Grupa GPEC

# SECURITY GUIDE

CYBERSPACE THREATS AND HOW TO TAKE CARE OF SECURITY

# CYBERSPACE THREATS

## I. Phishing

Spam can be dangerous: it may contain messages from criminals who are trying to get confidential information. They present themselves, for instance, as a service provider and try to convince you to install a program containing a virus or spyware.
Thanks to phishing, criminals can extort confidential data or infect your device.
Criminals develop fraudulent websites. They pass themselves off as public trust institutions and encourage you to enter their website. Criminals send e-mails the title or content of which is to convince you to open the link or attachment. Many times such messages contain information about a blocked account, need for additional data verification or unpaid invoice.

**Phishing on social media and messengers is popular.**

Fraudsters can write a message to you from your friend's account after they take control over it. In the conversation, they will ask for your help and money transfer. If you click the link they sent and enter your data, you are exposed to data theft. Another way is promotion of the fraudulent website in the browser. A fraudulent website is usually strikingly similar to the true website. To mislead you, the address of such a website often contain a name of a real institution they are pretending to be.

## II. Malware

Malware (e.g. a computer virus) is a code that cannot function on its own. It needs a computer software. If you download such a program and run it, you will also start the virus.

A virus can work in several ways:

- **phishing data**
- **stealing identity**
- **infecting files when created or run**
- **deleting or corrupting data**
- **stealing data you use to log in the social media and electronic mail accounts.**

## III. Exploiting software holes

Criminals look for holes in the program codes and use them ruthlessly. When they gain access to a computer, they can install malicious software that changes the functioning of a computer or mobile device. Malicious software is developed to be then sent by e-mails that attract your attention and convince you to open the link or attachment. Very frequently such messages regard a blocked account, additional device verification or unpaid invoice.
Criminals can also infect your phone. In particular, when downloading software via a link from a text message received from an unknown sender. Criminals also upload malicious applications in the online stores. They often pass themselves off as other applications. Such applications will often require access to your text messages.

## IV. Fraudulent invoices

Criminals send a fraudulent invoice with a changed account number. The invoice can be received from your contractor's e-mail account if the criminals penetrate through the security measures on its computer. Malicious software can send messages without the mailbox owner's knowledge.

**If you have any doubts, call your contractor to ask if it sent you the suspicious invoice.**

## V. False messages on a website or web portal

Criminals can display false content even during connection via a website of your contractor or an institution. They can do it if your computer is infected. They can extort confidential text message data.

If your phone is infected, criminals can also display false content when you're starting an application. They will try to extort your data as well as receive and send text messages.

# VI. Fraudulent stores and offers

Criminals develop fraudulent Internet stores, offering goods at attractive prices. Even though you pay for your purchases in such a store, the package may never arrive.

Before you buy, please verify who you are buying the goods from:

**how long the given company has existed**

**whether it is possible to call it**

**whether you can receive a reply to your e-mail**

Criminals can also offer goods on a website "for free" - in exchange for paying the shipment costs. Sellers send a link to quick transfers, i.e. to a fraudulent website. They capture your logging data, define a new user or change the transfer value.

# HOW TO TAKE CARE OF SECURITY?

## I. Secure devices

Use transaction websites only on verified devices.
Avoid logging in to applications or websites from computers and mobile devices of other persons.

Update the computer operating system regularly.

Applications and programs must be downloaded only from official sources.

Use additional software (e.g. antivirus, firewall) that protects your computers and mobile devices.

Do not change the security settings of the device and, in particular, do not remove restrictions set by the producer.

Block the device screen by means of additional security measures (e.g. password, PIN).

## 1. Mobile devices

Smartphones and tablets are more and more frequently replacing other personal devices. Similarly to computers, mobile devices require protection against viruses.
When thinking about safety of their phone or tablet, many users are afraid of losing them or that somebody could steal them.
Meanwhile, what we should be afraid the most is that somebody could take control over them.

**When using mobile applications, remember:**

- Use of antivirus software is obligatory
- The screen must be blocked with a password and PIN
- Install updates of applications and the operating system
- Download and install applications only from official app stores
- Do not use links from text messages or e-mails if you have any doubts that they could originate from an unsecure and untrusted source
- Do not connect mobile applications with your accounts on other devices
- Do not read QR codes of unknown origin
- Be cautious when installing applications requiring authorisation to read and send text messages
- Switch off Wi-Fi and Bluetooth when not used

**Note!**

**No instructions ever ask you to install additional applications or certificates.**

## 2. Computer

**A secure computer must have:**

- Updated and legal operating system
- Firewall type software

  Firewall is one of the methods to secure computers, networks and servers against intruders. It has become an indispensable software for all computers connected to the web.

