# PRACTICAL CONSIDERATIONS FOR A SAFE E-LEARNING PROCESS

*Alexandru TĂBUȘCĂ*[1]
*Cristina COCULESCU*[2]
*Mironela PÎRNĂU*[3]

**Abstract:** *Considering the current pandemic context of 2020, it is of utmost importance for both students and teachers to know that in the online environment there are a plethora of threats, risks and vulnerabilities, all specific to most informatic environments. Because the internet and the mobile technology represent the main element for a successful continuation of the educational process during the Covid-19 pandemic, all users of a computer or similar device are in dire need of information and awareness regarding the informatic security topic.*

**Keywords:** *social network, cyber security, e-learning, computer security, homework, teleworking*

## 1. Introduction

In the current conditions, the professional and personal activities of a very large number of people are now very much interconnected through modern communication technologies. Electronic devices, mobility and the cloud concept all contribute to the increase of quality and efficiency of different tasks, of the collaboration level, but also to a growing culture of "easiness".

The main effects of this new tendency are the, on one hand, the facilitation of most legit/normal actions, but also the facilitation of cyber-crimes. Those illegit actions are also commercialized on an illegal market based on selling and exploiting sensitive data/information – a quite profitable market.

The cybersecurity concept tries to prevent such crimes, monitors its specific activities, and reacts to attacks. Specialists in this field protect IT infrastructure, including hardware devices, networks, data, and software applications.

In the case of the teleworking activities, with an abrupt increase during the Covid-19 pandemic, the European Union Agency for Cybersecurity recommends a set of items considered necessary for a "cybernetic hygiene". Recommendations to this

[1] PhD Associate Professor, Romanian-American University, School of Computer Science for Business Management, tabusca.alexandru@profesor.rau.ro
[2] PhD Associate Professor, Romanian-American University, School of Computer Science for Business Management, coculescu.cristina@profesor.rau.ro
[3] PhD Associate Professor, Titu-Maiorescu University, Faculty of Informatics, mironelapirnau@yahoo.com

topic are addressed both to employers as well as to the employees which work under such conditions. At international level there are also other highly regarded organizations that emitted their own updated guides for cybersecurity and teleworking, such as the NIST[4].

In order to avoid the negative consequences of the cybernetic attacks the below recommendations are to be considered:

- avoid using technologies and software solutions which do not benefit of current maintenance/development (e.g., Adobe Flash, Java Applets etc.)
- define complex usernames and passwords for a more secure access to IT infrastructures
- make a physical separation between the internal network (intranet) and the external one (internet)
- use updated antivirus/security suites on all devices, including mobile phones
- update the operating systems and applications used for monitoring/supervising the IT infrastructures
- make regular backups of data and store them safely, in a different physical location
- ensure a safe usage of external memory devices, such as CD/DVDs, USB drives etc.
- do not install or operate software without proper licensing and support
- use detection and prevention of intrusions systems (IDS/IPS)
- do not open email messages, and especially attachments from these messages, which are not veridic
- avoid accessing direct links from within email messages if the message itself is not completely legit and traceable
- avoid filling in with personal data in webpages
- avoid using unrestricted access Wi-Fi networks
- it is recommended that users should use unique credentials, with timed expiration preset, when accessing the internal WLAN
- all WLAN networks should use encryption, at least WPA-2 standard.

## 2. Improving the security of a computer device

Because computers today have a huge role in our day-to-day lives, both professional and personal wise (payments, shopping, e-learning, socializing etc.), it is of utmost importance to improve their security levels so that we can depend upon them and keep our data safe. Among the methods that we deem necessary for such a goal we can mention:

