INTRODUCTION TO INFORMATION SECURITY

The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people’s idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware(Для предотвращения кражи или повреждения оборудования)

- To prevent theft of or damage to the information(
Для предотвращения кражи или повреждения информации)

- To prevent disruption of service(Для того, чтобы не допустить срыва службы)

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and are of growing importance in line with the increasing reliance on computer systems of most societies worldwide. It includes physical security to prevent theft of equipment, and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security", though these terms generally do not refer to physical security (locks and such).

- **Top 10 Cyber Crime Prevention Tips**

1. Use Strong Passwords- Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. Secure your computer

- **Activate your firewall-**Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
- **Use anti-virus/malware software-** Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
- **Block spyware attacks-** Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

3.Be Social-Media Savvy- Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

4. Secure your Mobile Devices- Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

5. Install the latest operating system updates- keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

6. Protect your Data - use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

7. Secure your wireless network - Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

8. Protect your e-identity - be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you’ve enabled privacy settings (e.g. when accessing/using social networking sites).

9. Avoid being scammed - always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

10.Call the right person for help - Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

Principle security

There are six principles of security. They are as follows:

1. Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message.

2. *Integrity:* The confidential information sent by A to B which is accessed by C without the permission or knowledge of A and B.

3. Authentication: Authentication mechanism helps in establishing proof of identification.

4. Non-repudiation:

5. Access control: Access control specifies and control who can access what.

6. *Availability:* It means that assets are accessible to authorized parties at appropriate times

Attacks

We want our security system to make sure that no data are disclosed to unauthorized parties.

- Data should not be modified in illegitimate ways
- Legitimate user can access the data
- *Passive attacks:* does not involve any modification to the contents of an original message
- *Active attacks:* the contents of the original message are modified in some ways.