



BEZPEČNĚ V ONLINE SVĚTĚ: JAK SE CHRÁNIT PŘED PODVODY

brožurka pro lidi se zrakovým postižením

Milí čtenáři, vítejte v brožurce o online bezpečí

Dostává se vám do rukou brožurka, která vám pomůže zorientovat se ve světě online podvodů. Možná si říkáte, že vás se to netýká. Ale pozor – podvodníci dnes číhají i na internetu.

Zatímco dřív podvodníci zvonili u dveří nebo lákali na „výhodné nabídky“ po telefonu, dnes se často schovávají za obrazovku. Využívají internet, e-maily, sociální sítě, SMS zprávy nebo telefonáty.

Možná si říkáte, že podvodníky už dávno prokouknete. Ale oni se neustále zdokonalují. Mění tvář, styl i metody. Někdy se tváří jako pracovník banky, jindy jako dobrá duše z charitativní sbírky, vaše dcera nebo vnuk. Umí vzbudit důvěru i strach, tlačí na čas, hrají na city. A bohužel – čím více se orientují v technologiích, tím jsou nebezpečnější a vynalézavější. Jejich cíl je jediný: získat vaše peníze nebo osobní údaje.

Internet nám přináší spoustu výhod – můžeme si z domova nakoupit, podívat se na zprávy, zaplatit účty, napsat rodině. Zároveň je to ale prostor, kde se pohybují i lidé, kteří chtějí zneužít naši důvěru.

Ale nebojte se. Kdo ví, ten se může lépe bránit. Právě proto vznikla tato brožurka – abychom vás upozornili na nejčastější podvody a poradili vám, jak je rozpoznat a jak se jim bránit. Dozvíte se, jak podvodníci pracují s důvěrou, emocemi i tlakem na čas. Ukážeme si konkrétní triky, na které si dát pozor – ať už vám někdo volá, píše nebo nabízí „výhodnou“ koupi.

A kdybyste si i přesto nebyli jistí, na konci najdete kontakty na naši bezplatnou spotřebitelskou poradnu, kam se můžete obrátit.

Přejeme vám pohodové čtení a hlavně: Bezpečí v online světě i mimo něj.

Váš tým Sdružení obrany spotřebitelů Moravy a Slezska, z. s.

O online podvodech obecně



Co je to kyberpodvod?

Kyberpodvod je **podvod, který probíhá v online prostředí** – přes internet, e-mail, sociální sítě, telefon nebo mobilní aplikace.

Podvodníci z nás se z snaží **vylákat peníze nebo citlivé údaje** (hesla, čísla karet). Často se vydávají za banku, úřad nebo známou firmu a působí velmi důvěryhodně.

Dnes už zloděj nemusí číhat na ulici. Stačí mu počítač, telefon a trocha vychytralosti. Myslíme si, že jsme opatrní, ale podvodníci jsou stále vynalézavější a dokáží zaskočit i zkušené lidi.

Jaké triky používají?

- Naléhavá zpráva: „Hrozí vám pokuta, klikněte sem.“
- Telefonát od „bankéře“ či „policisty“: „Někdo se snaží dostat k vašim penězům!“
- Nabídka výhry, zázračného léku nebo výhodné koupě.
- Vydávání se za příbuzného v nouzi (třeba dceru nebo vnuka).

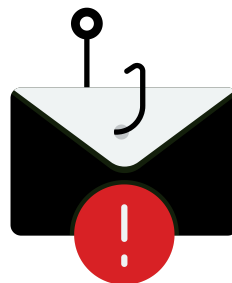
Podvodníci používají falešné weby, ukradené fotky a připravené scénáře. **Útočí na naši důvěru, emoce nebo zmatení.**

Pamatujte:

- Podvodníci jsou trpělivi a zkoušejí to znovu.
- Neustále mění metody.
- I zkušený uživatel se může nechat nachytat.

Proto je důležité znát jejich triky a vědět, jak se chránit.

Falešné e-maily a SMS zprávy (phishing a smishing)



**Když zpráva vypadá důvěryhodně,
ale ve skutečnosti vás chce oklamat.**

Co to je?

Phishing a smishing jsou podvodné zprávy, které napodobují oficiální komunikaci od banky, úřadu nebo jiné důvěryhodné organizace.

- **Phishing = podvodný e-mail**
- **Smishing = podvodná SMS zpráva**

Cílem je oklamat vás a přimět vás, abyste klikli na odkaz, zadali své údaje (např. číslo platební karty, přihlašovací jméno a heslo) nebo otevřeli přílohu, která může obsahovat škodlivý program.

Jak tyto zprávy vypadají?

- Tvrdí, že jde o **důležitou nebo naléhavou věc** (např. problém s účtem, výhra, nutné ověření).
- Obsahují **odkaz na stránku**, která vypadá důvěryhodně, ale není skutečná.
- U e-mailů může být **podezřelá adresa odesílatele**. U SMS je často odkaz zkrácený (např. bit.ly/...).
- V **příloze** může být dokument s názvem jako „faktura“, „smlouva“ nebo „upozornění“.