[4] www.nist.gov

- Router safety, in order to ensure the computer's safe access to networks. The security of the router is based on the user manual of the respective device, by using the web address for its administration interface, which should allow the following: choosing an encryption method for the data circulated through the wireless network (at least WPA2-AES), changing the username and password for accessing the router's administration interface, hiding of the wireless network identifier (SSID).
- Activating and configuring the firewall. Most modern operating systems include a software firewall. Most wireless routers also have a software firewall built-in. A strong password should be used to protect the access to the firewall settings. The firewall offers protection against external cyber attacks by protecting the access to the network/computer from useless/malevolent network traffic. Firewalls can also stop the access to a computer or network from the internet, as well as the access from that item to the internet. Firewalls can be configured to block certain locations (network addresses), applications or ports, while permitting access for legit and relevant data. There are two large categories of firewalls: software and hardware. Even though they do have differences, advantages and disadvantages based on specific scenarios, the decision to use a firewall is much more important that choosing a certain category for it (Securing Network Infrastructure Devices, 2020).
- Installing and using an anti-virus software. Any software / security suite must be continuously updated. Such an application can detect malware (Increased Emotet Malware Activity, 2020) by regularly verifying the memory and the files on the device and looking for known code sequences. These applications use signatures of the known viruses and malware apps. As new malware and viruses appear daily, these signature sets must also be updated continuously. After installing a security suite, you should periodically scan the entire device (Understanding Anti-Virus Software, 2020). All antivirus programs can be configured to run automatic scans of different files/folders/discs in real-time and run full scans at predefined times. All antivirus programs also have the possibility to manually scan a certain file/folder/disc before using them.
- Removal of unused applications. After checking that an application is really not used anymore, removing such applications increase the level of security by removing a potential security risk. Removal should be done only after making backup copies as a safety measure. If possible, keep the physical media from which the application was initially installed (CD, DVD, USB drive etc.), in case you later decide to reinstall it.
- Deactivating non-essential services. Deactivating operating system services is a high-level step and should be done only after a thorough verification and only by experienced personnel. For example, two of the most common services in the Windows environment are those for file

sharing and printer sharing – in case you are sure you will not need them at some point (or make sure you know how to re-enable them) one can deactivate them and thus reduce the risk of an attack by the way of such insertion point.

- Modifying the default features of the operating system. This thing can also translate into a higher level of security by eliminating another set of attack vector. Carefully evaluate the features that are activated by default and stop or personalize them. As in the case of non-essential services, this step requires extensive knowledge in the field. For example, the Auto Run facility in the Windows environment was activated by default at the time of the Conficker virus, a thing that greatly helped the virus spreading. When this feature is activated, it permits the automated running of certain applications when you connect a CD/USB drive to your device.
- Use the device based on the principle of necessary privileges. In order to minimize the impact of malware in case of an infection, it is advisable to currently use a standard user account on your operating system, with basic rights and privileges. The administrator user should be used only when you install new applications or need to make modifications to the specific settings at operating system level.
- Securing the web browser. This step is critical for improving the security today, especially when an ever-increasing number of attacks are based on browser vulnerabilities. The main stage of securing a browser is to deactivate (as much as possible) dynamic code execution (e.g., Java applets, Flash, ActiveX or JavaScript) for new websites or those that you do not trust. Nevertheless, keep in mind that this step, while greatly ensuring an increase in security, might also come with a degraded level of usability for some websites which heavily rely on such technologies. Another similar step would be to deactivate (as much as possible) the cookies usage. This thing might allow an attacker to find out your credentials and replicate your access of a previously legit access to a website (for example, an online banking system).
- Activate the automated security updates. Most software producers offer periodical updates that solve vulnerability issues related to their products. Because wrong doers can exploit such problems to attack an electronic device, the automatic update of all software is an important step in increasing the overall level of security. Most operating system and important applications have the possibility to automatically update. Try to set these automated features on, every time you install a new electronic device or software application. Keep in mind that cyber criminals can create website that look very similar to the original ones, and manually downloading updates from a website might bring home an unwanted and tainted application. It is advisable to use only the producer's website or

automatic downloads for such operations (Understanding Patches and Software Updates, 2020).

