CYBERSHIELD-
WZMOCNIENIE KOMPETENCJI POLICJI
W ZAKRESIE ZWALCZANIA
CYBERPRZESTĘPCZOŚCI

POLICJA
MAZOWSZE

CYBERSHIELD:

YOUR SHIELD'S ONLINE

A practical set of rules for a safe internet, cyber hygiene and identity protection.

‘CyberShield – Strengthening the Police’s Competence in Combating Cybercrime’. The project is co-financed by the European Union from the Polish Internal Security Fund Programme for 2021-2027.

Material developed in accordance with the guidelines of the Act on the National Cybersecurity System and the recommendations of NASK and CERT Polska.

European Funds for Migration, Borders and Security

Republic of Poland

Co-funded by the European Union

INTRODUCTION
AND CONTENT MAP

The Internet is a space of unlimited possibilities, but also real threats. The Cybershield project was created to provide specific tools and habits that will turn your devices into a fortress.

The content of the e-book is based on official standards of state and international security, translating complex regulations into the language of practical actions.

TABLE OF CONTENTS (YOUR PROTECTION PLAN):

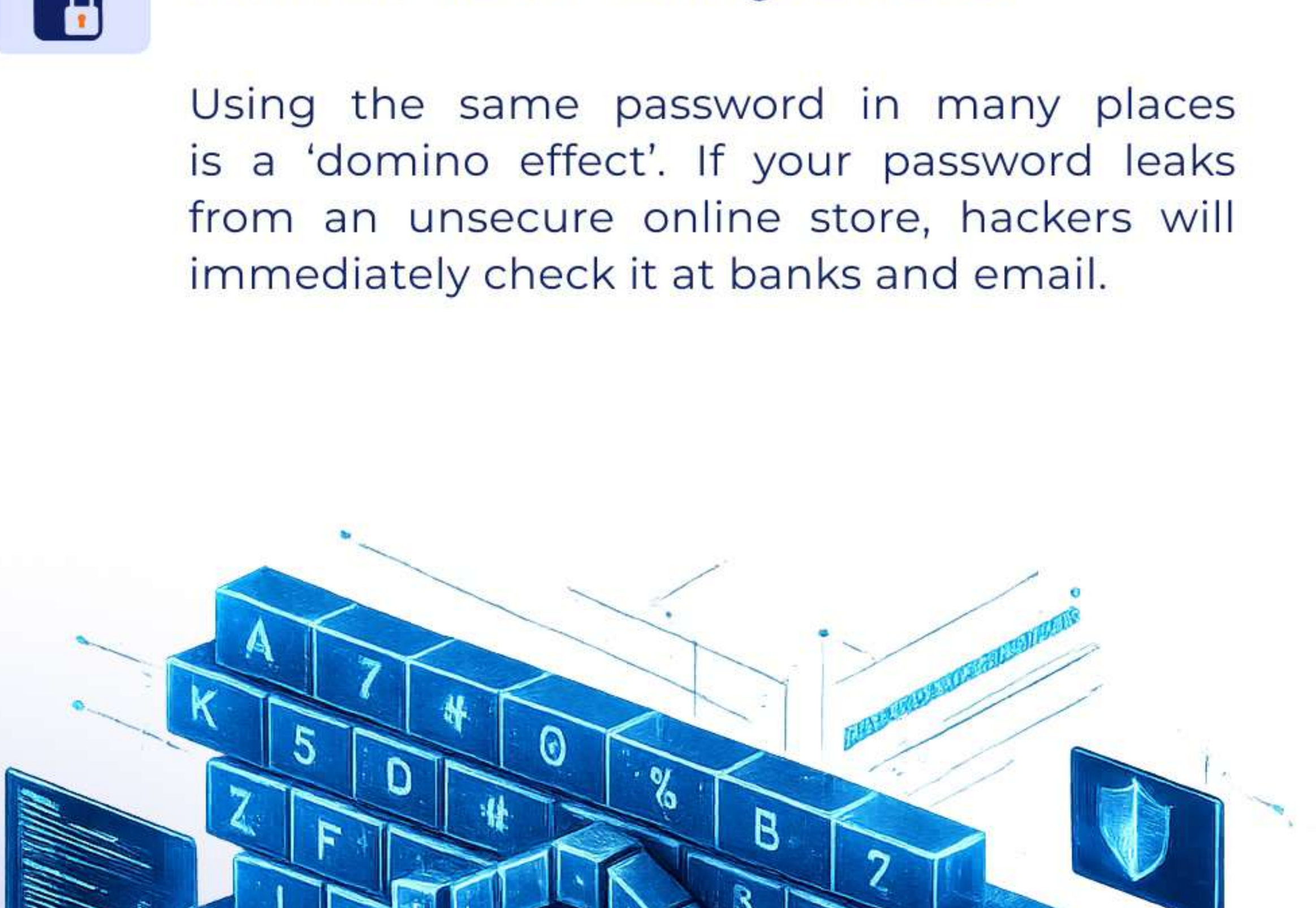
PASSWORD FORTRESS
– YOUR FIRST LINE OF DEFENCE

LENGTH INSTEAD OF COMPLEXITY:

Modern standards (NIST) move away from forcing special characters to length. Password consisting of 15-20 characters creating an easy - to - remember sentence (e.g. MyCoffeeSmellsAt7AM!) is almost impossible to break by brute-force, and at the same time easier to type than random X$z7!q.

PRINCIPLE OF UNIQUENESS:

Using the same password in many places is a ‘domino effect’. If your password leaks from an unsecure online store, hackers will immediately check it at banks and email.



PASSWORD FORTRESS
– YOUR FIRST LINE OF DEFENCE

PASSWORD MANAGER AS STANDARD:

Human memory is unreliable. Using applications - managers allows you to have hundreds of unique passwords, of which you need to remember only one - the main one.

WHEN DO I CHANGE MY PASSWORD?:

Forget about changing passwords every 30 days – this is a myth that leads to weak passwords. In accordance with NASK's recommendations, we change the password only in three cases: when you suspect a data leak, when the service has been hacked or when you accidentally entered a password on a suspicious site.