Proč je to nebezpečné?

Po kliknutí se můžete dostat **na falešnou stránku**, která napodobuje banku nebo úřad. Tam po vás mohou chtít **zadání citlivých údajů**.

Jindy se po kliknutí **stáhne škodlivý program**, který sleduje, co píšete, nebo ovládne váš telefon nebo počítač.

Pamatujte! E-maily a SMS mohou vypadat jako od banky nebo úřadu, ale často jde o dobře připravený trik. Nikdy nevyplňujte údaje, pokud si nejste jistí, komu je posíláte.

Zprávy často tvrdí, že:

- máte nedoplatek nebo vám naopak přijde balík,
- že někdo zneužil váš účet a musíte ho okamžitě zabezpečit,
- nebo že vás čeká peněžní výhra, když „potvrdíte údaje“.

Příklad ze života:

Paní Milada dostala e-mail, který vypadal jako zpráva z České pošty. Psalo se v něm, že má nedoplatek 29 korun a že balík nebude doručen, pokud nezaplatí. Klikla na přiložený odkaz, vyplnila své údaje a zaplatila.

O pár dní později jí z účtu odešly tisíce korun. **Podvodník pomocí získaných údajů získal přístup k jejímu bankovníctví.**



Jak se bránit?

- Neklikejte na odkazy ve zprávách, kterým nerozumíte nebo které působí podezřele.
- Zkontrolujte adresu odesílatele.
- Neposílejte své údaje ani čísla karet přes e-mail nebo SMS.
- Pokud si nejste jistí, volejte přímo dané instituci.

Poznámka:

Podvodné adresy nebo odkazy často vypadají velmi podobně jako ty skutečné. Rozpoznání nepatrných rozdílů v doméně je velmi obtížné, zejména při používání čtečky obrazovky, která čte adresu monotónně bez kontextu.

Proto nespolehejte na to, že adresu rozpoznáte.

Jakmile má zpráva podezřelý obsah, neklikejte a vše si raději ověřte.

Praktické rady

- Banky a úřady nikdy neposílají zprávy s výzvou k zadání údajů.
- Pokud vám zpráva přijde podezřelá, ověřte si ji jinde – ideálně telefonicky.
- Uživatelé čteček a slabozrací lidé by neměli spoléhat na kontrolu vizuálních detailů.
- Pokud používáte hlasovou čtečku a slyšíte podivnou adresu (např. s .com místo .cz, nebo s pomlčkou navíc), zpozorněte a neklikejte.

Podvodné telefonáty



Dejte si pozor, kdo vám volá

Co to je?

Podvodníci vám mohou **zavolat a vydávat se za někoho důležitého** – například za pracovníka banky, úředníka, policistu, technickou podporu nebo dokonce rodinného příslušníka.

Chtějí z vás **vymámit osobní nebo finanční údaje**. Tento typ podvodu se nazývá **vishing** – od slova „voice phishing“, tedy podvod přes hlasový hovor.

Jak podvodný hovor vypadá?

Telefon zazvoní. Na displeji neznámé číslo. Ozve se hlas, který se představí jako pracovník banky, policista nebo třeba úředník z finančního úřadu:

„Váš účet je v nebezpečí. Hrozí ztráta peněz. Musíme to hned vyřešit. Poradím vám, co dělat.“

Hovor může znít velmi přesvědčivě – volající mluví **klidně, slušně a profesionálně**. Současně využívá **naléhavý tón**, aby vás přiměl jednat rychle.

Co může podvodník chtít?

- Přihlašovací údaje k účtu.
- Kódy z SMS zprávy.
- Číslo platební karty.
- Instalaci programu do počítače nebo telefonu.
- Převedení peněz „na bezpečný účet“ – který ve skutečnosti patří podvodníkovi.

Proč je to nebezpečné?

Pokud tyto informace předáte, může vám útočník **vybrat peníze z účtu nebo získat přístup k vašim osobním údajům**.

Někteří podvodníci vás mohou požádat, abyste nainstalovali program, který jim umožní **ovládnout váš počítač nebo mobil**.

Příklad ze života:

Paní Anně zazvonil telefon. Neznámé číslo, ale vzala to. Volal muž, který se představil jako pracovník její banky. Zněl slušně, mluvil klidně, ale naléhavě:

„Paní Anno, někdo se pokouší dostat na váš účet. Musíme ho hned zabezpečit, pomohu vám.“

Chtěl, aby mu nadiktovala své přihlašovací údaje k bankovnímu účtu i kód z SMS, který jí právě přišel. Prý jen pro ověření. Paní Anna kód řekla. Pak ještě jeden.

Za pár minut jí přišla zpráva, že z jejího účtu odešla platba 60 000 korun. Volající mezitím položil telefon a už se neozval.



Jak se bránit?

