SECURITY GUIDE

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 no 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 or 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.