DOI:10.4467/25436104HS.20.010.13243

Andrei Șestacov
ORCID: 0000-0001-5395-6135
Military Academy Of The Armed Forces, Republic Of Moldova

CYBER SECURITY DEFICIENCIES IN THE EDUCATION ENVIRONMENT

Abstract
Information technologies have already radically transformed the communications and information technology sectors, trade, media, and the education sector, especially education, which is on the top priority. Digital technologies will radically change the way data is sent and retrieved, will allow immediate and real-time feedback from students, will facilitate access to education through distance learning, will allow new service providers to enter traditional markets education. Thus, a diligent and well planned implementation of cyber security, as well as information security of information networks of educational institutions will provide a definite competitive advantage in the information environment.

In the context of a dynamic information environment prone to large-scale cyber-attacks, in which cybercriminals are using increasingly advanced methods to implement attack vectors that are undetectable and difficult to neutralize, this scientific study is designed to protect data and security of your institutions as well as to ensure the confidentiality of your students and teachers.

Whether we are talking about large or small educational institutions, this study provides a series of recommendations on the secure use of social networks with a minimum set of measures needed to prevent cyber-attacks as well as reduce the damage caused in case of attacks. At the same time, it will examine the best practices in the online environment, effectively analyze the privacy settings of mobile devices and present some top tips for the secure use of social networks.
The study aims to comply with the following minimum set of measures in order to prevent cyber-attacks in educational institutions, and reduce the damage caused in the event of attacks.

Keywords: cyber security, software, passwords, risk, information, virtual private networks.

Tips and recommendations on the safe use of social networks

Social networks, such as Snapchat, Facebook, Twitter, Instagram, and LinkedIn are amazing resources that allow us to meet, interact, and share things with people around the world. However, there are risks, not only for you as individual, but also for family, friends, etc. In this scientific publication, we will cover the key steps to make the most of security in the information media space.

Posts

Be careful and think before you post anything. Any post will become public at some point, which can affect your reputation and future or the organization you belong to. The more information you publish about your personal life, the easier it is for a criminal to personalize an attack on you.

For example, if you post extensive information about your confidentiality, integrity or availability – an attacker could collect all those specific details and create a phishing email or phone call that would target you in particular.

If you still think it's a real message and you don't have any suspicions, then you should know that you just got rid of the extra problem.

Passwords

Protect your data The best way to protect each individual account on social media is to use a strong and unique password for each account. An access phrase consisting of a collection of multiple words can serve as a password, making them easy to type and remember.

For example, instead of using "*123456789*" as your password, an effective password might be "*RomeoIndia ^ $!*". Using a single passphrase for each account ensures that if one account is compromised, the others remain secure. If you can't remember all your passwords, you can use a password manager that will keep your passwords safe.

Weak and easy-to-guess passwords are the most vulnerable to cyber-attacks. The perpetrators can easily break and take over your personal information, if you have the same passwords.

Confidentiality

Whenever you choose to post personal information in the information environment, it is good practice to assume that any information you publish may become public. Avoid sharing sensitive or private details about yourself.

It is also wise to avoid posting pictures of yourself that wouldn't be appropriate with the policy of your company or sensitive for your family. When you register on a social network, the first step must be to activate and personalize privacy controls. Although it can help, keep in mind that they can be confusing, can often change, and may not fully protect your information.

Don't assume that once you've set these privacy settings, your account is fully protected. Having the latest security software, web browser, operating system and applications is the best defense against malware and other cyber threats.

Always be careful with other accounts, they may be compromised as well. After breaking the account, they can access your contacts, personal information, photos, messages, important data, etc. These security measures can also help protect your information in case your devices are lost or stolen.

To further protect yourself, always turn on multifactor verification (sometimes called two-step verification or two-factor authentication) whenever available. Multi-factor authentication is done when you are given access only after you have successfully provided two or more proofs, such as a password and a unique code generated by your smart phone, which will then be sent by email.

Third-Party Applications

Your mobile devices are just as vulnerable as your computer or laptop. Many of the social networks or their applications for mobile devices also support and support third-party applications. Check the details when downloading an application or registering for a new network. Only install apps from trusted sources as well as the ones you think you need. Make it a habit to check the ratings, reviews, and permissions of any application before choosing to install it. It could be very suspicious if a new application has few or negative reviews, or very few downloads. In this case, it would be wiser not to install such applications.

It often happens that you download an application for specific, short-term purposes, such as planning a vacation or renovating a home. Perform regular audits on your apps. If you no longer need an app, uninstall or disable it from your social networking profile because it may collect data about you.

In the end, you are the best defense. If you have suspicions about the Wi-Fi connection, avoid connecting. Find another Wi-Fi network that you feel more secure with, or share one from your mobile device. If you receive an email, message or phone call that seems strange or suspicious, especially the extremely urgent ones, then you are most likely at risk of being the victim of a cyber-attack. Be careful and always on the alert. It is unethical to tell people at work to never use public Wi-Fi.

