threats

- **Strong passwords are your friend**
  - A strong password is the equivalent of a deadbolt on a door. The more difficult it is to gain entrance to your accounts, the safer your accounts are. Make your passwords difficult to figure out, by using a combination of letters, numbers, and special characters, and most importantly, change them regularly.
- **Update your security software.**
  - It’s not enough to install security software one time; you must install each update as it is made available. Cyber criminals are constantly finding new ways to infiltrate systems and launch new threats, and security software developers release updates to combat this trend.
- **Be wary of clicking links in email or instant messages.**
  - Viruses spread easily through links in instant messages and email attachments. Even if you know and trust the person who sent it, it’s possible the link is infected, and the sender is unaware of it.

- **In fact, be wary of clicking links, period.**
  - Free toolbars, popup windows offering freebies, sidebar ads on websites, links in public forums – clicking any of these could open your computer to a host of issues. Just don’t do it. That free trial of a new game isn’t worth it.
- **Bookmark important sites.**
  - If there are sites you visit regularly, it’s a good idea to bookmark them in your browser. A mistyped address could take you to a false site that mirrors the site you intended to go to, but with malicious code that can harm your computer and compromise your information. Bookmarked addresses take you to the same site every time.
  - Most importantly, realize that the care you take to protect yourself in your everyday life extends to your online life. Don’t share personal information unless you are absolutely certain that where you share it is secure. Be aware that any information you share over a public wireless hot spot (say, at your favorite coffee shop) is not secure and can be seen by anyone looking at information as it travels over that network. Just as you wouldn’t leave your debit card on the dashboard of your unlocked car, don’t make your information easy to attain.

Backup

- Backup your data and backup your system
- Be able to restore system in case of a catastrophic event