BEST PRACTICES

FOR EMPLOYEES

THE BEST PRACTICES FOR EMPLOYEES ARE A PART OF THE PPHS CYBERSECURITY STANDARD FOR SMALL AND MEDIUM-SIZED ENTERPRISES AND PUBLIC INSTITUTION DEVELOPED BY THE POLISH PLATFORM FOR HOMELAND SECURITY.

TABLE OF CONTENTS

SPIS TREŚCI

03

PASSWORD AND AUTHENTICATION SECURITY

Use multi-factor authentication (MFA)

If you have this possibility, use multi-factor authentication (MFA). Often, multi-factor authentication with two factors is available for services with sensitive data - usually called 2FA authentication.

EXPLANATION

There are usually three types of authentication defined:

- Something the user knows (e.g. a password).
- Something the user has (e.g. mobile device, email account, hardware security key).
- Something that the user is (e.g. fingerprints).

Multi-factor authentication requires at least two types of authentication. For example, this could be:

- Password and code sent by email or SMS.
- Password and code generated by the application installed on your phone.
- Password and hardware security key (e.g. connected to USB).
- Multi-factor authentication is an additional security measure to protect the account when login data is stolen or made public - an attacker, even if he or she knows the login and password, will not be able to log in without a second type of authentication.

LINKS (EXAMPLES OF APPLICATIONS AND DEVICES USED FOR MFA):

2FA configuration for Google account

2FA configuration for Microsoft account

FreeOTP – application which generates one-time codes, can work with many applications and services

Google Authenticator – application which generates one-time codes, it can work with many applications and services

Authy – an application which generates one-time codes, just like Google Authenticator

YubiKey – the hardware security key, used as a second component of authentication, can work with many applications and services

Thetis Fido – a hardware security key, used as a second component of authentication, similarly to YubiKey

04

PASSWORD AND AUTHENTICATION SECURITY

Create your passwords according to good practice

Good password should:

- Be long (preferably over 12 characters) - long passwords are much harder to crack.
- Not contain information related to your or your relatives' data (e.g. name, surname, date of birth, etc.) - an attacker may use the knowledge of your data to crack the password more quickly.
- Do not use well-known sayings (e.g. "TwinkleTwinkleLittleStar") - such passwords are easier to crack with use of a dictionary attack.
- Be easy to remember and at the same time difficult to guess - in this case a combination of words works best, e.g. "there is a white cow sitting in a red tree". Such passwords are difficult to crack and at the same time much easier to remember than a random sequence of letters and numbers. If you use the password manager you can use the passwords generated by this software - because the passwords are stored in the manager there is no need to remember them.

EXPLANATION

Very often, rules for passwords are imposed on the user and require characters of different sizes, numbers and special characters. However, NIST in "SP 800-63B Digital Identity Guidelines; Appendix A" indicates that in such situations users tend to create predictable passwords (e.g. password -> Password1!). This means that such requirements are not really profitable. At the same time, the harder it is to remember a password, the more likely it is to be written down or saved in digital form, which poses another threat. NIST recommends paying attention, first of all, to the length of the password and to check if the password is not too vulnerable to dictionary attacks, does not contain specific words (such as the name of the service) and is not one of the commonly used passwords.

LINKS:

SP 800-63 Digital Identity Guidelines

05

PASSWORD AND AUTHENTICATION SECURITY

Do not use the same password in more than one service

The password should be unique for each service.

EXPLANATION

This is a principle of risk mitigation - even if your password for a service has been made public, it cannot be used to log in to another service. Publication of the password may occur as a result of many events, e.g. data leakage, social engineering attack, etc. If you use the same password in all places, data leakage, e.g. from an insignificant forum or portal, may result in the leakage of a password to your bank account or email.

Never give your password to anyone

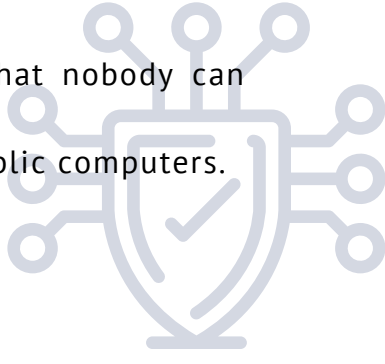
EXPLANATION

No one should ever ask you for your password. If someone does and presents themselves as your company's technical support, you are most likely a target of a phishing attack.

