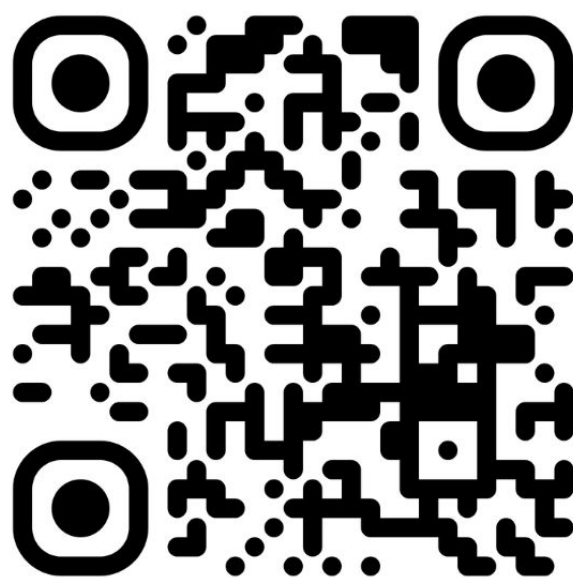




**Internet je okno do světa.
Otevírejte ho bezpečně!**



Technologie je pro lidi.

Stačí trocha opatrnosti, abyste si ji užívali bez obav!



Dofinansowane przez
Unię Europejską

mOST
STOWARZYSZENIE

KS
Ostrava



Na síti používejte zásadu omezené důvěry

Dejte si pozor na „urgentní“ záležitosti

Podvodníci vytvářejí dojem časového presu, aby vyřadili vaše logické myšlení. Cítíte časový tlak? Zastavte se. Tato krátká pauza je vašim nejlepším štítem proti ztrátě peněz nebo krádeži dat.

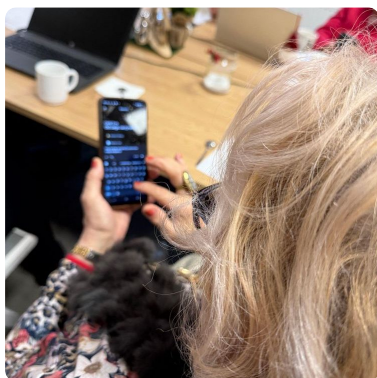
Typické příklady podvodů:

"Váš účet bude zablokován!"

"Máte nezaplacený balíček!"

"Doplaťte 2 Kč k účtu za elektřinu!"

Nejčastější metody podvodů



Phishing

Podvodníci rozesílají falešné e-maily nebo SMS zprávy a vydávají se za banky, úřady či kurýrní firmy. Jejich cílem je vylákat vaše osobní údaje a hesla.



Spoofing

Zločinci falšují telefonní číslo, ze kterého volají — tak, aby vypadalo jako číslo vaší banky, policie nebo jiné důvěryhodné instituce. Nenechte se napálit!



Metoda „na vnoučka“

Volající se vydává za blízkou osobu nebo úředníka a žádá o urgentní převod nebo hotovost. Vždy si ověřte totožnost volajícího tak, že sami zavoláte přímo rodině.

Pamatujte: Žádná banka, úřad ani policie vám nebude volat s žádostí o zadání hesla, PIN kódu, předání hotovosti nebo instalaci „aplikace na ochranu peněz“!

V případě pochybností vždy volejte na oficiální infolinku dané instituce, jejíž číslo si ověřte ve smlouvě nebo na oficiálních webových stránkách.

Jak chránit sebe a svá data?

Bezpečnost na internetu začíná jednoduchými návyky. Těchto pět jasných pravidel tvoří základ vaší bezpečnosti v síti.



Silná hesla jsou základ

Nejlepší heslo je takové, které si snadno zapamatujete, ale je těžké ho uhodnout.

Použijte dlouhou větu, která pro vás má smysl.

Příklad:

ZimaJeMojeOblibeneRoc
niObdobi1961!

To je bezpečnější než krátká hesla typu Katerina123.

Pamatujte! Svá hesla se vyplatí každých pár měsíců měnit.



Neuklikněte se

Dostali jste odkaz ve zprávě od neznámého odesílatele?

Neklikejte na něj.

Místo toho zavolejte přímo instituci, od které zpráva údajně přišla.

Najděte si číslo na oficiálních stránkách, **zavolejte a ověřte si jej** — tento jeden hovor vás může uchránit před nebezpečím.