  A firewall on your home computers checks the entire web traffic and restricts access of unknown software or users.

- Antivirus software as well as anti-spyware and anti-adware software

  This software detects, secures, eliminates, removes and repairs damage caused by viruses. If an application contains malicious software, the antivirus will take proper measures to exclude the virus and ensure secure access to the started software. It is important that the antivirus software is frequently updated. This allows it to be "up-to-date" with the world of viruses.

  Updates allow the software to collect information about the latest viruses and add instructions helping to eliminate viruses and repair the damage they cause. Antivirus developers that are well recognised on the market update their virus definitions daily.

- Anti-spam software

  This is a type of software that blocks unsolicited e-mail correspondence. The software filters messages and uses the so-called "black lists" of addresses and domains used by spammers. In most cases, such a software allows to change the settings of rules (e.g. determine the keywords found in advertising materials). This allows to block messages containing such words in the message title from entering our inbox.

  However, this software is not perfect and may sometimes block correspondence we want to be delivered, therefore checking the spam folder and verifying if all messages stored there should have actually been transferred there is important.

## II. Secure passwords

**Use complex passwords and make sure it is difficult to guess them.**

**At least eight characters, including special characters, numbers, capital and lowercase letters.**

**In your passwords, do not use typical expressions and information that can be easily linked to you (e.g. name or surname) or that are easy to guess (e.g. current month, year).**

**Change your passwords regularly and do not share them with anybody.**

**Use unique passwords for websites. Do not use the same passwords you use in other systems, on Internet forums or websites.**

## III. Secure e-BOK logging

- Never share your identifier (login) or access password with other persons. The logging password for the website is set separately.
- When entering the identifier (login) and password, make sure nobody is watching.
- Do not log in applications on computers available in public areas.
- Use safe passwords and try to avoid passwords that are easy to guess.
- Do not write your passwords down and remember to change them regularly.
- Before leaving your computer, log out and close the browser.
- Check the date of last successful and unsuccessful logging.
- If additional fields to be completed, e.g. personal data or one-off password, appear on the logging page or if you notice any irregularities, do not provide your data and report the issue to the Customer Service Office.

# IV. Secure application installation

**If you decide to download any software to your device, remember:**

**Applications should be downloaded from authorised stores.**

**App Store**
(iOS - Apple)

**Google Play**
(Android)

**Windows Phone Store**
(Windows Phone)

**Windows Store**
(Windows 8.1)

**Use only these stores as the software offered there is digitally signed and verified in terms of security.**

**Never download applications from untrusted sources and avoid downloading applications from third parties (e.g. sent via Bluetooth or in a text message).**

**Be cautious when installing applications requiring authorisation to read and send text messages.**

# V. Secure e-mails

- Do not open suspicious e-mails and attachments.
- Be extra cautious about attachments having several file extensions at the same time, e.g. przelew.pdf.zip, wyplata.jar.doc.
- Check if the actual link address is compliant with what you see in the e-mail content.
- Be cautious about the sender's reliability and the way he/she is titling you.
- Never log in a transaction website from a link you received by e-mail.
- Do not realize transactions based on an e-mail. Check such payment orders carefully.

## VI. Secure websites

- Check correctness of the website you are connecting to (certificate and HTTPS connection).
- Do not enter suspicious and unknown websites.

  Pay attention to the URL addresses of the websites you visit, especially in case of the so-called shortened URLs. Such websites can infect your device with malicious software.
- Do not provide your personal data on untrusted websites, especially your login and password you are asked for on unknown websites.
- When logging in on websites, type the address of the logging page yourself or use the "Log in" button after you type the website address.

  Never use logging links you receive by e-mail or on social media.

  Do not search for the logging website in the Internet browser - this could lead you to fraudulent websites that pretend to the website you want to log in.

## VII. Secure profiles and offers

If you received a request from your friend to make a transfer for him/her, be careful - it is possible you are messaging with a fraudster. Contact your friend using a different method to confirm that it is actually him/her who is requesting the given transfer.

Before you buy anything, check who you are buying the goods from: how long the given company has existed, whether it is possible to call it or what opinions other buyers published about it.

Do not trust job offers sent directly to your mail box, especially those particularly attractive. When you are looking for work, use only websites you know.

## VIII. Secure telephone conversations

- Do not share your private data until you are sure who you are talking to. Employees of all institutions can be verified - call the Customer Service Centre and ask for confirmation of their identity.
- Do not trust unknown persons contacting you who want you to provide your data (passwords, PINs).