Keep your password secure

Make sure no one gets to know your password. This includes, among others:

- Not writing your password down in places to which someone else has access.
- When entering your password, making sure that nobody can see what you are typing.
- Not logging in to any important services on public computers.



06

PASSWORD AND AUTHENTICATION SECURITY

Use password manager

Use a password manager to manage your login data.

EXPLANATION

Maintaining good practices regarding password creation and the principle of not using the same password in more than one service at the same time is difficult due to the number of different services requiring login. It is much easier to use a password manager - a program that allows you to manage your authentication data. Password manager usually works according to the following scheme:

- At the beginning of its operation it creates an encrypted database file, usually protected by the so-called main password.
- When logging into a service or setting up an account, the password manager allows you to save your login data.
- After saving the login data to a particular service, you can log in using the password manager. In order to use the data saved in the password manager you need to enter your main password.

Password manager allows you to have a different password for each service without having to remember it - just remember your main password.

LINKS (EXAMPLES OF OPEN SOURCE PASSWORD MANAGERS):

KeePass
KeePassXC
pass

07

SECURITY OF REMOTE WORKING

When connecting remotely, use the VPN

If your company has a VPN, every time you work remotely, start by connecting to it.

EXPLANATION

The VPN significantly increases the security of remote working (see Technical Guide: VPN).

Do not leave your device unattended in public places

Never leave your device in public without supervision of a trusted person. Remember that your device is not only equipment, but also data that is often worth much more, and its loss can cause great losses for you and your company.

EXPLANATION

Leaving your device unattended in a public place poses many threats such as:

- Theft of your device,
- Theft of data from the device,
- Installation of malware.

08

SECURITY OF REMOTE WORKING

When working in a public place, pay attention to your surroundings

If you work in a public place, pay attention to what and who is next to you. Make sure no one can see or record the passwords or other sensitive data you enter. Preferably, avoid working on sensitive data in places where it is easy to see the contents of the screen (e.g. train, coffee shop).

EXPLANATION

"Peeping" is a very simple yet difficult to detect method of data leakage. Even if the data displayed on the screen does not seem to be particularly important, it can afterwards be used for social engineering attacks.

Create a separate account on your device

If you work with use of a device shared with other people (e.g. your private computer at home), create a separate account to which no one else has access.

EXPLANATION

Even if you trust your family, there is still the possibility that someone will be able to get to know the password of your family member's account. Having a separate account will minimize possible threats and suspicions in case of an incident.

09

SECURITY OF REMOTE WORKING

Use only equipment approved by company's policy for remote working

Follow the company's policy for devices which can be used for remote working.

EXPLANATION

Some companies may provide company equipment and require to work only with use of it, others may allow work with use of employees' equipment. These policies are designed to protect company data and services from hacking.

Avoid using unknown devices for any activities concerning company data

Use only known and trusted devices - your own, your company's or affiliated organization's (e.g. business partner's) device to perform any operations concerning company data (such as checking your email).

EXPLANATION

One never knows if the unknown device is properly protected and if it has not been infected with malware. Using such a device may cause data theft.

10

SECURITY OF REMOTE WORKING

Secure your home network

While using your home network for remote working, remember to:

- Change the default password on the devices in the network.
- Disable the ability to configure devices outside the network.
- If you are not using a Wi-Fi network, make sure that your devices do not provide it. If you are using a Wi-Fi network, make sure you have adequate protection (see: Make sure your home Wi-Fi is secure).
- Keep the software on your network devices updated.
- Don't connect your computer or laptop directly to the network provided by your provider, use some kind of intermediary device (router). This allows you to protect your computer from an unexpected connection from outside the network.

EXPLANATION

If your home network used for work is not properly secured, it may be a vulnerability of the whole system and allow interception of transmitted data or Man-in-the-middle attacks (see Technical Guide: Man-in-the-middle).

11

SECURITY OF USING WI-FI NETWORKS

Avoid using public Wi-Fi networks on the device on which you store your company data

If your device stores company data, avoid connecting to public Wi-Fi networks.

EXPLANATION

If the network is falsified or intercepted by an attacker, your device may be infected with malware and the transmitted data may be intercepted.