YOUR PASSWORD AUDIT
(Do It Today):

- [ ] Is your password for the main e-mail different than for other services?
- [ ] Do your passwords have at least 12 characters?
- [ ] Do you use a password manager instead of saving it in your browser?

PASSWORD FORTRESS
– YOUR FIRST LINE OF DEFENCE

CURIOSITY:

Hackers use the so-called ‘rainbow arrays’ – gigantic databases containing billions of already calculated hashes of popular passwords. Passwords such as ‘123456’ or ‘polska1’ are broken in a fraction of a second because they are at the very beginning of each such list.

DID YOU KNOW, THAT...

GOLDEN RULE:

One universal key opens all doors – and so does the hacker. Take care of the uniqueness: One account, one unique key.

DOUBLE RIG
– TWO-STEP VERIFICATION (MFA)

MULTI-FACTOR AUTHENTICATION (MFA):

This is a login process that requires two of the three components: what you know (password), what you have (phone, USB key) and who you are (biometrics – fingerprint, facial scan).

WHY IS THE PASSWORD NOT ENOUGH?:

In the era of data leaks, password alone is only half the battle. MFA means that even if a hacker takes over your password, they won't enter your account without physical access to your other component.

METHODS FROM THE WEAKEST TO THE STRONGEST:

- SMS (possible to be taken over by the so-called SIM-swap).
- Authorisation applications – generate codes valid for only 30 seconds.
- U2F hardware keys - physical devices that are completely phishing resistant.

DOUBLE RIG
– TWO-STEP VERIFICATION (MFA)

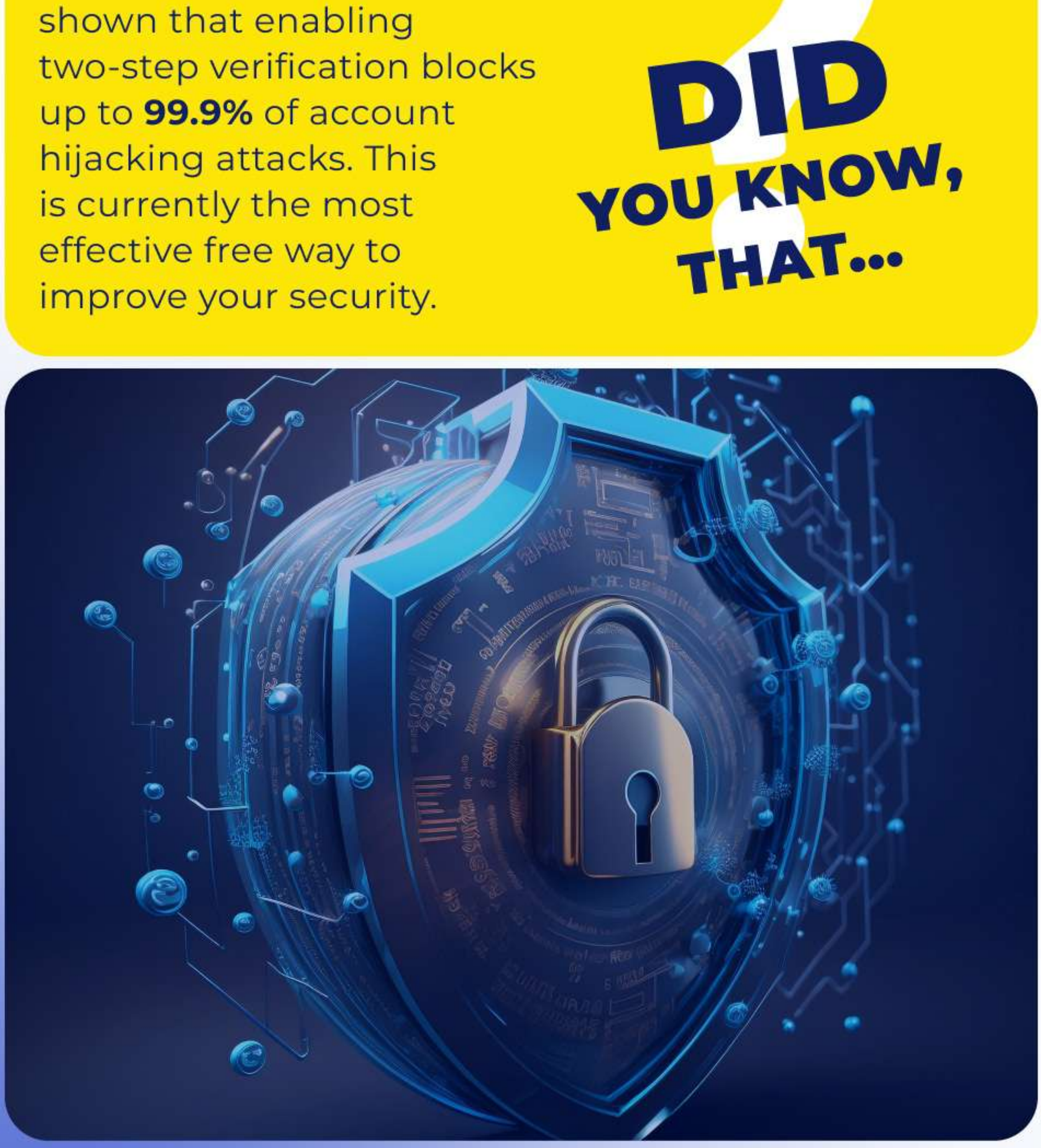
GOLDEN RULE:

On the internet, a mere 'knock, knock' is not enough – true security requires the presentation of two different identity cards.

CURIOSITY:

Microsoft research has shown that enabling two-step verification blocks up to **99.9%** of account hijacking attacks. This is currently the most effective free way to improve your security.

DID YOU KNOW, THAT...



