wellcome
home

HOW NOT TO GET SCAMMED?

A GUIDE TO A SAFE INTERNET (AND BEYOND)

There are no exceptions - any of us can become a victim of fraud and a scam.
Yes, you can too (unfortunately)!

It doesn't matter if you use a smartphone, a computer, hundreds of apps daily, and you log in to your bank every day, or you use an old phone just to receive calls and text messages. The ways of thieves and cybercriminals are getting more and more sophisticated. They can call you from a number that looks like your bank's number, send you a text message from a courier's number, or impersonate a government employee.

Get to know the most popular methods scammers use and know how to protect yourself from them.

In a virtual world

The Internet (when used carelessly) is the most probable way to be scammed and there are thousands of different stories and possibilities. While you're reading this guide, someone is probably falling victim to a brand new attack. We can't predict everything, but we can awaken your vigilance to the following situations.

1. AN E-MAIL FROM A FRIEND

Dangerous emails don't have to come from unknown addresses and suspicious links. It can happen that a cybercriminal impersonates a person we know and the email address is very similar to the one we know.

What's the most common scenario?

You receive a message from a (theoretically) verified source: a company, bank, mobile operator. You're asked to download an attachment (in which you've installed a virus in your computer) or to make a money transfer (which, of course, doesn't go to the sender).

Another common scenario:

you get an email from yourself, from your email address. Scammer says that he knows what you do online, threatens to make your videos public, and demands a wire transfer to his account, usually in cryptocurrency.

What to do?

- don't be fooled and don't pay. Impersonating your email is popular and doesn't mean that someone has access to your material. Paying just proves that such scams are effective;

- don’t download any unknown attachments, don’t click on suspicious links. Verify the transfer on two screens (there is always an SMS with the confirmation of the account number and the amount);
- use the predefined transfer option. Companies you regularly deal with usually use Mass Transaction Manager so you have your individual and unchangeable account number;
- if the account number has suddenly changed, contact the company before you pay anything. This way maybe you can help detect a scam;
- don’t copy the account number from the invoice - use the predefined transfer option instead;
- verify the account number from the invoice with the number provided in the verification text message;
- use the e-mail boxes that provide built-in tools to minimize the risk of a scam. Popular services that actively prevent spam and viruses are Gmail and outlook.com.

2. DANGEROUS WEBSITES

When visiting a website do you pay attention to the link displayed in your browser? It's especially important when it comes to banking and all pages where you are required to log in, provide sensitive data, and perform financial transactions.

What’s the most common scenario?

You receive a message or an email with a link to your bank. The page you visit looks like always, the webpage address seems familiar, but… it’s not. Scammers can cheat you by changing one letter in a link (amażon.com instead of amazon.com) or registering a domain with a typo.

What to do?

- use the "Favorite Pages" tab;
- when logging in to your bank, it’s better to enter the address manually. Be careful not to make a typo. The browser itself will suggest a page you have already visited before;
- never ever log in to your bank from the unknown link;.
- if you want to know more: by clicking on the padlock in front of the link you can see who the certificate was issued to. The name should match the name of your bank.

3. NEW APPS

The amount of apps we can download is enormous - and not all of them are safe. The most problematic ones are new apps that can have malware or access to your data.

What’s the most dangerous?

All unverified apps (especially the ones where we provide any personal data) and games that are randomly downloaded by our kids. Older phones where the operating system is not updated regularly are most at risk.

What to do?

- don’t install any unknown apps on a mobile with banking access;
- if your kid downloads a lot of apps and games, give them another mobile;
- think twice before you decide to download anything;

- update your software regularly. It’s really important!

4. MAKING A TRANSFER

Did you know that a computer with a virus can "swap" your account number and put a different, wrong one on the transfer page? And the worst thing is that the virus will show us the correct one, so we can't catch the mistake.

What’s the most common scenario?

The account number comes to you by email, is provided on the website, or someone sends it to you in a chat. You copy and paste it into the appropriate field on the bank's website. You authorize the transfer by text message and check off the task. Meanwhile, the recipient is waiting for his money which will never arrive, because it went to a completely different account...