- **Nikdy nikomu po telefonu neříkejte své přístupové údaje.**
- Ani banka, ani úřad, ani policie po vás nikdy nebude chtít přihlašovací jméno, heslo nebo kód z SMS.
- **Nenechte se tlačit do rychlého rozhodnutí.**
- Podvodníci spěchají, protože nechtějí, abyste si vše promysleli.
- **Ukončete hovor. Řekněte: „Omlouvám se, ověřím si to přímo u banky“**
- Ověřte si situaci na oficiálním čísle instituce, za kterou se volající vydával.
- **Nastavte si u banky bezpečnostní limity.** I když něco zadáte omylem, předejdete vysoké ztrátě.
- Pokud se jednalo o podvod, **nahlaste to** bance a Policii ČR.

Poznámka:

Podvodníci často používají techniku zvanou **spoofing** – vaše zařízení může ukazovat **běžné nebo známé telefonní číslo**, ale ve skutečnosti volá někdo jiný. Takže ani když se na displeji ukáže „Vaše banka“, nemusí to být pravda. V tomto případě je vizuální kontrola čísla k ničemu.

Pamatujte! Banka, policie ani jiná instituce vám nikdy nevolá proto, aby z vás dostala hesla, PINy, kódy z SMS nebo číslo karty. Nikdy vás nebude žádat o převod peněz telefonicky.

Podvodné e-shopy

Zboží si objednáte, ale nic vám nepřijde – nebo přijde něco úplně jiného



Co to je?

Podvodné e-shopy jsou **falešné internetové obchody**, které napodobují skutečné stránky. Nabízejí různé zboží – často velmi levně. Cílem podvodníka je, abyste zboží **zaplatili předem, ale nic vám nepošle**. Může také **získat údaje o vaší platební kartě**.

Příklad ze života:

Pan Antonín našel na internetu obchod, kde prodávali pánské hodinky s velkou slevou. Stránka vypadala seriózně, dokonce měla i českou vlajku a popis v češtině. Hodinky stály jen 399 korun místo původních 1 800.

Pan Antonín objednal, zaplatil předem, ale zboží nikdy nedorazilo. Na e-shop už se později nedalo ani přihlásit. Když se snažil dohledat firmu, zjistil, že na stránce nebyl žádný kontakt, jen anonymní e-mail.

Jak podvodný e-shop poznáte?

E-shop může na první pohled působit normálně. Ale přesto je falešný.

Následující znaky vám mohou pomoci:

- Nabízí zboží za **podezřele nízké ceny**.
- Web **nemá žádné kontaktní údaje** – chybí telefon, adresa, sídlo firmy.
- **Není zde uvedeno IČO, ani obchodní podmínky**.
- Vyžaduje **platbu předem** a nenabízí žádnou jinou možnost.
- Nemá **žádné recenze nebo hodnocení, nebo jsou podezřele „dokonalé“**.

Proč je to nebezpečné?

- Zaplatíte zboží, ale žádné nepřijde.
- Zadáte údaje o své platební kartě – a podvodník je zneužije.
- Můžete si nevědomky stáhnout virus, pokud na stránce na něco kliknete.



Jak se bránit?

- **Nakupujte jen na známých webech nebo ověřených e-shopech.**
- Pokud web neznáte, **hledejte si o něm informace** – recenze, zkušenosti jiných lidí.
- **Ověřte si e-shop** na stránkách České obchodní inspekce - přehled dosud známých rizikových e-shopů najdete na stránce <https://coi.gov.cz/pro-spotrebitele/rizikove-e-shopy/>
- Zkontrolujte, zda má web **kontakty, IČO a obchodní podmínky**.
- Pokud web vyžaduje **platbu předem** kartou, **buďte opatrní**.
- Pokud máte pochybnosti, nakupte raději jinde – **raději bezpečně než levně**.

Poznámka:

Mnohé výstražné znaky jsou vizuální (např. vzhled loga, grafika, podezřelá doména), což je pro lidi se zrakovým postižením obtížné nebo nemožné zkontrolovat.

Proto se doporučuje spoléhat hlavně na:

- informace v textu (např. jestli web obsahuje obchodní podmínky a kontakty),
- zkušenosti druhých (ověřené recenze z nezávislých webů),
- a opatrnost při platbě – předem nikdy neposílejte peníze do neznámého obchodu.

Na internetu dnes nakupuje čím dál více lidí. Je to pohodlné, rychlé, často i levnější. Ale právě na důvěřivost zákazníků čekají podvodníci. Vytvoří falešný e-shop, který vypadá lákavě – nabízí nízké ceny, zboží skladem a rychlé dodání. Jenže po zaplacení se nic nestane.

Stránka buď přestane existovat, nebo vám pošlou něco úplně jiného – třeba místo bot levné pantofle, nebo vůbec nic.

Pamatujte! Na internetu může obchod spustit každý. Vzhled stránky ještě neznamená, že je důvěryhodná.

Když něco vypadá podezřele levně, buďte opatrní.

Bazarové podvody

Když prodáváte nebo nakupujete v bazaru a někdo vás chce napálit



Co to je?