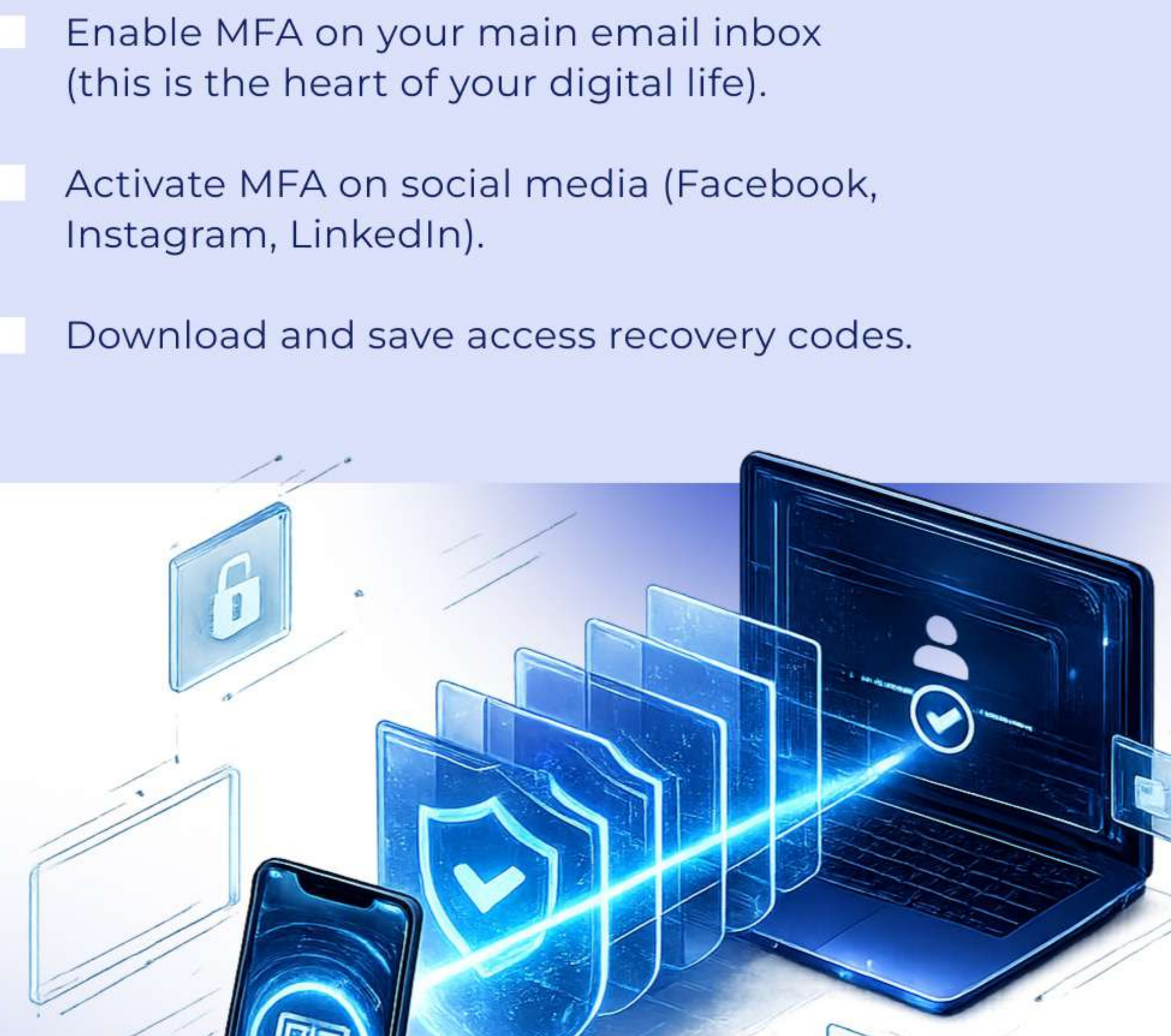
DOUBLE RIG
– TWO-STEP VERIFICATION (MFA)

BACKUP CODES:

When you enable MFA, the system will generate one-time codes. Print them out and store them in a safe place – this is your "backup key" if you lose your phone.

IMPLEMENTATION PLAN
(your checklist):

- [ ] Enable MFA on your main email inbox (this is the heart of your digital life).
- [ ] Activate MFA on social media (Facebook, Instagram, LinkedIn).
- [ ] Download and save access recovery codes.



DIGITAL IDENTITY
– CONSCIOUS PRESENCE ON SOCIAL MEDIA

PRIVACY MANAGEMENT:

The default settings for social media tend to favor the audience, not privacy. Each portal (e.g. FB, IG, LinkedIn) has a "Privacy" section, where the visibility of posts should be limited to "Friends" only.

OVERSHARING - EXCESS TRAP:

Publishing photos of tickets, boarding passes (with barcodes!), new documents or keys to the apartment is a ready-made scenario of identity theft. Your personal data is encrypted in QR codes and barcodes in the photos.

CURIOSITY:

The Internet does not forget. The ‘digital footprint’ phenomenon means that even deleted photos can survive on web archiving servers or other people’s screenshots. Your activity today builds your image in the eyes of future employers over the years.

DID YOU KNOW, THAT...

DIGITAL IDENTITY
– CONSCIOUS PRESENCE ON SOCIAL MEDIA

LOCATION RISK:

The real-time geotagging feature lets you know exactly where you are and, more importantly, that you are not at home. Publish your holiday pictures only when you return.

CLONING OF PROFILES:

Criminals copy photos and a list of friends, creating your ‘duplicate’ to extort money from your close family/friends (BLIK method). Hiding your friends list in settings almost completely eliminates this risk.

QUICK IDENTITY AUDIT:

- [ ] Is your list of friends visible to everyone? (Change to "Only Me").
- [ ] Can strangers see your phone number and email in your profile?
- [ ] Don't you see sensitive background documents in your photos?

GOLDEN RULE:

On the internet, you are what you say about yourself – but what you keep silent is your safest secret.