What to do?

- first: be educated! Every account number in the EU consists of 26 digits: The first 2 are the checksum, the next 8 are the bank reference, the next 16 are the account number. If the first 2 don't match, you already know something is going on;
- when accepting a transfer in the app or via SMS, verify the first two and last six digits of the number. Only then can you see the difference. Recently, banks automatically delete these digits and ask you to type them manually. If you don’t use the above mentioned predefined transfer option, it’s better to type the entire number digit by digit.

5. HOT CRYPTOCURRENCIES

Investing in cryptocurrencies has become very popular in recent times. Thus, it’s becoming more and more common to receive investment offers and to be tempted by the easy and quick returns.

What’s the most common scenario?

A cryptocurrency “specialist” contacts you and promises quick returns. The only thing you have to do is install software to give him remote control of the entire process. Of course, it’s the easiest way to give him remote access to all your data.

What to do?

- first of all: don’t believe in any magical way of getting extra money;
- never agree to install unknown software on your computer. The AnyDesk or TeamViewer names should awaken your vigilance, but the software name can be different.

6. TIME TO CHANGE YOUR PASSWORD!

When was the last time you changed your password for the bank? Where do you keep all the login and password information? How do you create a new password and how many different websites share the same one?

wellcome
home

Why is it so dangerous?

From time to time we hear about a big data leak. And what if one of these passwords is yours? If you use the same one for many websites, you leave the door for scammers open. On the other hand, using too simplistic passwords puts your data at risk for theft. Even seemingly innocuous ones - like your Facebook account - are a valuable thing for fraudsters.

What to do?

- use different logins for different websites;
- create passwords that are seemingly unrelated to you, e.g. strings of easy-to-remember words like: Umbrella1Rain.Weather;
- never keep your password in an open file (or on a random piece of paper). Use a password management system instead. We recommend BidWarden.
- if you're not using any password manager, make sure your login info to your bank is unique (not used in other places);
- if possible, use a Two Factor Authentication tool. Apart from entering a password, you'll also have to confirm the login with a text message or token. We highly recommend the 2FAS app.

In the real world

You don't have a smartphone, online bank account, or even an email address? It doesn't mean you're safe! The scammers' ideas have no limits. Be aware of danger even when receiving a simple phone call or spending a night out.

7. WHAT'S THAT NUMBER?

Any one of us has surely received a phone call from an unknown or even strange-looking number. This example has been less common lately, but it's worth remembering the most common (and still possible) scenario.

What does it look like?

You've got a strange missed call from an exotic-looking number. When calling back, you will be charged for the call, which can be extremely expensive.

What to do?

- NOTHING! Don't answer, don't call back;
- pay attention to the area code at the beginning of the phone number. A Polish number is easy to recognize as it starts with +48 or 0048. Also, you surely know the area code of your country. The rest better ignore them.

8. A CALL FROM MY BANK

This kind of phone call is more and more common recently and tough to be recognized.

Do you know that anyone can call you from any phone number? As a consequence, the scammer can call you from the real number of your bank. And not only that! The phone will even display the name of that bank. Then it only gets worse...

What is the most common scenario?
The person on the phone introduces himself as an employee of your bank. He or she verifies that you just made a transfer for X amount. After denying it (of course you didn't, you should be worried now), he/she warns you about an attempt to hack into your account and asks you to install a program on your computer or phone that will stop the illegal transaction. By downloading the indicated software you're not protecting yourself, you're just giving the scammer remote access to your computer and all your information.

What to do?
- as we've already mentioned, never install any software at the request of a stranger, even if he says he calls from your bank. You are under no obligation to do so;
- ask for the identity of the employee calling you. Hang up and call the bank yourself, checking the number on its website. Calling the bank will certainly take some time, but it'll save you an unpleasant situation. Ask if such and such a person could have called from that phone. If not, they will help you to lead the thief away;
- have in mind that even bank employees cannot understand your behavior and cannot be aware of a danger. That's okay, be persistent and keep yourself safe.

