DIGITAL SECURITY

Digital Security: Security basics. Password security. Hardware security. Malware. Social engineering. Encryption

1. What are the main types of hackers? What crimes do they perform?
2. What is malware? Describe the most common types of malware.
3. How can hackers get our passwords? Describe the most common methods.
4. What is identity theft? What is software piracy?
5. What should we do to prevent hardware problems?
6. What is encryption?

The Internet provides a wide variety of opportunities for communication and development, but unfortunately it also has its dark side. **Hackers** are computer criminals who use technology to perform a variety of crimes: **virus propagation**, **fraud**, **intellectual property theft**, etc. Hackers differentiate themselves into three groups:

A white hat hacker, or ethical hacker, is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks. **A white hat hacker,** upon finding some **flaw** in a system, will report the flaw to the vendor of that system.

A black hat hacker is the person normally depicted in the media. Once he/she gains access to a system, their goal is to cause some type of harm (steal data, erase files). Black hat hackers are sometimes referred to as crackers.

A gray hat hacker is normally a **law-abiding** citizen, but in some cases will **venture** into illegal activities.

Due to its anonymity, the Internet also provides the right environment for cyber stalking, online harassment or abuse**. Piracy,** the illegal copying and distribution of **copyrighted software**, information, music and video files, is widespread.

Internet-based crimes include **scam**, email fraud to obtain money or valuables and **phishing**, Phishing is a form of **social engineering**, in which a hacker poses as a legitimate representative of an official organization such as your **ISP** or an online payment service in order to persuade you to disclose highly confidential information. When someone gains unauthorized access to your personal data and uses it illegally, it is called **identity theft**. Hackers employ a whole range of ways to steal passwords. The **brute force attack** uses password-cracking software. Because it exhausts all possible combinations of letters to decrypt a password, a brute force attack can run for days to crack some passwords. A **key logger** is software that secretly records a user's keystrokes and sends the information to a hacker.

Malware (malicious software) is software created to damage or **alter** the computer data or its operations.

- Viruses are programs that spread by attaching themselves to executable files or documents. They may exist in the system but will not spread until the user opens the infected program. When the infected program is run, the virus **propagates** to other files or programs on the computer. An email virus spreads by sending a copy of itself to everyone in an email address book.

- Worms are self-copying programs that can move from one computer to another without human help, by exploiting security flaws such as outdated OS or no antivirus installed. While viruses require the spreading of an infected host file, worms are standalone software and do not require a host or human help to spread.

- **Trojan horses** are malicious programs **disguised** as **innocent**-looking files or **embedded** within legitimate software. Once they are activated, they can give hackers access to your system. They don't copy themselves or **reproduce** by infecting other files.

- **Ransomware** blocks the use of your own computer software, files or data until you pay money to criminals behind that act. Then, they may unblock your computer or files.

- **Spyware**, software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software. It usually comes hidden in fake freeware or shareware applications downloadable from the Internet.

ENCRYPTION

If your network is not secured, hackers can easily connect to it, monitor transmitted data, access connected devices, spread viruses, and your network as a launching pad for spam. Encryption transforms a message in such a way that its contents are hidden from unauthorized readers. Encryption is designed to keep messages secret.

Symmetric key encryption uses the key to encrypt a message as well as decrypt it. Symmetric keys are not practical for e-mail and other situations in which the person receiving encrypted data does not have the key beforehand.

Public key encryption eliminates the key-distribution problem by using one key to encrypt a message, but another key to decrypt the message. Public key encryption is a crucial technology for e-commerce and e-mail.

HARDWARE SECURITY

To prevent hardware problems you can undertake some preventive maintenance to extend the life of your computer equipment. Regularly clean your computer components and peripheral devices to keep them in good condition.

A good computer maintenance routine:

- ✓ Back up your files regularly, particularly those that are most important to you. Test your back up procedures periodically.
- ✓ Run utilities that ensure peak performance for your hard disk drive.
- ✓ Delete your browser's history and cache files on a monthly basis in order to free up space for your temporary files. The free space results in faster downloads from the Internet.
- ✓ Apply the latest operating system, driver, and security updates.
- ✓ Scan your computer for viruses and spyware once a week.
- ✓ Keep antivirus and spyware definitions updated.