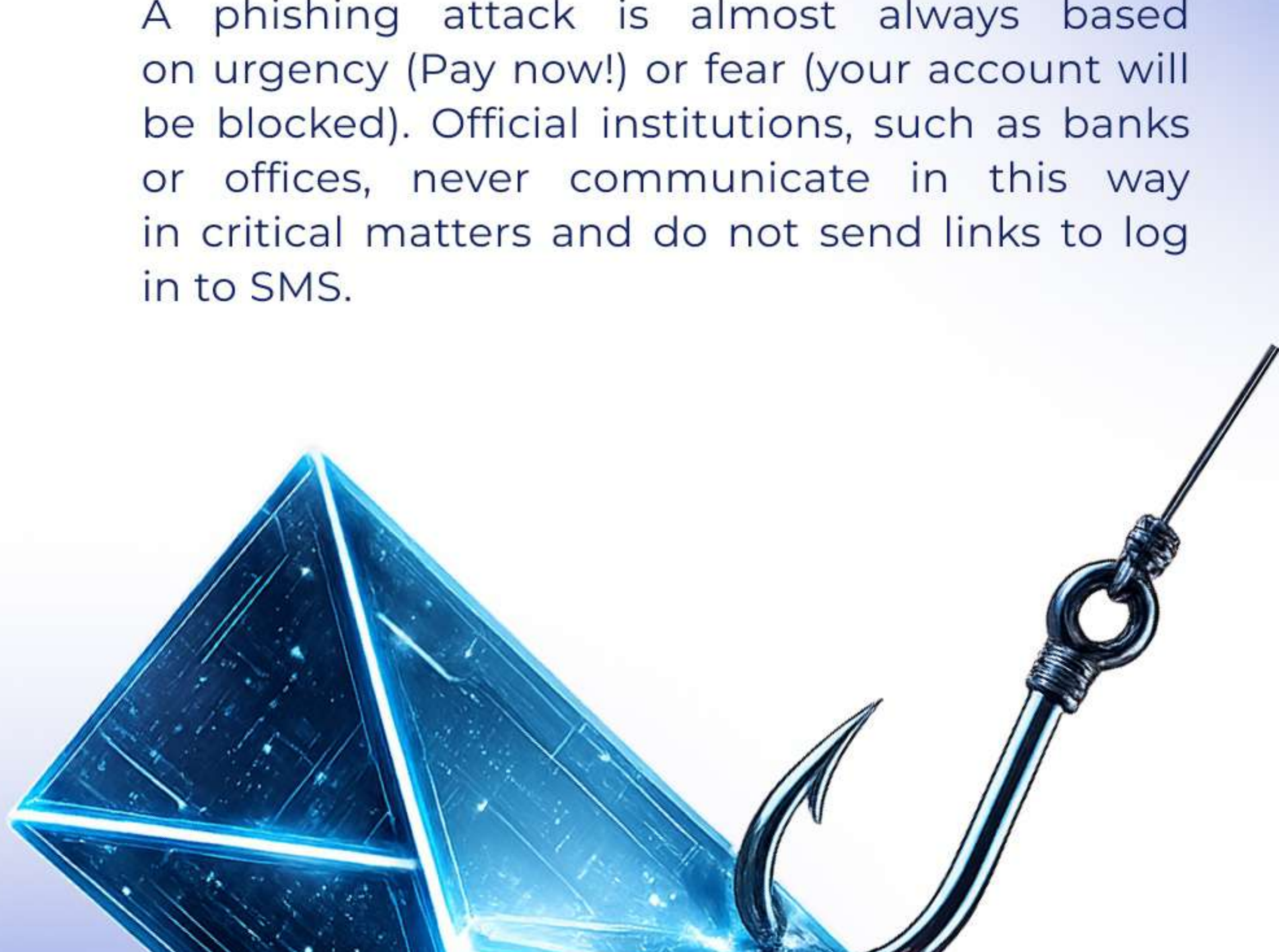
PHISHING ANATOMY
– DON'T GET CAUGHT

DOMAIN ANALYSIS (URL):

That's the fraudster's weakest point. Always check if the address is twojbank.pl and not twojbank-pl.security-check.com. Literówki type paypa1.com instead of paypal.com is standard. Remember: subdomains can be confusing, always look at what is just before the .pl or .com ending.

THE EMOTIONAL MECHANISM:

A phishing attack is almost always based on urgency (Pay now!) or fear (your account will be blocked). Official institutions, such as banks or offices, never communicate in this way in critical matters and do not send links to log in to SMS.



PHISHING ANATOMY
– DON'T GET CAUGHT

TRAP ATTACHMENTS:

Invoices in .zip, .exe or .docx documents requesting to 'enable macros' are almost a certain malware infection. Even a .pdf file can be dangerous if it comes from an unknown source.

HTTPS IS NOT EVERYTHING:

The green padlock at the address only means that the connection is encrypted, not that the site is secure. Scammers massively buy free SSL certificates to put your alertness to sleep.

METHOD 3 SECONDS (BEFORE YOU CLICK):

- Stop and take a deep breath - hurry is your enemy.
- Hover your cursor over the link (without clicking) and check the destination address in the corner of the screen.
- Ask yourself: 'Did I expect this message in this communication channel?'

PHISHING ANATOMY
– DON'T GET CAUGHT

GOLDEN RULE:

Curiosity is the 'first step to hell', but online is the first step to losing your savings.

CURIOSITY:

The first documented phishing attacks took place as early as 1995. Despite the passage of 30 years, the method remains almost unchanged, because it is not technology that is evolving, but a way of manipulating the human psyche. Today, AI helps scammers, for example, write emails without language errors, which makes it difficult to recognize them.

DID YOU KNOW, THAT...

SECURE ONLINE SHOPPING
AND FINANCE

VERIFICATION OF THE E-SHOP:

Before you buy, check the regulations, NIP and address details of the company. Spectrum stores often have ‘super promotions’ (-70% for everything), but they lack the physical address of the headquarters or the possibility of telephone contact. Use feedback portals, but look for negative ones – they are harder to falsify.