9. ... OR THE CITY OFFICE

You already know a scammer can call you from any phone number, so he can present himself as a bank employee, a policeman, or a social worker. A public service employee puts your guard down and is a great pretext for all kinds of scammers.

Possible scenario

An office worker calls you under the pretext of taking a survey. He's asking about sensitive data that - provided to the wrong person - can end up really bad for you.

What to do?

- hang up and call the office back. Have in mind that the employee may not understand why you're doing so;
- be especially prudent if anyone asks about such information like: your PESEL number*, credit card number, banking data. Never ever provide such information to an unknown person.

*In Poland, if you're a shareholder of a company, your PESEL number is publicly available. There is not much you can do in this situation, but the last number on this list will certainly help a little.

10. JUST A TEXT MESSAGE

Well, really? Same as phone calls, text messages can arrive from any number. Any kind of message with a link to click on is highly suspicious.

wellcome
home

What are the most common text messages?

- a shipping company informs you that there's a little shipment underpayment and they ask you to pay small amount so they can deliver your order;
- your mobile operator apologizes for the network failure and offers you some rebates for the breakdown you weren't even aware of;
- you receive a message for an e-commerce platform with a link to an online payment where you're asked to provide credit card details.

What to do?

- ignore such messages. By replying to them you add your data to the database so you'll keep on receiving spam. Also, such messages can cost you some money;
- watch out for suspicious links, especially those with a suffix like: hxxp://link.com/sdSFAD8.

11. THE GRANDPARENT SCAM (YES, IT STILL WORKS!)

Also called the grandchild scam, it used to be a very common scam targeting seniors. But they still occur. Recently, scammers may even pretend to be your friend and ask you for a small amount of money in an online chat.

What is the most common scenario?

These scams usually involve a phone call from someone who pretends to be your grandchild (or other cherished family member). The scammer claims to be in trouble and asks for your help. Another possible scenario is a call from a policeman that asks you to take part in a top-secret mission and wire some money. The fact that we receive a phone call from a person we (apparently) know is not a big deal for scammers. But you already knew this, right?

What to do?

- never hand over any money; it doesn't have to be a large sum. Lower amounts make you even less suspicious;
- hang up and call the person that needs your help. If it's impossible to reach them, contact another family member or trusted person to find out what's really going on;
- don't stop at one means of communication. If someone texts you on a chat app, call them and confirm that fact.

12. A NIGHT OUT

You don't have to party hard to be scammed. When out, in a crowd, it's really easy to feel relaxed, stop controlling the situation, and be an easy victim.

What is the most common scenario?

In a bustling place, while letting your glass out of sight for a moment, you are "treated" with a roofie. The next day you regain consciousness and find that you had been making wire transfers from a mobile app all night. You probably had your eyes open and approved the transfer via biometrics (face scan or fingerprint), but you just just don't remember it.

wellcome
home

What to do?

- secure your bank app with a PIN code. It's not fully safe, but when drunk or drugged, it'll be better than biometrics;
- check your bank for limits on phone-authorized transactions, BLIK payments, and transfers. Set them from your computer before you go out;
- if your mobile has a secure folder option, move all your sensitive data and apps there. They'll add another layer of protection.

13. LOAN PROTECTION

If you have Polish residency (even temporary) and a Polish PESEL number, you can apply for a loan in Poland. This means you're also a possible victim of fraud. If you're afraid somebody can have access to your personal data (you lost your documents), protect yourself from the possibility of a loan being taken out in your name or a contract being signed using your information.

How?

- In Poland, there's an institution called BIK. It's authorized to process and make available information to banks and other institutions statutorily authorized to grant loans;
- there, you can activate a loan alert to be advised anytime anyone would use your data to apply for a loan;
- the service works 24/7 and costs 24 PLN/year.
- the website is: https://www.bik.pl/klienci-indywidualni/alerty-bik. It's available only in Polish, but you can receive more info in English by calling 22 348 44 44.

Do you care about the safety of others too?

Share this info with your friends and family, send it to as many people as possible.
Help others protect themselves and let's all be aware, online and offline.

Keep safe!
Wellcome Home Team