The goal is to manage your human risk by allowing people to insure themselves in ways that anyone can follow. The next time you travel and need to connect to Wi-Fi, try to keep these four key behaviors in mind.

Safe browsing

Business trips or rather business meetings can be easily compromised. The security risk you are exposed to is very high. And that's because you always have to connect to WIFI networks in the public space where you are. The information transmitted through public networks can be easy regardless of the device used: smart phone, laptop or tablet. Therefore, when you want to connect to a public network, it's best to limit it as much as possible.

Updated systems are much more difficult for cyber attackers, which is why it is advisable not to ignore the system update recommendations. So in many cases, enabling and setting up automatic updates is one of the easiest ways to make sure your system stays protected and secure. In addition, before installing any software, plugins, or extensions, be sure to check your institution's security policies and procedures to ensure that the programs are authorized.

Encryption is a technique that helps protect your information when it is transmitted over information networks

When you connect to public Wi-Fi hotspots, you want to make sure all your online activity is encrypted, making sure others can't monitor or capture what you do online. For example, when browsing the web, you want to make sure that your browser is connected to encrypted websites. Not sure if your browser connection is encrypted? Pay attention to the top of your browser. If you see a padlock or HTTP near the site address, this is an indicator that your connection to the site is encrypted.

Portable hotspot

Mobile data sharing, also known as mobile hotspot, refers to the act of connecting one device such as a smartphone or tablet, to another one such as a laptop, so that you can share your mobile data connection between devices when no Wi-Fi network is available.

When in doubt about the security of a public Wi-Fi network, it's a good idea to connect your mobile data sharing to your smartphone instead of using a public Wi-Fi network.

One of the simplest and most efficient ways to encrypt your entire online activity is to use a virtual private network (VPN). The technology behind a VPN creates a private, encrypted tunnel for your online activity, making it much more difficult for anyone to track or monitor your online activities. A VPN can also help you hide your location, making it much more difficult for the websites you visit to determine your exact location.

Virtual Private Networks (VPNs)

You may feel compelled to use the public Wi-Fi network to access the internet when you are away from home.

But how secure are these public networks and who tracks or records your online activity? You may not even trust your ISP (Internet Service Provider) at home and want to be sure they can't monitor what you're doing online. Protect your online activities and privacy with a virtual network called a VPN. It is much more difficult to track and monitor your education process. In addition, a VPN helps you hide your location, which makes it difficult to identify the websites you visit.

How does it work? A VPN works by creating a private encrypted tunnel to a VPN provider you select. All your online activity goes through this tunnel, then leaves your VPN provider's network to the desired destination. For example, if you are based in Tampa, Florida and connect to a VPN server in Warsaw, Poland, any website you connect to will think you are connected from Warsaw, Poland. Using a VPN is very simple. The first step is to identify a potential VPN provider and then establish a contract with it. Once you have acquired an account, you can download, install and configure the VPN software. Once installed and configured, you can connect to the Internet. The VPN software will silently create your encrypted tunnel and begin protecting your privacy.

Select a VPN provider

Your online activities are as secure and private as your VPN provider. Make sure you select one that you can trust. Here are some key issues when selecting a VPN service provider.

LOGGING IN

If your VPN service provider doesn't collect logs, it's much harder for anyone to come back and see your online activity. Where the company is based: Different VPN providers are based in different countries. Make sure you select a VPN provider based in a country that has strong privacy laws. VPN providers in countries with poor privacy laws may be required to discontinue the information they collect about you.

SERVERS

Look for a VPN service that has servers located in the countries or cities you need. Some VPN providers have thousands of servers and locations around the globe. Do you need to make your connections appear as they are from a particular country? Can the VPN provider offer this?

COMPATIBILITY

Look for services that work on different computers and mobile devices. For example, you can use a Windows Laptop, a tablet, and an iPhone. You will want a VPN service that works on all of these devices.

AVOID FOR FREE

Be very careful with "free" VPN services; how do I make money and stay in business? Free services can collect and sell your information. A VPN is a great way to help protect your online privacy [8]. However, a VPN does nothing to secure your computer, devices, or online accounts. Even if you're using a VPN, make sure you always follow basic security steps, including keeping your devices up to date with a lock screen and strong passwords that are unique to all accounts.

Many of students and teachers choose to shop online for various electronic materials and components looking for great deals and avoid long lines and impatient crowds. Unfortunately, this is also the time of year when many cybercriminals create fake shopping sites to deceive people. While many online stores are legitimate, there are a few fake websites created by cybercriminals. Offenders create these fake sites by falsifying the appearance of real sites or using the names of well-known stores or brands. Then they use these fraudulent websites to deceive people who are looking for the best possible offer. When you search for the lowest prices online, you can access one of these fake sites.

Protect yourself by doing the following:

- Buy from websites you already know, trust or have previously used

- Verify that the website has a legitimate mailing address and phone number for sales or support questions. If the site looks suspicious, try calling. If you can't contact anyone, this would be the first sign that the site is fake.
- Look for obvious warning signs, such as offers that are too good to be true or with grammatical and spelling mistakes.
- Enter the store name or URL in the search and see what other people have said about this website. Look for terms like "Fraud", "never" or "fake". Lack of reviews can also be a sign that the website is new and may not be trustworthy.