- Carefully use the email attachments or in-message links. Malware is usually transmitted through people opening email attachments or links that trigger the malware. Some malware applications use the infected devices to further spread their messages. Even if an email appears to originate from a known sender, it is possible and in fact very easy for a cyber criminal or an infected device to masquerade as a legit sender name.
- Pay attention to handling personal or sensitive information. Even if it would be much more comfortable to just tell your password to somebody else and ask him to do something in your place this is a very big security breach.
- Use secure passwords. Do not use passwords that can be easily guessed by others, such as birthdates, child name, significant years etc. There are applications dedicated to cracking passwords that will try attacks by using words from dictionaries until your password is found. The lengthier and the more complex the password, the longer it takes for such an application to work. Moreover, when configuring security questions do not select answers which can be found easily on the internet.
- Consider encrypting the emails. This would greatly increase the security level of your correspondence (The small business guide to secure email, 2019)
- Make sure your passwords are secured. Each employee must have his own password for a certain device or email account. This must be changed every three months, and, for a better security, a multi-factor authentication system should also be deployed for the process of password changing. The standard password today should be at least 12 characters long and include a combination of figures, small and capital letters, and symbols. Passwords must not be some evident possibilities but should be easy to memorize.
- Create policies for archiving email messages at preset times (15-30 days) and deleting non-important messages at predefined times.
- In case of using a mobile device (either from work or personal) for sending/receiving institutional emails, employees must encrypt data, keep the device access restricted with at least a password/pin and install approved security software, so that potential cyber criminals could not easily access the shared Wi-Fi networks.

Even now, the world is preparing to change the entire electronic communications paradigm by implementing the new 5G mobile networks. The huge increase in speed and features will bring electronic communications to virtually any new electronic device and in all modern cars. Observing the impact of the cyber security concepts will become a must for all users and producers, as a potential security breach will become a thousand times more important in the future all-linked scenarios.

If a security breach of a home router today is an important issue but (in probably more than 99% of the cases) it is not something critical, think of such a similar breach that would enable a cyber terrorist to take control of a 5G networked car thousands of kilometers away. In the first case the privacy breach might bring some unpleasant personal details under the public scrutiny, while in the second scenario a paranoid terrorist from Iran or North Korea can take control of a bus in New York, drive it into a public square and produce a massacre, all from the safety of its rat hole across the world.

## 3. The flux of web searches for telework and security

Google Trends is a free tool that allows us to analyze data based on searches made by Google users as well as by using its services, including YouTube.

By using Google Trends, we have analyzed the tendency of searches, for the last five years, of the terms "cyber security" and "teleworking". In Figure 1 and Figure 2 below, we can see a huge increase of the interest in searches for "teleworking", while the general "cyber security" search is more stable.

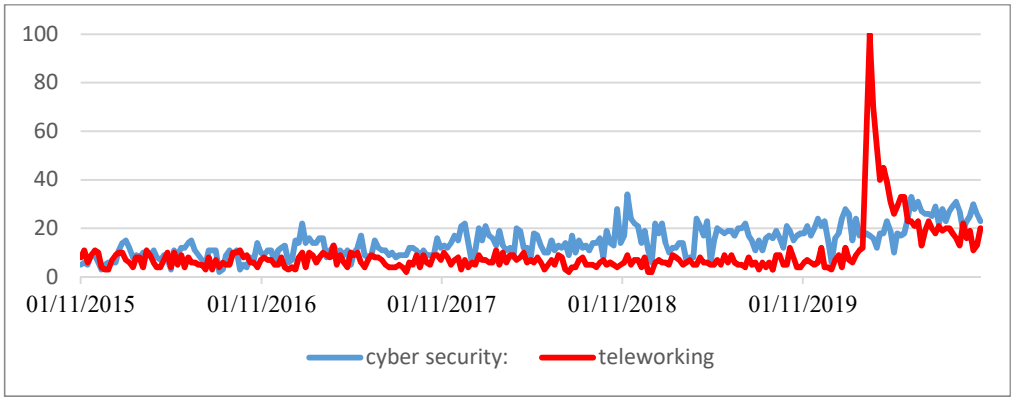


Figure 1. Tendency of searches for the terms "cyber security" and "teleworking" during 2015-2020