Disable automatic connection to public Wi-Fi networks

EXPLANATION

Automatic connection to public Wi-Fi networks can result in a connection to a specially prepared network, which can infect the device with malware or cause data leakage (see: Technical guide: Fake Wi-Fi network).

LINKS:

Instructions for changing settings of connection to open networks for Windows, Android and IOS

12

SECURITY OF USING WI-FI NETWORKS

Do not connect to unknown and untrusted Wi-Fi networks

Never connect to a Wi-Fi if you are not sure of its authenticity. In hotels, trains, etc., make sure that the network is provided by a service provider.

EXPLANATION

The Wi-Fi network can be specially created to intercept data or to infect devices with malware (see Technical Guide: Fake Wi-Fi network).

Turn off Wi-Fi if you are going out of an area with a known Wi-Fi network

If you are leaving an area where you are connected to a Wi-Fi network which you know (e.g. office), turn off the Wi-Fi on your device.

EXPLANATION

The aim is to prevent the device from automatically connecting to a fake Wi-Fi network (see Technical Guide: Falsified Wi-Fi network).

Pay attention to which Wi-Fi network you are connected to

If your device automatically connects to known Wi-Fi networks, you should pay attention to which Wi-Fi network you are connected. If your device is using a Wi-Fi network which should not be available in a particular location, it means that you are connected to a fake network (see: Technical guide: Falsified Wi-Fi network).

13

SECURITY OF USING WI-FI NETWORKS

Ensure the security of your private Wi-Fi network at home

If you are using your home Wi-Fi network for work, you should implement basic security measures such as:

- Rename your network (SSID).
- Disable the broadcast of the network name. This action will make it harder for unauthorized people to connect to the network.
- Use strong encryption of the transmitted data. NIST recommends WPA2 with AES as the preferred encryption method.
- Use a password, which follows the good practices indicated in this document, to connect to the Wi-Fi network.
- Disable wireless configuration of Access Point.

EXPLANATION

If the Wi-Fi network used for working is not properly secured, it may be a weakness of the whole system and allow interception of transmitted data or Man-in-the-middle attacks (see Technical Guide: Man-in-the-middle).

14

WORKSTATION SECURITY

Never connect unknown and untrusted data carriers/devices

If you are not completely sure about the contents of a data carrier or device, never connect it to your computer. Follow the company's procedures for responding to such situations.

EXPLANATION

An unknown device may contain malware. One of the methods used by attackers is leaving marked data carriers , e.g. "Earnings in the company", with the hope that one of the employees, who is curious, will plug it into their computer.

Do not run or install unknown or untrusted programs

EXPLANATION

Running an untrusted program can lead to infecting the device with malicious software, and consequently, even to infecting the entire company.

15

WORKSTATION SECURITY

Always lock your device when you are not using it

Lock your device when you are not using it. Use strong safeguard (good password, complex pattern, etc.).
Additionally, turn on the automatic lock of the device after a certain period of inactivity.

EXPLANATION

It is much easier to acquire data from an unlocked device, e.g. in case of theft or temporary "borrowing". For this reason, you should block the device even if you go out "only for a while". Since everyone makes mistakes and sometimes forgets to turn the lock on, it is worth setting the automatic lock of device after a certain time (e.g. 1 minute).

16

BROWSING SECURITY

Verify if the websites you visit, use a secure connection

Check whether the sites you visit transfer data using HTTPS, i.e. if the data is transferred in encrypted form. This applies in particular to pages with forms with use of which data is sent.

EXPLANATION

The transmission of data in encrypted form protects against data modification and reading during the transmission. It also reduces the probability of being a victim of Man-in-the-middle attack (see Technical Guide: Man-in-the-middle).

Verify details of website certificates

Apart from checking whether the data is transmitted via HTTPS, verify the details of the website certificate. An OV SSL or EV SSL certificate (see Technical Guide: SSL Certificate Types) should be used for institutions that use sensitive data. Certificate details are usually available by clicking on the "padlock" next to the address bar.

EXPLANATION

OV and EV SSL certificates provide information about the authenticity of the organization which manages the domain, so you can be sure who you are communicating with.