SECURE PAYMENTS:

Avoid traditional transfers to private account numbers. Use a payment gateway, temporary one-time codes (never give it over the phone!) or virtual cards for one-time transactions that become useless after purchase.

YOUR SAFETY BASKET:

- Does the store have an SSL certificate (lock) and a valid domain?
- Have you checked the reviews of the store for the last 30 days?
- Do you use a unique password for your account in the store?

SECURE ONLINE SHOPPING
AND FINANCE

THE CHARGEBACK PRINCIPLE:

If you pay by credit card directly, you are entitled to the chargeback procedure. In case of fraud or lack of delivery of goods, the bank can help you recover funds from a dishonest seller.

LOG OUT:

Always end the session after you've finished shopping or banking, especially if you're not doing it on your own home computer.

GOLDEN RULE:

If an offer on the internet seems too good to be true, it probably isn't.

SECURE ONLINE SHOPPING
AND FINANCE

CURIOSITY:

Fake online stores often appear just before Black Friday or Christmas. They can disappear from the network just 48 hours after collecting deposits from unsuspecting customers.

DID YOU KNOW, THAT...

HARDWARE HYGIENE
– YOUR DIGITAL RESILIENCE

STRENGTH OF UPDATE:

The operating system and applications are not only new features, but above all security patches. Criminals exploit vulnerabilities in the old code (so-called exploits). Set up automatic updates wherever possible – this is your cheapest and most effective insurance policy.

ANTIVIRUS SOFTWARE:

It's not outdated. Modern EDR/AV systems scan files in real time and block suspicious process behavior before they can encrypt your data.

THE "CLEAN DESK" PRINCIPLE IN THE SYSTEM:

Remove apps that you don't use. Any redundant program is a potential gateway for an intruder. Download the software only from official sources and manufacturers' websites.

HARDWARE HYGIENE
– YOUR DIGITAL RESILIENCE

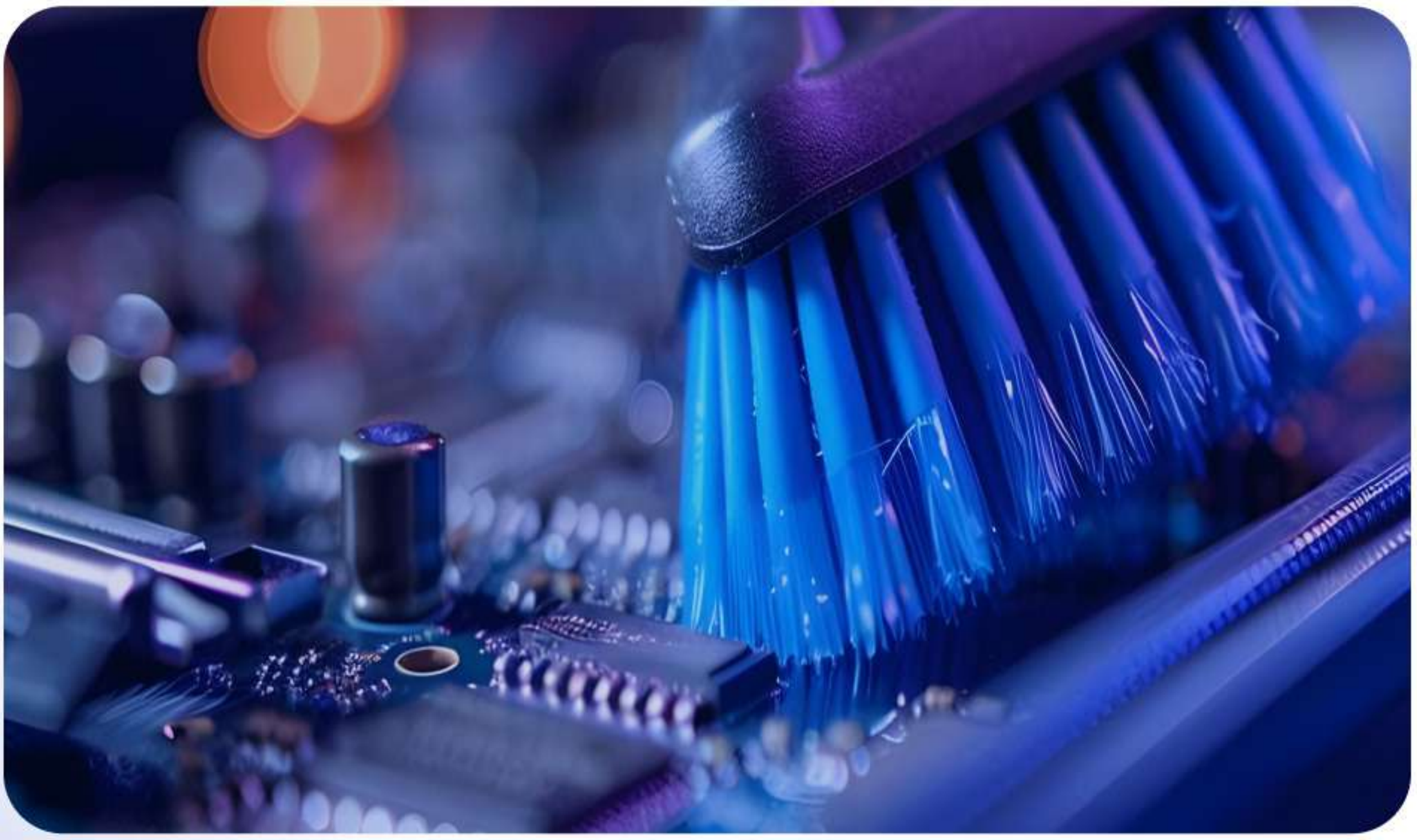
PHYSICAL LOCK:

Cybersecurity begins with physical access. Always lock the screen (Win+L / Cmd+Ctrl+Q) when you leave the computer, even at home or in the office.

PRINCIPLES OF DIGITAL CLEANLINESS:

- Is your operating system up to date?
- Do you have an active antivirus with an up-to-date signature database?
- Have you uninstalled unnecessary browser plugins (they are often spying on you)?