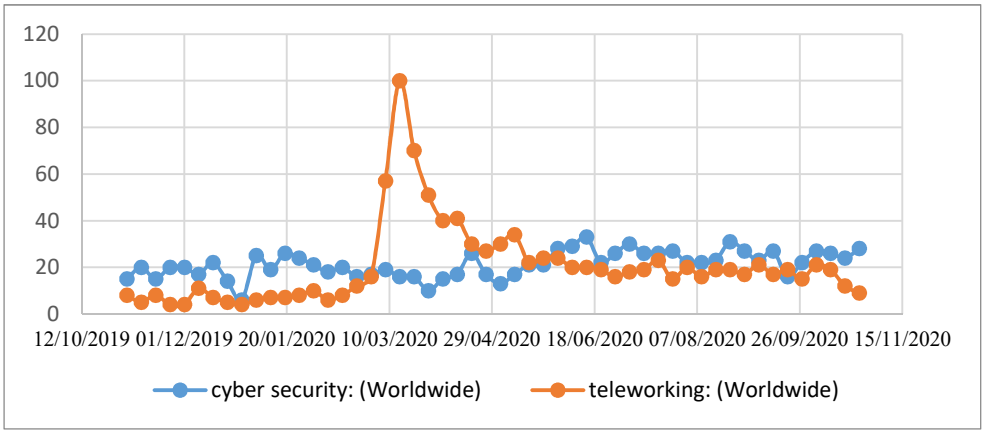


Figure 2. Tendency of searches for the terms "cyber security" and "teleworking" during 2019-2020

The tendency for searches during the last five years of the terms "elearning" and "teleworking" is presented in the Figure 3 and Figure 4 below. By analyzing the images we also see a huge increase for "elearnin" term after march 2020, a phenomenon due to the world health crisis of the Covid-19 pandemic.

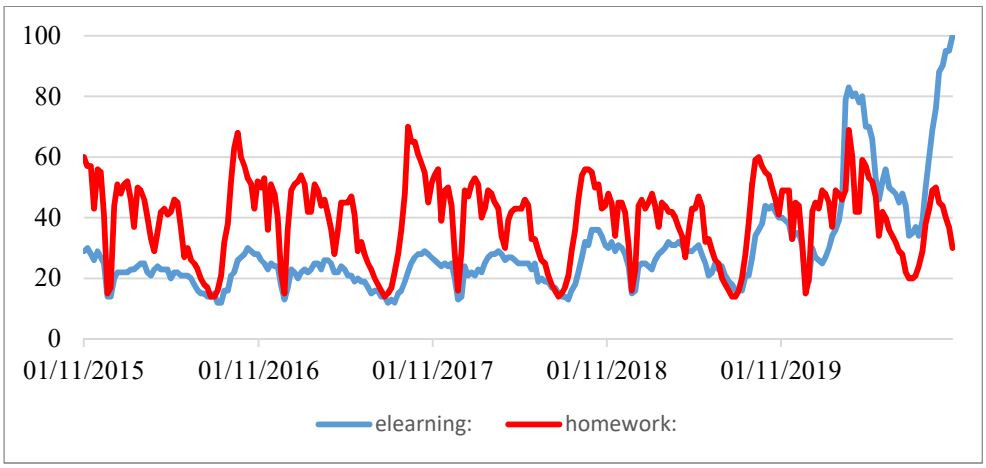


Figure 3. Tendency of searches for the terms "elearning" and "teleworking" during 2019-2020