Bazarové podvody jsou **podvody spojené s nákupem nebo prodejem věcí přes inzeráty** – například na stránkách jako Bazoš, Sbazar, Facebook Marketplace nebo Mimibazar.

Na bazarových webech a aplikacích můžete najít výhodné nabídky nebo si přivydělat prodejem věcí, které už nepotřebujete. Jenže právě tady číhá čím dál víc **podvodníků – a to jak na kupující, tak na prodávající.**

V obou případech chtějí získat vaše peníze nebo údaje.

Jak vypadá podvod “prodejce”?

- Někdo nabízí zboží – například mobil, kočárek nebo náradí – za nízkou cenu.
- Komunikace probíhá přes e-mail, Messenger nebo WhatsApp.
- Podvodník vás požádá o platbu předem, často pod záminkou, že „zboží hned odesílá“.
- Po zaplacení zboží nikdy nepříjde. Podvodník kontakt přeruší.

Příklad ze života:

Pan Luděk chtěl na Facebooku koupit použité chodítko. Prodávající požadoval platbu předem. Po zaplacení přestal komunikovat. Objednané zboží nikdy nepřišlo.

Jak se bránit?

- Platte pouze po převzetí zboží, nebo používejte ověřené platební brány (např. přes Alza, Aukro, Vinted).
- Pokud musíte platit předem, ověřte si prodávajícího – např. telefonicky nebo podle recenzí.
- Neklikejte na odkazy poslané ve zprávě – místo toho si najděte web ručně.

Jak vypadá podvod “kupujícího”?

- Vy sami prodáváte něco přes bazar.
- Ozve se zájemce, který chce zboží rychle koupit.
- Tvrdí, že zaplatí ihned, ale potřebuje „ověřit platbu“.
- Pošle vám odkaz na falešnou stránku, která napodobuje službu (např. Českou poštu, Zásilkovnu nebo platební bránu).
- Tato stránka vás vyzve, abyste zadali číslo karty a další údaje.
- Pokud to uděláte, podvodník vám může z účtu ukrást peníze.

Příklad ze života:

Paní Marta nabízela přes internetový bazar starší mobilní telefon. Krátce po zveřejnění inzerátu jí napsal zájemce. Byl milý, psal česky a ihned souhlasil s cenou.

„Pošlu pro zboží kurýra,“ napsal. „Stačí jen potvrdit příjem platby přes odkaz.“

Zaslal paní Martě odkaz na stránku, která vypadala jako web přepravní služby. Marta na něj klikla a objevila se výzva k zadání údajů z platební karty – prý aby mohla „přijmout platbu“. Vyplnila číslo karty, datum a kód.

Jenže o žádný nákup nešlo. Podvodník takto získal přístup k její kartě a z účtu jí následně odešlo 9 000 korun.

Jak se bránit?

- Neposílejte žádné údaje o své kartě. K příjmu platby je nikdy nepotřebujete.
- Opravdový kupující nepotřebuje vaši kartu ověřovat.
- Pokud vám někdo tvrdí, že pro ověření platby musíte kliknout na odkaz, jde o podvod.

Proč je to nebezpečné?

- Ztratíte peníze, aniž byste cokoli dostali.
- Podvodník může získat vaše údaje – číslo karty, přihlašovací jméno a heslo.

Pamatujte! Pokud si nejste jistí, raději obchod nedokončujte. **Lepší přijít o nabídku než o peníze.**

Falešné inzeráty na Facebooku

Pozor na reklamy na léčivé přípravky a zdravotní pomůcky



Co to je?

Na Facebooku se často objevují reklamy, které slibují zázračné uzdravení nebo rychlé řešení zdravotních problémů – například bolesti zad, cukrovku, či vysoký krevní tlak. Může jít o léky, doplňky stravy, zdravotní pomůcky nebo přístroje. K tomu může být připojeno **falešné doporučení od známého lékaře** či **vymyšlené recenze**.

Tyto reklamy často vedou na podvodné stránky, které napodobují známé weby – např. Novinky.cz, iDnes.cz nebo televizi Nova.

Cílem je nalákat vás na nákup. Zboží však buď vůbec nedorazí, nebo přijde **nekvalitní, nepovolený a někdy i nebezpečný výrobek**. A vaše údaje (například telefon nebo adresa) mohou skončit u dalších podvodníků.

Jak takový podvod poznám?

- Text inzerátu **slibuje neuvěřitelné účinky** – třeba že „vyčistí cévy za 3 dny“ nebo „nahradí operaci“.
- Stránka **vypadá jako zpráva z televize nebo rozhovor s lékařem** – ale ve skutečnosti je falešná.
- U výrobku jsou **falešné recenze** – všichni ho chválí, nikdo si nestěžuje.
- Na stránce není **žádná kontaktní adresa nebo IČO firmy**.
- Chtějí po vás, abyste **rychle objednali** nebo „vyplnili formulář“.
- Oslovují vás **naléhavě nebo emotivně** – „Neváhejte, zdraví nepočká!“

Proč je to nebezpečné?