Cybernetic security is increasingly used in teaching, research, and institutional management. Computerization is an absolutely necessary tool, which capitalizes on the work capacity and creativity of students and teachers, while reducing the workload by automating processes.

The implementation of these useful cyber security tips is based on a clear vision and efficient management. Thus the study of policies and objectives to ensure information security aims to establish a modern, open and transparent management, based on results, involving all tools and decision makers, but also teachers, students, as direct beneficiaries of the cybernetic security process of information networks of educational institutions.

Cyber security provides support for all communication processes carried out in the university environment, so it will aim to implement a reliable and well-structured information system, based on electronic communication, aimed at providing accurate information and data in real time. This transformation will allow teachers to bring a modern breath and better results in the educational and academic process, through innovative experiences of cyber security in the information environment.

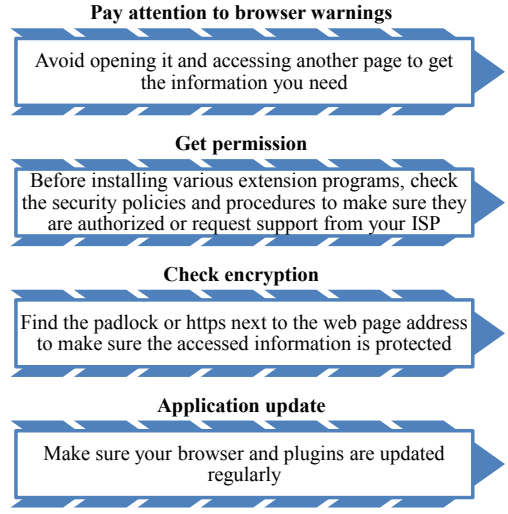

Fig. 1. Four simple steps to navigate the information environment

Conclusion

Based on the theoretical-scientific analysis on the topic, it was found that the problem of cyber security becomes particularly acute at the level of educational institutions where sensitive information is managed, which can lead to compromising confidentiality, integrity or availability of this information.

Therefore to the causing of financial or other damage, including to the impairment of national security, for which it is characteristic, the preparation and commission of cybercrime, acts of cyber terrorism and other malicious acts intended to affect, directly or indirectly, national security. Also, the penetration of information systems related to the critical infrastructure of the Republic of Moldova may lead to obtaining unauthorized control over these systems, and consequently, to affecting the economic, social, political, information, military, etc. processes.

At the same time, the global nature of information systems and electronic communications networks, as well as the transnational nature of cybercrime requires close coordination between all educational institutions at national and international level. Information and communication technology is developing rapidly; accordingly, new methods of information protection are emerging as fast.

References

Action plan on the implementation of the National Strategy for the development of the information society "Digital Moldova 2020". Retrieved from: https://mei.gov.md/sites/default/files/anexa_i_hg_857_md.pdf p. 14

Clarke R.A., Knake R.K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco.

Dumitru O. (2003). *Information protection and security*. Iaşi: Polirom Publishing House.

Information Technology and Cyber Security Service. Retrieved from: https://stisc.gov.md/

Ion R. (2007). *Friends and enemies of software – about viruses and antiviruses*. Bucharest: Publishing House of the Academy of Higher Military Studies.

Iulia I. (2013). *Cyberterrorism Handbook "A New Form of Terrorism"*. Bucharest: Publishing House.

Kizza J.M. (2017). *Guide to computer network security*. London: Springer.

Mihai I.C., Petrică G. (2014). *Information security*. Sitech: Publishing House.

National Cyber Security Program of the Republic of Moldova for the years 2016-2020. (2015). Official Gazette no. 306-310/905.

Rid T., McBurney P. (2012). Cyber-Weapons. *The RUSI Journal*. vol. 157, no. 1, 6–13.

Cyber-bezpieczeństwo w obszarze edukacji

Streszczenie

Technologie informacyjne radykalnie przekształciły sektory komunikacji, handlu, mediów i edukacji. Technologie cyfrowe zmienią sposób przesyłania i wyszukiwania danych, umożliwią natychmiastową informację zwrotną od uczniów w czasie rzeczywistym oraz ułatwiają dostęp do edukacji poprzez kształcenie na odległość. Zatem rzetelne i dobrze zaplanowane wdrożenie cyberbezpieczeństwa, a także bezpieczeństwa informacyjnego sieci informacyjnych placówek oświatowych zapewni zdecydowaną przewagę konkurencyjną w środowisku informacyjnym. Artykuł ma na celu przedstawienie środków zapobiegawczych przeciw cyberatakom w placówkach edukacyjnych i ograniczania szkód wyrządzanych w przypadku takich ataków.

Słowa kluczowe: cyber-bezpieczeństwo, edukacja, oprogramowania, sieci internetowe, hasła internetowe.