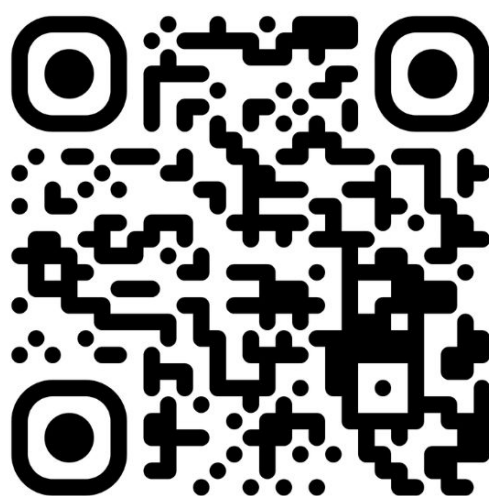




**The Internet
is a window to the world.
Open it safely!**



Technology is for people.

A little caution is enough to enjoy it without worry!



Dofinansowane przez
Unię Europejską

most
STOWARZYSZENIE

KS
Ostrava



In the network, apply the principle of limited trust

Beware of "urgent" matters

Scammers force haste to switch off your **logical thinking**. Do you feel time pressure? Stop. This short pause is your best shield against losing money or having your data stolen.

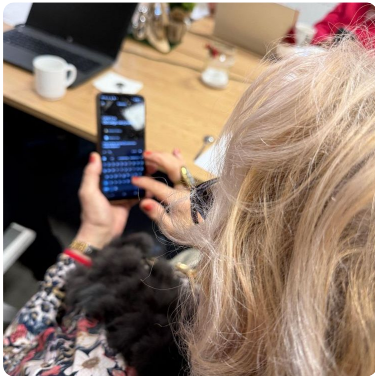
Typical examples of scams:

"Your account will be blocked!"

"You have an unpaid package!"

"Pay 2 PLN for your electricity bill!"

Most common fraud methods



Phishing

Scammers send fake e-mails or SMS messages, impersonating banks, offices, or courier companies. Their goal is to extort your personal data and passwords.



Spoofing

Criminals fake the phone number they are calling from — so that it looks like your bank, police, or another trusted institution. Don't be fooled!



"Grandchild" method

The caller pretends to be a relative or an official and asks for an urgent transfer or cash. Always verify the caller's identity by calling your family directly.

Remember: No bank, office, or police officer will call you to ask for your password, PIN, cash, or to install a "money protection app"!

When in doubt, always call the official helpline of the institution by checking the number in your contract or on their website.

How to protect yourself and your data?

Online safety begins with simple habits. These five simple rules are the foundation of your security on the web.



Strong passwords are the basis

The best password is one that is easy to remember but hard to guess. **Use a long sentence that makes sense to you.**

Example:

WinterIsMyFavouriteSeason1961!

This is safer than short passwords like Kathy123.

Remember! It's worth changing your passwords every few months.



Don't click blindly

Did you receive a link in a message from an unknown sender? **Don't click.** Instead, call the institution that the message supposedly came from directly.

Check the number on the official website, **call and verify** — that one phone call could protect you from a threat.



Verify requests for money

Someone is messaging you on Messenger or WhatsApp claiming to be your daughter or son, and asking for a quick transfer because they "lost their phone" or "have an emergency"?

Before you do anything — call them and verify using the number you know. Your loved ones will understand this caution.



Protect your personal data

Never provide over the phone or in suspicious messages: your ID number, payment card number, bank account password, or PIN code. No legitimate institution ever asks for this.



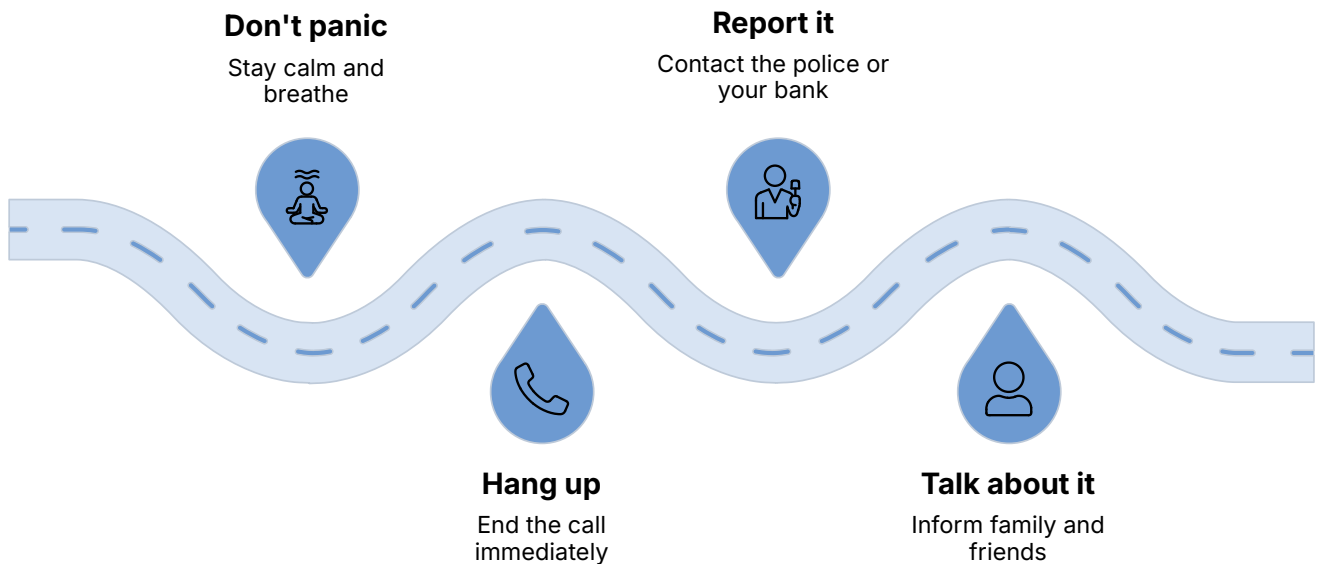
Update your software

Regular updates of your system, browser, and applications are the **best shield** against new threats. When your phone or computer asks for an update — **don't put it off until later.**

Remember, you are not alone!

If you suspect that someone tried to scam you, or you clicked on a strange link – don't panic. This happens even to technology experts. It is important that you know how to react and who to turn to for help.

What to do when something worries you?



Don't panic!

Scammers intentionally create time pressure and fear. Take a deep breath — **calmness is your advantage.**



Hang up!

If you suspect a scam, **end the call immediately.** You don't have to be polite to a scammer.



Report it!

Call the **Police (112)**. If a transaction occurred — notify your bank immediately.



Talk to your loved ones!

Share your concerns with family or friends. Together, you can recognize the threat and find help more easily.

Important numbers:

- Police: **112**
- Your bank: **number provided on the back of your payment card**

Your safety is important! Share this knowledge with neighbors, friends, and family. Together, we can protect ourselves more effectively against scammers. Be vigilant — and enjoy the Internet without fear!