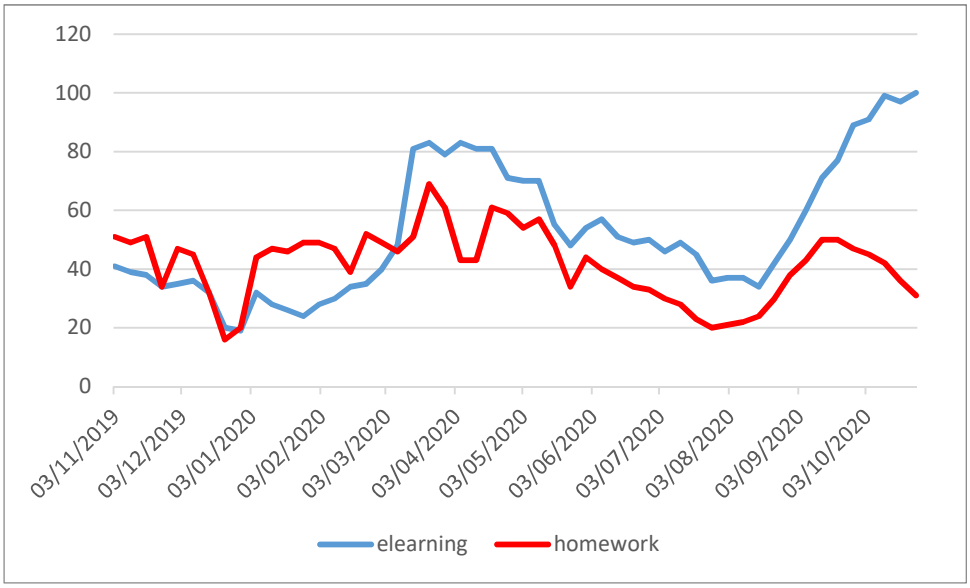


Figure 4. Tendency of searches for the terms "elearning" and "teleworking" during 2019-2020

Going further, we have analyzed the tendency of searches for the topics of "social network", "cyber security", "elearning" and "computer security". The images show that, while the generic preoccupation for the "elearning" existed before, after the start of the current pandemic the world interest for "elearning" spiked exponentially – see Figure 5 and Figure 6 below.

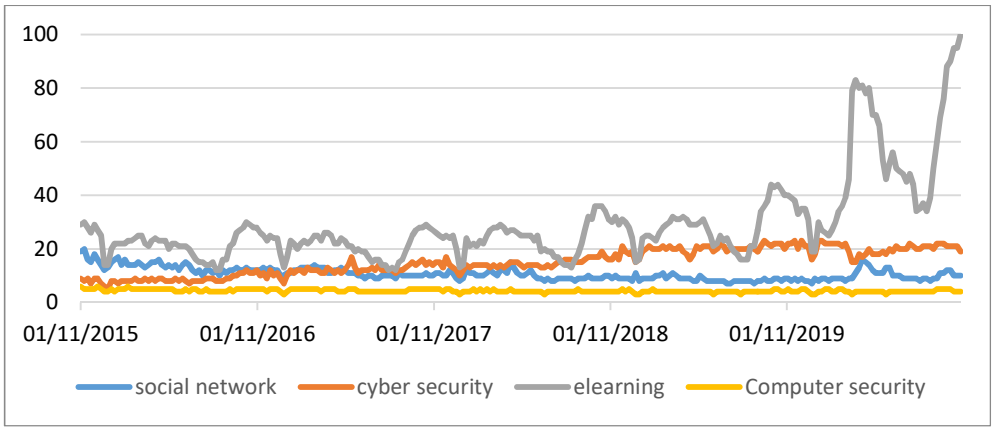


Figure 5. Tendency of searches for the terms "social network", "cyber security", "elearning" and "computer security" during 2015-2020

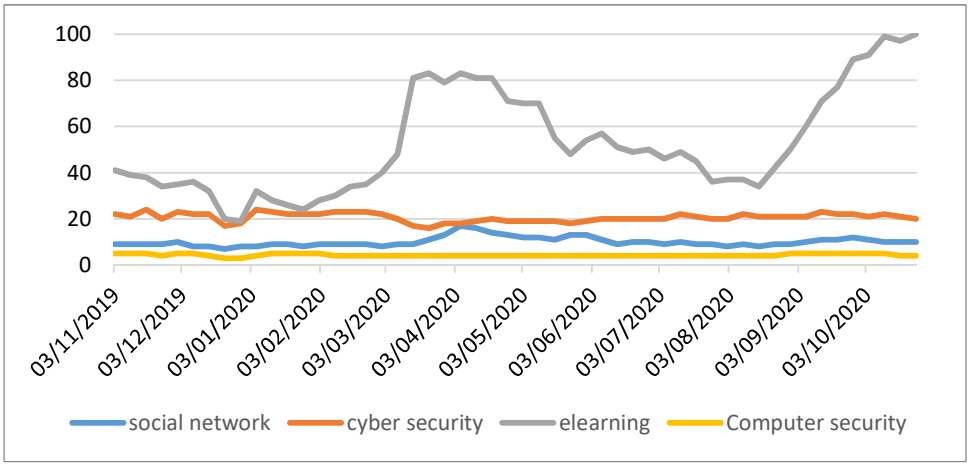


Figure 5. Tendency of searches for the terms "social network", "cyber security", "elearning" and "computer security" during 2019-2020