LINKS:

Mozilla Firefox Security Certificate
Check if a site's connection is secure for Google Chrome
Safari Security certificate
Microsoft Edge Security Certificate

17

BROWSING SECURITY

Verify the correctness of website addresses

Before you provide your login or transfer any data, verify whether the website address is correct. For frequently used websites (e.g. bank or mail provider's website) use bookmarks in your browser or enter addresses manually - avoid clicking on links sent by email (there is a possibility that the message was forged and contains an incorrect link).

EXPLANATION

Some attacks are based on creating fake websites similar to the original ones and at the same time they have a very similar address to the original one. An attacker collects data entered on such a site (e.g. login data) and uses it in further attacks. Examples of incorrect, and at the same time difficult to distinguish, addresses are: gogle.pl, rnbank.pl.

Enable pop-up windows blocking

Make sure that you pop-up window blocking is enabled in your browser.

EXPLANATION

Pop-up windows are often used for phishing attacks, e.g. showing the user that a virus has been found on his computer and asking the user if he can remove the virus. By clicking the confirmation button, the user unknowingly allows the computer to be infected.

LINKS:

Configure pop-up blocking in Mozilla Firefox
Configure pop-up blocking in Google Chrome
Configure pop-up blocking in Microsoft Edge
Configure pop-up blocking in Safari

18

BROWSING SECURITY

If your browser remembers your login data, activate additional main password protection

EXPLANATION

If the browser stores authentication data without a set main password, the stored passwords can be read by anyone who accesses the browser on a particular computer. The master password is an additional security feature that prevents passwords from being read even if someone accesses a user account on a computer.

LINKS:

Configuration of the main password in Mozilla Firefox

Google Chrome, Microsoft Edge and Safari automatically use the password to the user account as the main password

Delete unused browser add-ons

Verify all add-ons installed in your browser and remove any unnecessary ones.

EXPLANATION

Browser add-ons may have vulnerabilities or be malicious softwares themselves. Therefore, there is a need to regularly check which add-ons are needed and remove all unnecessary or unknown ones

LINKS:

Removing add-ons in Mozilla Firefox
Add-ons manager in Google Chrome
Extensions in Microsoft Edge
Add-ons manager in Safari

DATA PROTECTION

Do not copy data onto unprotected data carriers, do not send it to your private accounts

If it is prohibited by company policy, never copy company data onto data carriers that are not intended for this purpose (such as a private flash drive) or send it to your private accounts (such as email or Google drive).

EXPLANATION

Such data carriers may be connected to an infected computer, lost or stolen which can result in data leakage. Sending company data to your private accounts is a similar case.

Do not connect data carriers to untrusted devices

Do not connect data carriers to devices if you are not sure of their security.

EXPLANATION

If a storage medium is connected to an infected device, data stored on that medium may be stolen, and the medium itself may be infected, resulting in compromising company systems.

EMAIL PROTECTION

Do not open attachments from uncertain sources

If you are unsure about the authenticity of a message, do not open the attached files and follow the company's policy for responding to such situations. Never open the .exe files if you have any doubts. Before using the uploaded files, check them with an antivirus.

Do not click on the links in the message

If you are not sure about the authenticity of the message you received, do not click on the links in it, especially beware of short links (e.g. tinyurl.com). If you receive a message from a bank or any other service, enter the site manually via your browser, do not click on or copy the sent link. If a file starts downloading after opening the link, be careful: before opening the file, make sure it comes from a trusted recipient, scan the file with an antivirus.

EXPLANATION

The message may be forged and the link may lead to a specially prepared page which is aimed at stealing your data or money. The fabricated site may accurately forge the appearance of the bank's website in order to induce you to provide your login details.

21

EMAIL PROTECTION

Ensure that messages and attachments are encrypted

When transferring sensitive data, use end-to-end encryption of messages and attachments or encryption of attachments.

You can use PGP or S/MIME technology (described in the PGP and S/MIME section of the Technical Guide) to encrypt messages. The public key is used to encrypt the transmitted information. The private key allows you to read it. Due to the fact that the private key is available to only one person (the recipient), no one else can decrypt the message. An encrypted message can be sent by anyone with recipient's public key. Most modern email clients provide the option of message encryption, generated keys are needed and the appropriate configuration (depending on the email client).