Ověřujte žádosti o peníze

Někdo vám píše na komunikátor (např. WhatsApp, Facebook Messenger), vydává se za vaši dceru nebo syna a žádá o rychlý převod peněz, protože "ztratil telefon" nebo "má náhlou situaci"?

Než cokoli uděláte — zavolejte a ověřte si to na číslo, které znáte. Vaši blízcí tuto opatrnost pochopí.



Chraňte své osobní údaje

Nikdy po telefonu ani v podezřelých zprávách neuvádějte: rodné číslo, číslo platební karty, heslo k bankovnímu účtu ani PIN kód. **Žádná skutečná instituce o to nikdy nežádá.**



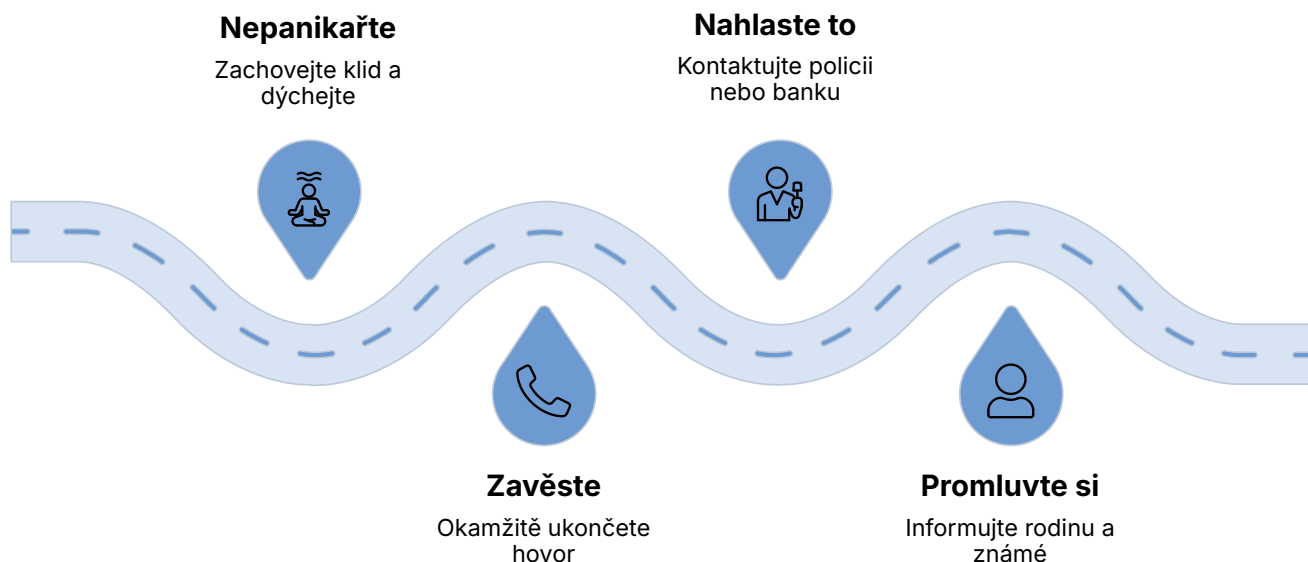
Aktualizujte software

Pravidelné aktualizace systému, prohlížeče a aplikací jsou **nejlepším štítem** před novými hrozbami. Když telefon nebo počítač vyzve k aktualizaci — **neodkládejte ji na později.**

Pamatujte, nejste na to sami!

Pokud máte podezření, že se vás někdo pokusil podvést, nebo jste klikli na podivný odkaz – nepropadejte panice. Stává se to i technologickým expertům. Důležité je vědět, jak reagovat a na koho se obrátit o pomoc.

Co dělat, když vás něco znepokojilo?



Nepanikařte!

Podvodníci záměrně vyvolávají časový tlak a strach. Zhluboka se nadechněte — **klid je vaše největší výhoda.**



Zavěste!

Pokud máte podezření na podvod, **okamžitě ukončete hovor.** Nemusíte být na podvodníka slušní.



Nahlaste to!

Zavolejte na **policii (112)**. Pokud došlo k transakci, okamžitě informujte svou banku.



Promluvte si s blízkými!

Sdílejte své obavy s rodinou nebo přáteli. Společně hrozbu snáze rozpoznáte a najdete pomoc.

Důležitá čísla:

- Policie: **112**
- Vaše banka: **číslo uvedené na zadní straně platební karty**

Vaše bezpečí je důležité! Sdílejte tyto znalosti se sousedy, přáteli a rodinou. Společně se můžeme účinněji chránit před podvodníky. Buďte ostražití — a užívejte si internet bez obav!