- Zaplatíte za výrobek, který nefunguje – nebo ho ani nedostanete.
- Zadáte osobní údaje – jméno, telefon, e-mail. Může se stát, že vám pak budou volat podvodníci.
- Můžete užít něco, co vám ublíží, protože produkt neprošel žádnou kontrolou (např. SÚKL).

Příklad ze života:

Paní Drahomíra narazila na Facebooku na inzerát:

„Lékař z Brna vyvinul mast, která léčí klouby bez léků – sleva 80 % jen dnes.“

Na stránce byly citace známého chirurga, logo České televize a desítky „spokojených“ recenzí. Paní objednala dvě masti, zaplatila kartou. Přišlo jí cosi bez popisu v plastových obalech, bez návodu, bez výrobce.

Zneklidněla – a po delším hledání zjistila, že firma má sídlo v zahraničí, žádné recenze nejsou pravé a že produkt není registrován u žádného úřadu. O peníze už přišla – a použít mast se bála.



Jak se bránit?

- **Neobjednávejte nic přes neověřené reklamy** na sociálních sítích.
- **Zkuste si výrobek „proklepnout“** – napište jeho název do vyhledávače + „podvod“.
- Nikdy **nezadávejte údaje o kartě na stránkách, kterým nevěříte.**
- U **zdravotních pomůcek** se podívejte, zda jsou **registrované u Státního ústavu pro kontrolu léčiv (SÚKL)**

Poznámka:

- Falešné reklamy napodobují seriózní weby a média – např. vizuální styl, loga, titulky. To je velmi těžké odhalit pomocí čtečky obrazovky.
- Recenze mohou vypadat jako od běžných lidí, ale jsou vymyšlené. Čtečka přečte text, ale neodhalí falešné fotografie ani podvržené jméno „lékaře“.
- Pokud je stránka plná obrázků bez alternativních popisů (ALT), může být celá nečitelná.

Na Facebooku se často objevují zázračné přípravky, které slibují rychlé uzdravení – ale ve skutečnosti jde mnohdy o podvod. Pamatujte, že **seriózní léky se nikdy neprodávají přes anonymní inzeráty**. Vaše zdraví není zboží – a pokud nějaká nabídka zní až příliš dobře, je to důvod k opatrnosti. Když jde o zdraví, buďte opatrní dvojnásob. Na Facebooku může inzerovat každý – i podvodník.

Falešné výhry a soutěže

Slíbují vám výhru? Možná vás chtějí okrást



? ? Co to je?

Na internetu, hlavně na sociálních sítích, se často objevují soutěže a oznámení o výhře, které jsou ve skutečnosti pastí na důvěřivé uživatele. **Podvodníci tvrdí, že jste něco vyhráli – přestože jste se do žádné soutěže nepřihlásili.**

Může jít o zprávu typu:

„Gratulujeme! Byli jste vylosováni jako výherce nového telefonu. Klikněte sem a zadejte údaje pro doručení.“

„Vaše jméno bylo vybráno v soutěži o dárkový balíček! Stačí zaplatit poštovné 39 Kč.“

Jenže **žádná výhra neexistuje**. Odkaz vás odvede na falešnou stránku, která má **jediný cíl – získat vaše osobní nebo platební údaje**.

Příklad ze života:

Paní Olga viděla na Facebooku soutěž o kuchyňský robot. Stačilo napsat komentář a sdílet příspěvek. O pár dní později jí přišla zpráva, že vyhrála. Zpráva obsahovala odkaz – „potvrzení výhry“. Po kliknutí zadala své jméno, adresu a číslo platební karty kvůli „uhrazení poštovného“. O pár dní později jí z účtu zmizely peníze.

Když se snažila stránku znovu najít, už neexistovala.

Jak poznat falešnou výhru?

- Výhra **přijde nečekaně**, i když jste se žádné soutěže neúčastnili.
- Zpráva vypadá oficiálně (např. z ČEZ, České pošty, Tesca), ale **je z neznámého profilu**.
- Zpráva vás **nutí jednat rychle – výhru prý ztratíte, pokud hned nezaplatíte**.
- Požadují **citlivé údaje nebo číslo karty**.
- **Webová stránka** soutěže vypadá zvláštně, má chyby nebo je na **podezřelé adrese**.



Proč je to nebezpečné?

- Pošlete peníze – ale nic nevyhrajete.
- Zadáte citlivé údaje – podvodníci je mohou zneužít.
- Můžete se stát terčem dalších podvodníků, protože jste „zareagovali“.



Jak se bránit?

- Nevěřte výhře, o kterou jste nežádali.
- Nezadávejte údaje jen proto, že někdo slibuje dárek.
- Vždy se podívejte, kdo zprávu poslal – falešné účty se tváří jako oficiální.
- Neplatte nic dopředu – seriózní soutěže nevyžadují poplatky.
- V případě pochybností se poraďte s někým důvěryhodným.

