CYBER SECURITY

Prof. Palak Patel,
Asst. Professor,
Computer Department
Umiya Arts and Commerce College

INTRODUCTION

- What is Cyber Security
- Terminology
- Cyber Crime
- History
- Threats
- Protection
- Conclusion

CYBER SECURITY DEFINED

Protection of information systems **against unauthorized** access to or modification of information, whether in storage, processing or transit, and against the **denial** of service to authorized users, including those measures necessary to detect, document, and counter such threats.

WHAT IS CYBER SECURITY?

- Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.
- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.
- Though, cyber security is important for network, data and application security.

WHAT IS….?

- Communication security – Protecting organization communication media, technology and content.
- Network security – Protection of networking components, connection and content.
- Information security – Protection of information and its critical elements, including the systems and hardware that use, store or transmit that information.

WHAT IS CYBER CRIME?

- The former descriptions were “computer crime”, “computer-related crime” or “crime by computer”. With the pervasion of digital technology, some new terms like “high-technology” or “information-age” crime were added to the definitions. Also, Internet brought other new terms, like “cybercrime” and “net” crime.
- Other forms include “digital”, “electronic”, “virtual”, “IT”, “high-tech” and “technology-enabled” crime.

CYBER CRIME INCLUDES

- Illegal Access
- Illegal Interception
- System Interference
- Data Interference
- Misuse of Devices
- Fraud

HISTORY

- The first recorded cyber crime was recorded in the year 1820.
- The first spam email took place in 1978 when it was sent over the ARPANET.
- The first Virus was installed on an Apple computer in 1982.

CYBER SECURITY THREATS

- Viruses – Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.
- Hackers - Hackers are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

CYBER SECURITY THREATS

- Identity Thieves - People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.
- Spyware - Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It may also cause a wide range of other computer malfunctions.

CYBER SECURITY THREATS

- Ransomware - Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid and attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment.

PROTECTION

- Install OS Software updates
- Run Anti-Virus Software
- Turn on Personal Firewalls
- Avoid Spyware/Adware
- Protect Passwords
- Prevent Identity Theft
- Backup Important Files

INSTALL OS/SOFTWARE UPDATES

- Updates-sometimes called patches-fix problems with your operating system (OS) (e.g., Windows 7, Windows 10, Mac OS X) and software programs (e.g., Microsoft Office applications).
- Most new operating systems are set to download updates by default. After updates are downloaded, you will be asked to install them. Click yes!
- To download patches for your system and software, visit:
  - Windows Update: http://windowsupdate.microsoft.com to get or ensure you have all the latest operating system updates only. Newer Windows systems are set to download these updates by default.
  - Microsoft Update: http://www.update.microsoft.com/microsoftupdate/ to get or ensure you have all the latest OS and Microsoft Office software updates. You must sign up for this service.
  - Apple: http://www.apple.com/support
- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.

RUN ANTI-VIRUS SOFTWARE

- To avoid computer problems caused by viruses, install and run an anti-virus program like Sophos, Symantec, Norton or AVG.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the Last updated date.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.

TURN ON PERSONAL FIREWALLS

- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Microsoft 7/8/10 and Mac OSX have built-in firewalls.
- Once your firewall is turned on, test your firewall for open ports that could allow in viruses and hackers. Firewall scanners like the one on http://www.auditmypc.com/firewall-test.asp simplify this process.
- Firewalls act as protective barriers between computers and the internet.
- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent your computer from responding to these calls.

AVOID SPYWARE/ADWARE

- Spyware and adware take up memory and can slow down your computer or cause other problems.
- Use a free software such as MalwareBytes, Spybot or Ad-Aware to remove spyware/adware from your computer.
- Watch for allusions to spyware and adware in user agreements before installing free software programs.
- Be wary of invitations to download software from unknown internet sources.

PROTECT PASSWORDS

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.
- Change your passwords periodically (30 – 90 days).
- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a difficult password
- Store passwords in a safe place. Consider using KeePass Password Safe (http://keepass.info/), Keychain (Mac) or an encrypted USB drive to store passwords. Avoid keeping passwords on a Post-it under your keyboard, on your monitor or in a drawer near your computer!

PREVENT IDENTITY THEFT

- Don't give out financial account numbers, Social Security numbers, driver’s license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people’s information as you would your own.
- Never send personal or confidential information via email or instant messages as these can be easily intercepted.
- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. These often do not include a personal salutation. Never enter personal information into an online form you accessed via a link in an email you were not expecting. Legitimate businesses will not ask for personal information online.er a copy of your credit report from each of the three major credit bureaus-Equifax, Experian, and Trans Union. Reports can be ordered online at each of the bureaus’ Web sites. Make sure reports are accurate and include only those activities you have authorized.

BACK UP IMPORTANT FILES

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so you can easily create a back up copy.
- Save copies of your important documents and files to a CD, online back up service, flash or USB drive, or a server.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- Test your back up media periodically to make sure the files are accessible and readable.

CONCLUSION

- The only system which is truly secure is one which is switched off and unplugged.
- The end-user is the last stand against cyber security threats so, the best way to be safe is to be aware and act smart.