You can also encrypt the transferred files manually (e.g. with the free 7zip program or with the mechanisms built into your office packages). The recipient will be able to decrypt the file with use of a password which you should provide to him/her through a different communication channel than email.

EXPLANATION

Encrypting messages and attachments will protect against potential data theft or leakage. Even if a message is intercepted, it cannot be read by anyone but the recipient. End-to-end encryption also protects against reading data in case of hacking into the email server.

LINKS:

Configuring message encryption in Mozilla Thunderbird
Configuring message encryption in Microsoft Outlook
Configuring message encryption in Outlook Web App
Encrypting files in MsOffice package
Encrypting files in LibreOffice package

22

EMAIL PROTECTION

Verify the sender of the message and digitally sign your emails

Check whether the messages received are signed digitally. Use the digital signature to sign your emails. You can use PGP or S/MIME technology (described in the PGP and S/MIME section of the Technical Guide). To sign the message, the sender calculates its hash, which he then encrypts with use of his private key. The recipient of the message can verify that the message has not been changed during transmission by decrypting the hash with use of the sender's public key and a hash, which he or she calculates himself or herself from the received message.

A set of private and public keys is needed to add and verify signatures. Most modern email clients provide the option of signing messages, generated keys and appropriate configuration (depending on the mail client) are needed.

EXPLANATION

A digital signature with use of a trusted certificate provides:

- Authenticity - certainty about the sender of the message.
- Integrity - certainty that the content of the message has not been changed during transmission.
- Non-deniability- makes it difficult for the sender to deny authorship of the message.

LINKS:

Configuring signing of the messages in Mozilla Thunderbird
Configuring signing of the messages in Microsoft Outlook
Configuring signing of the messages in Outlook Web App

23

EMAIL PROTECTION

Verify that you do not share recipients' email addresses when sending a message to multiple persons

Each time you send a message to multiple recipients, verify if you address the message correctly and whether you do not share the recipients' email addresses with others.

EXPLANATION

Errors in addressing can lead to your entire list of addresses being made available to each recipient of the message. The result can have serious consequences, both legal and related to the potential loss of customers and their trust.

In order to avoid data leakage, you need to understand the three address fields used in emails:

- TO - addresses placed in this field will be visible to all recipients of the message.
- CC (Carbon Copy) – addresses placed in this field will be visible to all recipients of the message. Usually this field is used if someone is not the direct addressee of our message, but we want them to be informed about it.
- BCC (Blind Carbon Copy) – the addresses placed in this field will also receive a message, but will not be visible to anyone.

When sending messages to many people you need to consider whether all the recipients of your message should know about each other. If not, instead of putting your email addresses in the TO field, enter them into BCC. In this way, each of the recipients will get a message addressed only to him and will not see other recipients.

An example of harmful effects associated with incorrect addressing of messages can be sharing your entire customer list, which can be used by competitors.

24

EMAIL PROTECTION

Verify that your server is not an open relay

Make sure that your mail server allows to send messages only to your users. Require user authentication before send messages and limit the address range that can be used to send messages only to the internal addresses.

EXPLANATION

An open-relay is a term for a mail sever allowing to send messages that are not sent by its users. In other words, everyone may send a message from that kind of server providing name of the other individual (especially name of the real user which is owner of this email account).

This kind of servers are the main source of SPAM and fake messages. Adding the blacklists to the server will be one of the many effects of such a configuration. And as a result, messages from the open-relays severs will be ignored.

The basic way to protect is enabling the required authorization for messages sending. Also, numbers of addresses that have a permission to send messages to the internal email accounts may be limited.

Verify suspicious messages even if they come from known addresses

When you receive an unexpected message asking you to take some unexpected action, first, verify the authenticity of the request with the sender.

EXPLANATION

The message may be falsified by someone who hacked into the recipient's account or lost the device. An example of an unexpected message can be a request by a supervisor to suddenly transfer company funds to another account.

POLISH PLATFORM
FOR HOMELAND SECURITY

Polish Platform for Homeland Security

ul. Slowackiego 17/11
60-822 Poznań
www.ppbw.pl/en
tel.: +48 (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

European Funds Smart Growth

Republic of Poland

European Union
European Regional Development Fund

The project "Cybersecurity – PPHS Standard for SME and public institutions" was financed by the European Regional Development Fund.