Poznámka:

- Pokud vám soutěž přišla do soukromé zprávy nebo e-mailu, a tvrdí, že jste vyhráli, je to podezřelé.
- Čtečka obrazovky nemusí rozeznat rozdíl mezi falešným a pravým profilem.
- Falešný web může napodobovat např. Facebook, Tesko, Českou poštu – hlasová čtečka vám neřekne, že adresa je divná. Vždy si ověřte, kdo za soutěží stojí.

Pamatujte! Výhra bez soutěže neexistuje. **Když jsem nehrál, nic jsem nevyhrál.**

A pokud po vás někdo hned chce údaje nebo peníze – buďte opatrní. **Dárek, který chce zaplatit – není dárek.**

Nejspíš se nesnaží vám něco dát, ale vzít.

Falešné sbírky na sociálních sítích

Podvodníci se nebojí hrát na city a zneužívají
soucítí i důvěru



Co to je?

Na Facebooku a jiných sociálních sítích se často objevují příspěvky s fotografií nemocného dítěte, seniora po úrazu nebo člověka na vozíku.

Tyto sbírky často vzbuzují soucit a lidé je rychle sdílejí – nebo rovnou přispějí. Jenže ne všechny jsou skutečné. Podvodníci si **vymýšlejí příběhy**, kradou fotky z internetu a **lákají peníze na účty, které nepatří žádné charitě**. A žádná pomoc se ke skutečně potřebným nedostane.

Příklad ze života:

Pan Josef přispěl na sbírku, která prosila o pomoc „samoživitelce s dítětem po požáru bytu“. Příběh ho dojal. Přes odkaz ve Facebooku poslal 300 Kč.

Později mu známý poradil, ať si zkontroluje účet sbírky. Ukázalo se, že stránka byla vytvořena anonymně, žádná oficiální organizace ji nezastřežovala – a stejná fotografie dítěte se objevila už u jiných podvodných sbírek.

Jak poznat falešnou sbírku

- Není uvedena žádná oficiální charitativní organizace (např. Charita ČR, Člověk v tísni, Konto Bariéry...).
- Není dohledatelný skutečný příběh osoby, na kterou se sbírá.
- Sbírka nemá transparentní účet ani identifikační číslo.
- Fotografie působí obecně, často se opakují.
- Text apeluje silně na emoce, ale chybí konkrétní informace.



Proč je to nebezpečné?

- Ztratíte peníze, které nedojdou k potřebným.
- Vaše důvěra v charitu bude oslabena.
- Podvodníci mohou získat vaše platební nebo kontaktní údaje, pokud sbírka běží mimo oficiální platformy.



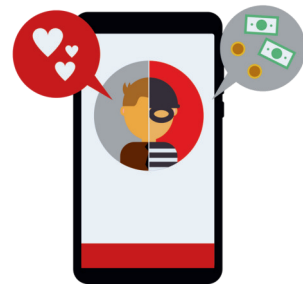
Jak se bránit?

- Přispívejte jen přes ověřené sbírkové portály.
- Nevěřte automaticky příběhu ve zprávě nebo příspěvku.
- Pokud vás sbírka osloví, zkuste si o ní něco zjistit – napište název do vyhledávače, hledejte zprávy nebo recenze.
- Zkontrolujte, zda je sbírka uvedena na oficiálním webu organizace.
- Pokud nemůžete sbírku ověřit sami, požádejte někoho důvěryhodného o pomoc.
- Neplatte na účet zveřejněný jen v obrázku bez dalších údajů.

Pamatujte! Srdceryvný příběh nemusí být vždy pravdivý. Pomáhat je jistě správné, ale než pošlete své peníze, ověřte si, že jdou skutečně na deklarovaný účel. Vaše dobrá vůle může být snadno zneužita a vy byste mohli přijít o víc než jen důvěru v charitativní sbírky.

Romantické podvody

Láska přes internet? Někdy je to jen hra na city a útok na vaši peněženku.



Co to je?

Romantické podvody (tzv. love scams) jsou případy, kdy se někdo na internetu vydává za vašeho partnera nebo partnerku a snaží se vybudovat si s vámi citové pouto.

Podvodníci se často vydávají za někoho, kdo hledá lásku, přátelství nebo porozumění. Využívají samoty a touhy po blízkosti.

Píší zprávy na sociálních sítích nebo přes různé seznamky. Jsou pozorní, milí, zajímají se o vás... A pak začnou mluvit o problémech a žádají o peníze.

Nejde o skutečný vztah. Je to **podvod** – a **velmi nebezpečný**.

Jak romantický podvod vypadá

- Osoba, kterou neznáte a nikdy jste ji neviděli, vás osloví s tím, že ji zaujal váš profil na sociální síti nebo v seznamce.
- Po navázání kontaktu s vámi začne budovat vztah. Podvodníci jsou ke svým obětem pozorní, zajímají se o ně, mají pro ně pochopení. Postupně si budují důvěru, prostřednictvím milostných zpráv, dárků nebo projevů náklonnosti. Tento proces může trvat několik týdnů i měsíců. Nakonec začne mluvit o společném životě.
- Má dojemný příběh – je voják, lékař v zahraničí, vdovec, podnikatel...
- Po čase začne tvrdit, že se dostal do potíží a potřebuje peníze: na letenku, na léčbu nemocného dítěte, na právníka...
- Když oběť peníze odešle, podvodník si často vymýšlí další a další důvody, proč je potřeba poslat víc. Takto může oběť postupně přijít o značné finanční prostředky, aniž by si dlouho uvědomila, že se stala obětí podvodu.