HARDWARE HYGIENE
– YOUR DIGITAL RESILIENCE



GOLDEN RULE:

Updating the system is not a tedious notification, but strengthening the armor of your digital fortress.

CURIOSITY:

Many of the biggest ransomware attacks in history (e.g. WannaCry) succeeded only because companies and private users waited to install a free security patch that was available months before the attack.

DID YOU KNOW, THAT...

PUBLIC WI-FI AND VPN – TRAVEL SAFETY

EVIL TWIN THREAT:

Criminals create fake access points with names identical to those of cafes or airports (e.g. “Airport_Free_HighSpeed”). When you connect to them, all your traffic passes through the hacker's computer.

MAN-IN-THE-MIDDLE (MITM) ATTACK:

In open networks, a hacker can capture the data transmitted between your device and the server. If the site does not have forced encryption, the hacker sees your logins and passwords in the form of clean text.

THE ROLE OF VPN (VIRTUAL PRIVATE NETWORK):

This is your private ‘shield’ on the public network. A VPN creates an encrypted tunnel – even if a hacker intercepts your data, it will only see an incomprehensible string of characters.

CONNECTION HYGIENE:

Turn off ‘Automatically connect to open Wi-Fi networks on your phone and laptop. Your device may unknowingly connect to a network prepared by a scammer.

PUBLIC WI-FI AND VPN
– TRAVEL SAFETY

YOUR TRAVEL PLAN:

- [ ] Do you have a VPN app installed from a trusted provider?
- [ ] Have you turned off your phone's automatic connection to public Wi-Fi?
- [ ] Do you avoid logging into a bank or mail in open networks without an active VPN?

GOLDEN RULE:

Free Wi-Fi is like talking about your finances in the middle of a full market – anyone who walks by can hear your secrets.

CURIOSITY:

Some free Wi-Fi networks in the terms and conditions (which no one reads) contain records about collecting and selling the full history of your browsing to third parties. "Free" Wi-Fi often pay with your privacy.

DID YOU KNOW, THAT...

PRIVACY AND GDPR
– YOUR DATA IS THE NEW CURRENCY

MANAGEMENT OF COOKIES:

The ‘I accept everything’ button allows hundreds of advertising companies to track your activity. Always select "Settings" and reject tracking (marketing) cookies, leaving only the necessary ones.

DATA MINIMALISM:

Provide only the information that is necessary for the performance of the service. Does the recipe app really need your date of birth and access to contacts?

PRIVACY AUDIT:

- [ ] Have you reviewed the cookie settings in your most used browser?
- [ ] Do you know what data your social network collects about you? (Check the "Your Data" panel.)
- [ ] Do you delete inactive accounts on services that you have stopped using?

GOLDEN RULE:

If you do not pay for the service with money, it means that you pay with your privacy, and the product is your data.

PRIVACY AND GDPR
– YOUR DATA IS THE NEW CURRENCY

CURIOSITY:

Your location, search history and likes allow AI algorithms to predict your future purchasing decisions (and even your health or political views) more accurately than your best friend would.

DID YOU KNOW, THAT...

THE RIGHT TO BE FORGOTTEN:

In accordance with the GDPR, you have the right to request the deletion of your data from the databases of companies with which you no longer have a relationship. Use it to reduce your digital footprint.

MARKETING 'HOOKS':

Often, registration in the service requires consent to the regulations, but underneath there are optional consents for profiling and data trading. Never mark them 'automatically'.

FAKE NEWS AND DISINFORMATION
– PROTECTING THE MIND

THE EMOTIONAL MECHANISM:

Disinformation is designed to make you angry, fearful or euphoric. If you have a strong reaction to a headline, stop. It's probably manipulation.

VERIFICATION OF SOURCE:

Check the ‘About us’ section of the portal. Does the editorial office exist? Are the authors real people? Fake pages often impersonate well-known news portals, changing one letter in the name.

YOUR TRUTH FILTER (BEFORE YOU SPECIFY):

- Is the information confirmed by at least two independent, reliable sources?
- Have you checked the date of publication? (Often old news is given as new.)
- Does the heading coincide with the content of the article or is it just a clickbait?

