INTERNET SECURITY

Belonozhko Y.E.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Sinkevich L. E. – Senior Lecturer

Annotation. Some advice how to secure your data and your computer on the Internet is presented in the paper.

Keywords. Security, Internet, protection, viruses.

Nowadays, when we live in the era of information technology, everyone has access to the Internet. On the internet, we can find a huge number of videos created to teach you what you really want to do. The Internet is a place where you can express your opinion, share experiences, communicate with friends,

being thousands of kilometers from each other However, we may face various problems such as data theft, cyberbullying, inappropriate content, spam, and access to confidential information.

In order to avoid difficulties, you should think of Internet security today.

1. You cannot completely delete all data about yourself, but you can control new photos, videos and texts that you post on the Internet. Do not share what may later be beneficial to attackers.

2. Be attentive. In order not to overload your brain with unnecessary tasks, you should be careful with advertising and spam in your mailbox. Most sites and social networks automatically agree to send you "update news" when you register, but if you always carefully check all the checkboxes, you can avoid 90 percent of unnecessary emails and notifications.

3. Use strong password. Surely, one of your friends uses his phone number, birthday or other well-known data in his password. Such a password is easy to guess after several dozen attempts. A password consisting of random uppercase and lowercase letters is impossible to guess. You can use a password generator. You should use different passwords for different social networks, because if you have only one password, a hacker will gain access to all existing accounts. You should remember that the Internet mailbox (the email you use on the Internet) is vulnerable. After gaining access to it, the hacker will be able to restore access to your passwords in other social networks and passwords. Think of a separate password for the mail and remember it well [1].

4. Use only verified, official sites. Most often, the sites created by hackers to steal your data are hard to distinguish from real ones. They use the same logos, input fields, advertisements and names. Often, a notification may pop up on social networks stating that the account has been blocked and in order to restore it, you need to sign in again. Carefully check the address of the site, does it match the real one, does it have the same domain? If you enter your personal data, you assume that you send hackers an email containing your username and password directly to hackers.

5. Be careful with software. Often users want to download the program free from unofficial site. It is possible that you can actually install this software on your computer and it will work, but it does not guarantee that malware will not be installed with it. To avoid this, install only legitimate software. Most often, the program needs to be bought once, but by paying money, you get a guarantee for the safety of your personal computer.

6. Use antivirus software. Antiviruses will help you detect and eliminate threats much faster. However, you should understand that they may not always work correctly and sometimes block the files you really need, maybe even the files you have created. However, look at antivirus from the positive side and install one from the suggested ones on your PC to reduce the risk of attacks [2].

In conclusion, remember that on the Internet hackers use not only the vulnerability of your computer, but also the vulnerability of your human qualities, gullibility, laziness, and self-interest. Therefore, you should be careful.

References:

1. Topics of National Institute of Standards and Technology
2. Topical Materials for Creative Presentation: пособие / М. В. Ладыженко [и др.]. – Минск : БГУИР, 2015
3. Wikipedia