Guideline 5 – Recommendations for the protection of personal data and minimizing threats and risks during work with computers, in mobile communication, or on networks while working from home

Ref. no. UKRUK/128065/2020
17 April 2020

Recommendations for employees

Be careful of e-mail scams

We are currently witnessing the increased activity of hackers attempting to misuse the situation surrounding the ongoing pandemic and requests for information relating to the novel coronavirus. One of the most common means is sending fraudulent e-mails with attachments or links that seemingly contain important information on the coronavirus.

Fraudulent e-mails could appear to very trustworthy. The aim of these attacks is usually the unjust procurement of funds or access to the information system in order, for example, to employ ransomware. Ransom is then requested. However, the purpose of such an attack could also be to paralyze the entire university.

It is no longer true that you can recognize e-mail scams by the use of flawed Czech. In addition, do not be fooled by the notion that a person you know is sending the e-mail. If you think an attachment is untrustworthy in any way or you are not expecting an e-mail with such an attachment, do not open it. Moreover, malicious code may not be immediately apparent after running it. If in doubt, always contact your local IT support.

Do not open suspicious links in e-mails

Phishing emails usually hide where the links lead. The hidden path for the link is the first indication of a fraudulent email. How do I find out where a link from an email leads? Right-click (NOT LEFT) on the link and select “copy link address” from the menu. Then copy it into Notepad or a file and you will see where the link really leads. Also beware of shortcuts that mask the real link.

Do not confuse your work computer with a private one

Knowing that Internet access while working from home does not normally take place through a connection provided by your employer could lead to reduced caution when using the Internet on company equipment. Employees can also access sites that are typically characterized by the increased occurrence of various malicious programs and that they would never access on the employer’s network. This could introduce a malicious program to an otherwise “clean” device, which in turn could pose a serious threat to both the device itself and the information stored on it and to the organization’s information system after reconnecting such device. Similarly, increased caution is required when a private computer is used for remote access to the employer’s information system. Never install suspicious or unlicensed software when using a laptop or other devices of the employer.

Avoid using public Wi-Fi networks

Personal data and other sensitive information cannot be transmitted by a Wi-Fi network in public places without special precautions. It is safer to transmit via mobile data or the use of VPN when allowed by the settings at the specific CU unit. If you intend to use a third-party VPN service, check your provider’s reputation, the location, and the legal regulations applying to the service.

Be careful when selecting passwords

Do not use the same passwords at home and at work. This recommendation is especially valid for the data you use to log in to work remotely. In the event of a successful attack on your home computer, it is usually easy to acquire stored login information from browsers and email clients. An attacker should not be able to log on to the work e-mail using the password for a private e-mail account or access anything else.

Do not enable macros in ordinary documents

For transmission, most crypto-viruses use fraudulent e-mails with an attached document. This includes a prompt to enable active content and macros. The attachment itself might look like a message that the document is written in an older version of a text editor and the actual content of the file cannot be displayed without the macros enabled. Never comply with such a request, as this would result in malicious code being downloaded and installed. New versions of office programs are able to work with older versions of documents, and there is no need to install or enable anything.

Do not underestimate the physical security of computers

A computer should require verification, e.g. by entering a password or biometric authentication. You can greatly mitigate the effects of theft by turning on hard disk encryption. For most computers, this feature can be turned on or installed for free, and the impact on performance is negligible. Encryption greatly reduces the risk when a device is lost.

Follow other practical security measures

Measures should be proportional to the level of risk. Adequate security relating to access of other family members to a device (its contents) is also important. This is especially true for children who could unknowingly also be the cause of some of the risks in this document.

When should you contact your local IT support?

- Files with unknown extensions are on the disk instead of your regular documents.
- There are new files on the disk containing information on accessing files after paying a ransom. They usually contain words like decrypt, recover, ransom, etc. in the file name and content.
- The desktop wallpaper has changed or a notification is displayed directly on the screen.
- In other cases, if you suspect your device is behaving abnormally.

When should you report a security incident?

Please be aware that there is an obligation to report any security incident to the Data Protection Officer. Reporting is the responsibility of any employee or their supervisor who discovers any of the following:

- a device or document containing a personal data file was lost or stolen;
- an unauthorized person has been given access to personal data in the device or document;
- personal data, in whatever form, were placed without adequate access protection in a location where unauthorized access could be made;
- personal data has been corrupted or lost;
- personal data may have been changed or modified, but it is not possible to verify that this has occurred.

Any loss must be reported to the e-mail address gdpr@cuni.cz. See also https://cuni.cz/UKEN-905.html

Recommendations for employers

- Do not underestimate backups and their protection
- Prepare specific procedures for a quick response
- Assess and report security breaches

Do not underestimate backups and their protection

If you encrypt a significant amount of data on the network, you must first and foremost protect the backups. If backup is performed by copying the files to another location at regular intervals, it should be possible to turn off automatic backups without the intervention of an administrator. This may not always be available, and any “saving” of a virus to backups could have a major impact. It is, therefore, highly recommended to implement the backup in a way that allows you to return to previous versions of files (e.g. using incremental backups). This should be taken into account when designing or updating the parameters for the unit’s information network, since advanced ransomware will already attack backups.

Prepare specific procedures for a quick response

If a crypto-virus begins to encrypt data, the affected computer must be shut down as soon as possible and the network administrator informed of the ongoing attack. In these cases, every minute is important and the least damage the virus can do, the better. Together with the controller, the Data Protection Officer or other persons responsible for compliance (e.g. communication with state authorities) should ideally be informed. Specific procedures should be part of the internal documentation for dealing with security incidents.

Assess and report security breaches

If there is a breach in the security of personal data, whether at work or as a part of work from home, that is assessed as a risk to the rights and freedoms of data subjects, Charles University is obliged to report this breach to the Office for the Protection of Personal Data. However, if a possible attack is stopped in a timely manner (personal data has not been compromised by the attacker and the data has been restored from backup), it is not usually necessary to report such an attack since it is not a risk to the rights and freedoms of the data subjects. However, even in such a case, the incident should be recorded, within the meaning of Article 33(5) of the GDPR.