Comparing all these tendencies, we can accurately sustain that the e-learning and the teleworking activities have greatly increased during the last year. Regardless of the type of activity, e-learning or teleworking, all online processes must make use of an ever-increasing security paradigm.

Our opinion is that even after the end of the current pandemic the developed countries will continue to make extensive use of online activities where it is most suitable. Even in the educational field, although at the present time most actors seem completely fed up with the online options, we think that the future is a carefully balanced mix of online and face-to-face experiences, taking the best parts of every option and creating a new, superior and more secure blend.

## 4. Conclusion

Even though no individual step will ever be able to eliminate all risks, when all steps are used together these practices will consolidate the security of your online environment and will greatly heal you mitigate and reduce most threats and risks.

In a world where the access to the internet is more and more viewed as a standard right for any citizen (Tăbușcă, 2010), in a world where anybody and everybody is relying more and more on electronic devices and online communications – there is an absolute and permanent need to increase the security levels that define our different activities.

From a malevolent but somewhat harmless Zoom-bomb, where unwanted guests can disrupt a Zoom video-meeting if a certain set of configurations is not put in place (O'Flaherty, 2020), to a journalist taking part into a secret and very high level security meeting (Barigazzi, 2020), from high school pupils connecting to Google Meet and screaming during a lecture up to Microsoft Forms quiz users

substitutions, all these issues must be addressed by the software producers in order to bring higher and higher levels of security. Moreover, there is also another thing that must be taken into account by the software producers: making an application as best as possible from the security point of view could render it actually unusable for standard usage which probably do not require so many safety precautions. There is a fine balance that has to be kept in order to ensure the safety of the users, of their shared contend, while not degrading the user experience to a level that might provoke the user to abandon the respective software.

## References


[1] Barigazzi, J. (2020, 11 20). *Dutch reporter gatecrashes EU defense ministers' videoconference* . Retrieved from Politico.eu: https://www.politico.eu/article/dutch-reporter-gatecrashes-eu-defense-ministers-videoconference/

[2] Increased Emotet Malware Activity. (2020, 12 06). *Cybersecurity & Infrastucure Security Agency*. Retrieved from Cybersecurity & Infrastucure Security Agency: https://us-cert.cisa.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity

[3] O'Flaherty, K. (2020, 03 27). *Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat*. Retrieved from Forbes: https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/?sh=6f8a7893618e

[4] Securing Network Infrastructure Devices. (2020, 12 06). *Cyber Security & Infrastructure Agency*. Retrieved from Cyber Security & Infrastructure Agency: https://us-cert.cisa.gov/ncas/tips/ST18-001

[5] Tăbușcă, S. (2010). The Internet Access as a Fundamental Right. *Journal of Information Systems and Operations Management*, 206-212.

[6] The small business guide to secure email. (2019, 04 02). *Microsoft 365 Team*. Retrieved from Microsoft 365 Team: https://www.microsoft.com/ro-ro/microsoft-365/business-insights-ideas/resources/the-small-business-guide-to-secure-email

[7] Understanding Anti-Virus Software. (2020, 12 06). *Cybersecurity & Security Infrastructure Agency*. Retrieved from Cybersecurity & Security Infrastructure Agency: https://us-cert.cisa.gov/ncas/tips/ST04-005

[8] Understanding Patches and Software Updates. (2020, 12 06). *Cybersecurity & Security Infrastructure Agency*. Retrieved from Cybersecurity & Security Infrastructure Agency: https://www.us-cert.gov/ncas/tips/ST04-006