Cybersecurity

©Абдулхаметова Н.Н.
преподаватель иностранного языка
АК СибГУ им. М. Ф. Решетнева

Cybersecurity

Internet crime

Malware

Preventative tips

Internet crime

The internet provides a wide variety of opportunities for communication and development, but it also has its dark side.

Crackers, or black-hat hackers, are computer criminals who use technology to perform a variety of crimes.

Internet-based crimes

Scam

Email fraud to obtain money

Phishing

Bank fraud to get passwords of internet bank accounts or credit card details

Other examples of internet crime

- Cyberstalking
- Online harassment or abuse mainly in chat rooms
- Piracy

Malware

Malicious software created to damage or alter the computer data or its operations.

Viruses

Worms

Trojan horses

Spyware

Types of malware

- **Viruses** are programs that spread by attaching themselves to **executable** files or documents. Some viruses are designed to work at a particular time or on a specific date.

- **Worms** are self-copying programs that have the capacity to move from one computer to another without human help by exploiting security flaws in computer networks.

- **Trojan horses** are malicious programs **disguised** as innocent-looking files or **embedded** within **legitimate software**. They may create a **backdoor** to the computer which can be used to collect stored data.

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

Preventative tips

- Don't open **email attachments** from unknown people, take note of the file extensions;
- Run and update **antivirus programs**;
- Install a **firewall;**
- Make backup copies of your files regularly;
- Don't accept files from high-risk sources;
- Use a **digital certificate**, an electronic way of providing your identity.

Identify the internet crime

- Crackers try to find a way to copy the latest game;
- Half a million people automatically open an email they believe to be from their bank and happily send off their security details;
- This software's danger is hidden behind an attractive appearance. That's why it's often wrapped in attractive packages promising photos of celebrities;
- There is a particular danger in Internet commerce and emails. Many people believe they have been offered a special gift to find out later they have been deceived;
- 'Nimda' spreads by sending infected emails and is also able to infect websites, so when a user visits a compromised website, the browser can infect the computer.
- *Identify the types of crimes and suggest your solutions.*

You and computers

- Answer questions about you

1. What do you do to prevent computer infections?
2. What do you do to keep you virus protection updated?
3. What should you do to improve your computer security?

- Do the quiz and find out your result.

More information

Think of the following statements. Are they true or false?

- 1. Keeping information locked is as important as locking a house or a car.

- 2. It's OK to use one and the same password for different websites.

- 3. There's more than 1 way to secure personal information.

Watch a video and check your predictions.

Video exercises

Ex. 1 Watch a video again and complete the gaps.

1. When it comes to information we tend to be less _____.
2. Most of us have a huge amount of data on computers, smartphones, _____ and on paper.
3. We need _____ for everything we use these days.
4. Criminals _____ usernames, passwords from _____ sites.
5. Using _____ passwords is important.
6. _____ makes it almost impossible for criminals to use the data.

Video exercises

Ex. 2 Watch a video and answer the questions.

1. What kind of address do encrypted websites have?
2. What does tailgating mean? What can be result of it?
3. Which software will prevent identity theft?
4. What is the first way to secure personal data?
5. Are the people always aware of everyday information profit?

Thanks for your attention