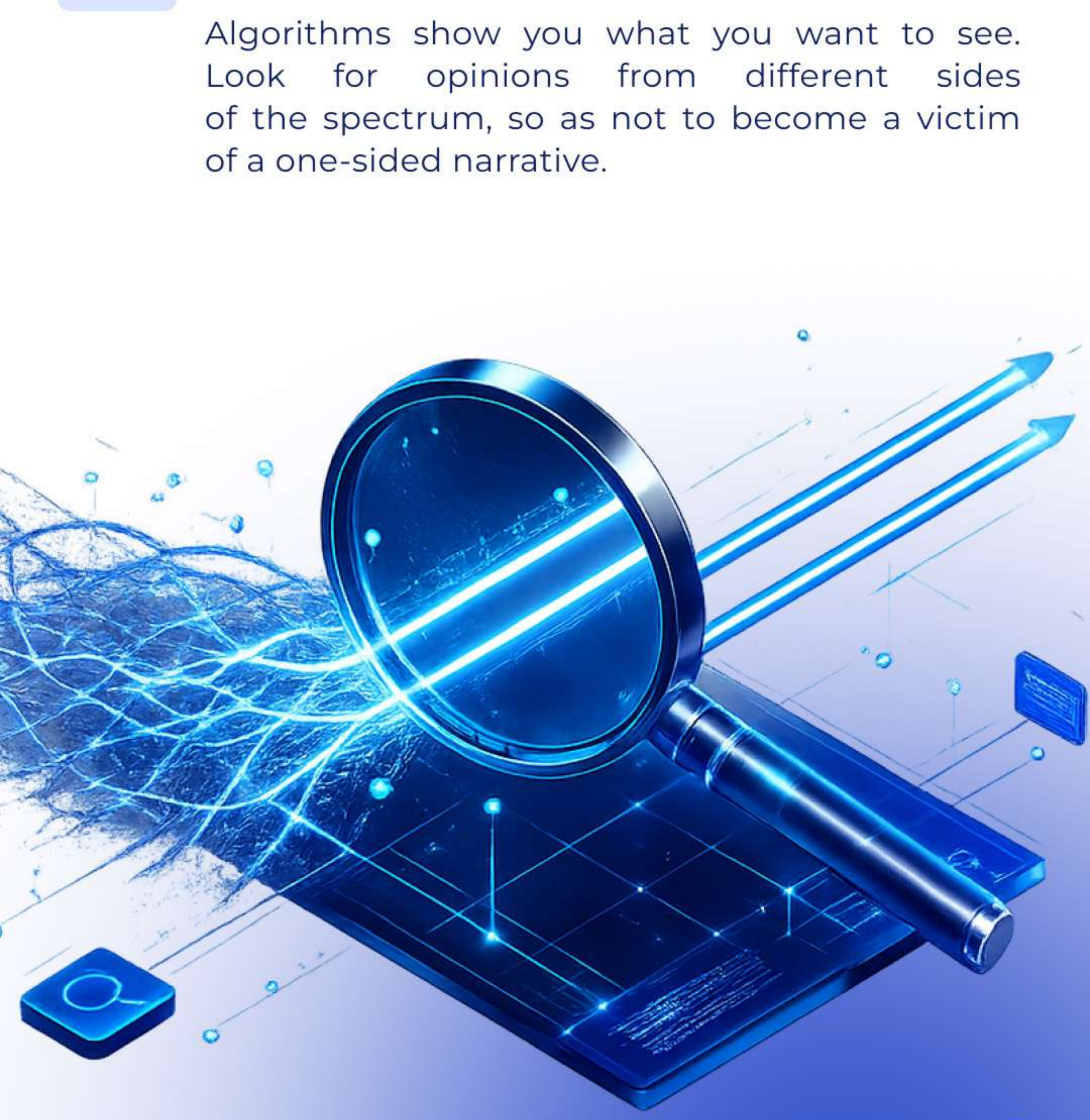
FAKE NEWS AND DISINFORMATION
– PROTECTING THE MIND

BACKWARD IMAGE SEARCH:

Scammers often use old photos from wars or disasters, assigning them a new context. Use publicly available image search engines or image identification tools to see where a photo really comes from.

INFORMATION BUBBLES:

Algorithms show you what you want to see. Look for opinions from different sides of the spectrum, so as not to become a victim of a one-sided narrative.



FAKE NEWS AND DISINFORMATION
– PROTECTING THE MIND

GOLDEN RULE:

In the digital information warfare, your pre-click pause is the most powerful weapon.

CURIOSITY:

MIT research has shown that fake news spreads on social media 6 times faster than the truth. This is because a lie is usually more sensational and "attractive" to the recipient than boring facts.

DID YOU KNOW, THAT...

SMARTPHONE
– YOUR MOST PERSONAL DEVICE

ENTITLEMENT MANAGEMENT:

Mobile apps often ask for access to contacts, microphones or galleries, even though they don't need it. Check your settings regularly to see what your games and tools know about you.

OFFICIAL SOURCES:

Never install applications from files downloaded directly from the Internet. Official system app stores automatically scan the software for malicious code – external services and websites do not.

BIOMETRICS AND CODE:

Use biometrics (fingerprint, facial scan), but always have a strong, at least 6-digit PIN code. Avoid simple graphic patterns ('set' or 'squares') that are easy to see on the screen.

REMOTE CLEANING:

Configure 'Find My Device' (Android) or 'Find My iPhone'. In case of theft, you can remotely erase all data so that it does not fall into the hands of the thief.

SMARTPHONE
– YOUR MOST PERSONAL DEVICE

MOBILE CHECKLIST:

- [ ] Do you regularly verify application permissions to work in the background?
- [ ] Have you enabled automatic hibernation of unused applications?
- [ ] Do you control background access (Bluetooth/UWB)?

GOLDEN RULE:

Your phone knows more about you than you do – make sure it doesn't tell anyone about your life.

CURIOSITY:

DID YOU KNOW, THAT...

Biometrics on your smartphone (fingerprint or facial scan) does not transmit your image to the network. This data is converted into a unique mathematical code and encrypted in an isolated, physical processor of the phone, to which neither the operating system nor any installed application has access.

RESCUE PROCEDURE
– WHAT TO DO AFTER A CYBERATTACK?

DIGITAL QUARANTINE:

If you find that something suspicious is happening on your computer or phone, immediately disconnect the device from the Internet. Turning off Wi-Fi or pulling out the network cable interrupts the hacker's connection to your hardware and stops a possible data leak in the background.

REPORTING INCIDENTS AS STANDARD:

Cyber-attack is not a shame, it's a crime. The official national contact point is CERT Polska. Applications can be made quickly and anonymously using a simple online form.

YOUR EMERGENCY CHECKLIST:

- [ ] Have you secured your other accounts and email inbox?
- [ ] Have you ‘cleaned up’ the system and installed any outstanding updates?
- [ ] Have you warned your loved ones about fraud?