Proč je to nebezpečné?

- Můžete přijít o velké částky peněz.
- Budete psychicky zraněni – člověk, kterému jste věřili, vás podvedl.
- Podvodníci často oslovují více lidí najednou – nejste jediní.

Příklad ze života:

Paní Milena si psala s mužem, který se představil jako americký voják na misi. Po několika týdnech dopisování jí začal vyznávat lásku. Pak požádal o pomoc – prý chce přijet, ale nemá peníze na cestu. Poslala mu 70 000 Kč.

Po týdnu napsal, že byl zatčen a potřebuje dalších 10 000 Kč na kauci. Tam už paní Milena znejistěla – a když se svěřila synovi, zjistili, že šlo o podvodníka, který měl stejný text v desítkách jiných případů.

Varovné znaky:

- Osoba, se kterou jste se sotva seznámili, vás brzy osloví „lásko“, „miláčku“, „moje duše“.
- Profil podvodníka často obsahuje **atraktivní fotografie** a pečlivě vytvořený **příběh, který má za cíl vzbudit důvěru a zájem**.
- Nechce se spojit přes **videohovor** (nebo tvrdí, že kamera nefunguje).
- Po čase **začne chtít peníze. Naléhavě potřebuje vaši pomoc**.



Jak se bránit?

- Budte opatrní, pokud vás kontaktuje **neznámý člověk** a rychle vám začne lichotit.
- **Nikdy neposílejte peníze** nikomu, koho jste osobně neviděli.
- Nenechte se zmást **emotivními příběhy** – podvodníci hrají na city.
- Pokud si nejste jisti, **poradte se s někým, komu věříte**.
- Zkuste **vyhledat profilovou fotku** online – může být zneužitá.
- **Ukončete komunikaci**, pokud vás někdo začne nutit k poslání peněz nebo sdílení osobních údajů.

Pamatujte! Pravá láska nikdy nežádá o peníze.

Podvodníci umí být přesvědčiví – ale ne všichni, kdo vám píší krásná slova, to myslí upřímně.

Investiční podvody

Když vám někdo slibuje rychlé zbohatnutí, bývá to past



Co to je?

Možná už jste někdy narazili na reklamu, která slibovala snadné zbohatnutí. Stačí málo – pár kliknutí, malá investice a brzy prý budete vydělávat tisíce korun denně. Takové nabídky znějí lákavě, zvláště když je doporučuje „známá osobnost“ nebo někdo, kdo působí jako odborník. Jenže právě v tom je nebezpečí.

Za těmito „výhodnými“ nabídkami se často skrývají podvodníci, kteří se snaží vylákat vaše finanční prostředky – a už vám je nikdy nevrátí.

Jak poznat podvodnou investici

- **Příliš slibné výnosy** – kdo slibuje rychlé a jisté zisky, lže.
- **Tlak na rychlé rozhodnutí** – „Je to jen pro omezený počet lidí.“
- **Nulové riziko:** „Nemůžete nic ztratit.“
- **Požadují vzdálený přístup do vašeho počítače nebo instalaci programů** (např. AnyDesk nebo TeamViewer).
- **Neexistující licence nebo netransparentní firmy.**
- **Falešné příběhy i deepfake videa**, zneužívající důvěryhodnost veřejně známých osobností.
- Požadavek na vzdálený přístup (např. přes AnyDesk nebo TeamViewer).
- Složitý jazyk, který má zakrýt nejasnosti.

Proč je to nebezpečné?

- Hrozí, že **přijdete o všechny finanční prostředky, které vložíte** – a někdy i o víc, pokud si na „investici“ půjčíte.
- Jakmile peníze odešlete, většinou je už nikdy nevidíte.
- Někteří podvodníci se vás snaží přimět, abyste jim umožnili vzdálený přístup k počítači. Tak mohou **ukrást vaše osobní údaje, hesla i přístup do internetového bankovníctví.**

Příklad ze života:

Panu Jiřímu volal „poradce“ z investiční společnosti, který tvrdil, že mu pomůže vložit malé peníze do „bezpečných akcií“. Aby mu mohl „nastavit účet“, požádal pana Jiřího, aby si stáhl program pro vzdálenou pomoc s počítačem.

Podvodník mu pak „ukázal“ fiktivní graf, na kterém jeho vklad rychle rostl. Po několika dnech „výdělků“ mu nabídl, že může investovat více, aby vydělal ještě víc.