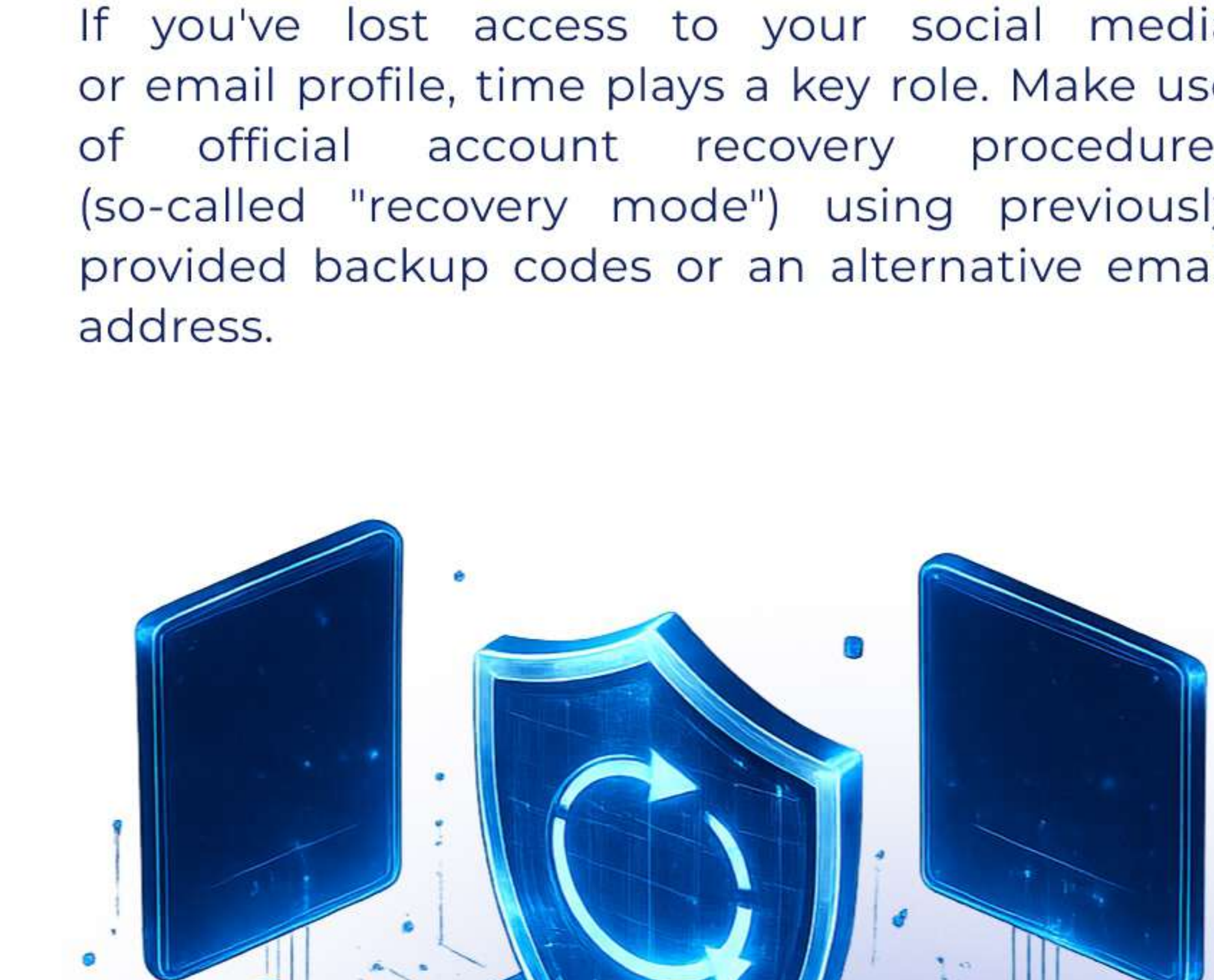
RESCUE PROCEDURE
– WHAT TO DO AFTER A CYBERATTACK?

FAST TRACK FOR SUSPICIOUS SMS:

Did you receive a suspicious message? Do not click on the link. Send all the content of this SMS to the free national number **8080**. The message will go directly to analysts who can block a fake website in the entire Polish network within a few minutes.

CONTINGENCY PLAN AFTER ACCOUNT LOSS:

If you've lost access to your social media or email profile, time plays a key role. Make use of official account recovery procedures (so-called "recovery mode") using previously provided backup codes or an alternative email address.



RESCUE PROCEDURE
– WHAT TO DO AFTER A CYBERATTACK?

CURIOSITY:

Reporting a fraudulent text message to the **number 8080** causes the dangerous domain to go to the official List of Warnings. From now on, national operators automatically block access to it, which means that one of your reports protects thousands of other people from losing money.

DID YOU KNOW, THAT...

GOLDEN RULE:

In the world of cybersecurity, response time is just as important as during a fire – the sooner you cut off the network and report an incident, the less losses will be.

ABOUT THE PROJECT:

The e-book was created as part of the implementation of the project entitled: **„CyberShield – Strengthening the Police's Competence in Combating Cybercrime"** under the terms of Financial Agreement No. FBWP. 03.01-IZ.00-0002/24 between the Department of European Funds of the Ministry of the Interior and Administration, the European Projects Service Centre of the Ministry of the Interior and Administration, and the Regional Police Commander in Radom.

The project is co-financed by the European Union under the **Internal Security Fund Programme for the period 2021–2027**

AUTHORS:

Police officers and employees of the Regional Police Headquarters in Radom and Field Branch in Radom Central Cybercrime Bureau

LIST OF OFFICIAL SOURCES AND SUBSTANTIVE FOUNDATIONS:

I. Legal and strategic acts:

- National Cybersecurity System Act of 5 July 2018 (Journal of Laws 2024, item 1077 as amended)
- Regulation 2016/679 of the European Parliament and of the Council (GDPR) on the protection of personal data and privacy of users.
- Cybersecurity Strategy of the Republic of Poland 2025-2029
- Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2), as regards measures for a high common level of cybersecurity across the Union.

II. Technical standards and recommendations:

- NIST (National Institute of Standards and Technology) standards – in particular NIST CSF 2.0 and SP 800-63B publications on digital identity.
- ISO/IEC 27001 and ISO/IEC 27032 - Information security management and cybersecurity guidelines.
- Guidelines of ENISA (European Union Agency for Network and Information Security) Cybersecurity) – in the area of digital hygiene and protection of terminal equipment.

III. Institutional materials:

- CERT Polska Annual Reports (NASK-PIB) – The safety landscape of the Polish internet.
- Recommendations and Guidelines of the Polish Financial Supervision Authority (KNF) – on the security of electronic access channels and payment services.
- Bulletin and Warnings of the Central Cybercrime Bureau (CBZC).

European Funds for Migration, Borders and Security

Republic of Poland

Co-funded by the European Union