Když pan Jiří chtěl peníze vybrat, zjistil, že na účtu nic není – a navíc mu z banky zmizely finanční prostředky, protože podvodník při vzdáleném přístupu získal přihlašovací údaje do jeho internetového bankovníctví.



Jak se bránit?

- Nespěchejte – podvodníci často tlačí na rychlé rozhodnutí. **Dejte si čas vše prověřit.**
- **Ověřte si společnost** – hledejte ji v oficiálním seznamu regulovaných subjektů (např. ČNB).
- Nevěřte „zaručeným“ výdělkům – **žádná investice není bez rizika.**
- **Neposkytujte vzdálený přístup k počítači** – tím byste dali cizím lidem kontrolu nad svými účty.
- Nikomu **neposílejte své přihlašovací údaje** k bankovnímu účtu – ani „poradcům“ nebo lidem, kteří tvrdí, že jsou z banky.
- **Prověřujte e-maily a weby** – falešné investiční stránky často vypadají profesionálně, ale mají drobné chyby v adrese nebo textu.
- **Nenechte se zlákat známou tváří** – podvodníci zneužívají jména fotografie i deep fake videa celebrit a politiků bez jejich vědomí.
- **Mluvte o nabídce s někým důvěryhodným** – druhý názor vám může pomoci odhalit past.

Pamatujte! Čím větší sliby, tím větší podezření. Vydělávat peníze není jednoduché. Když vám někdo volá a říká, že zbohatnete – **raději zavěste.**

Jak se chránit

praktické rady pro bezpečný pohyb na internetu



Internet může být užitečný pomocník, ale i nebezpečné místo, pokud nevíte, na co si dát pozor. Dobrá zpráva je, že základní bezpečnost na internetu zvládne každý – i bez technických znalostí.

Tady je několik jednoduchých zásad, které vám pomohou zůstat v bezpečí:



Zásady bezpečného chování na internetu

- Nikdy nikomu neprozrazujte svá hesla. Ani banka nebo policie je po vás nikdy nebude chtít.
- Neklikejte na podezřelé odkazy v e-mailech nebo SMS.
- Neinstalujte do telefonu nebo počítače aplikace a programy od neznámých lidí.
- Pokud se vám něco nezdá, raději se poraďte s rodinou nebo nám napište.
- Neodesílejte kopie občanského průkazu ani jiných dokladů přes internet.
- Používejte silná hesla (např. kombinace velkých a malých písmen, čísel a symbolů).
- Pravidelně kontrolujte svůj bankovní účet.

Doporučené bezpečnostní nástroje a nastavení pro lidi se zrakovým postižením:

- Čtečka obrazovky s upozorněním na odkazy: Doporučujeme například NVDA (zdarma), VoiceOver (pro iOS) a TalkBack (pro Android).
- Dvoufázové ověření (2FA): Umožněte si přihlašování pomocí SMS nebo bezpečnostní aplikace (např. Google Authenticator).
- Bezpečnostní antiviry s přístupností: Například ESET nebo Avast mají jednoduché prostředí a podporují čtečky obrazovky.
- Funkce čtení QR kódů a ověřování odkazů: Například aplikace Be My Eyes nebo Seeing AI vám pomohou zkontrolovat neznámé weby nebo čtečky QR kódů.

!! Co dělat, když vás podvedou

1. Okamžitě přerušete kontakt s podvodníkem

- Neodpovídejte na zprávy, e-maily ani telefonáty.
- Zablokujte kontakt na sociálních sítích, v e-mailu i telefonu.

2. Zabezpečte své účty

- Změňte hesla ke všem důležitým účtům (e-mail, bankovníctví, sociální sítě).
- Aktivujte dvoufázové ověření, pokud je k dispozici.

3. Kontaktujte banku

- Pokud jste poslali peníze, ihned zavolejte své bance.
- Požádejte o zastavení platby nebo reklamaci transakce.
- Nechte si zablokovat platební kartu, pokud jste údaje k ní zadali podvodníkovi.
- Banka vám může vystavit novou kartu a nastavit vyšší zabezpečení účtu.

4. Uložte důkazy

- Udělejte snímky obrazovky (screenshoty) zpráv, e-mailů, webových stránek a platebních potvrzení.
- Tyto informace si uložte pro policii nebo jiné instituce.

5. Podejte oznámení

- Obratě se na Policii ČR (lze osobně nebo online přes podání vysvětlení).
- Podvod můžete nahlásit také na webu www.bezpecnyinternet.cz nebo www.csirt.cz.

6. Nahlaste podvodnou stránku či profil

- Na Facebooku, Instagramu či jiných sítích použijte funkci „Nahlásit“.
- Tím pomůžete chránit další lidi.

7. Poradte se s odborníky

- Můžete kontaktovat poradnu [Sdružení obrany spotřebitelů Moravy a Slezska](#) – pomůžeme vám s dalším postupem.

Potřebujete poradit? Jsme tu pro vás

Sdružení obrany spotřebitelů Moravy a Slezska, z. s.

Neváhejte a využijte bezplatného spotřebitelského poradenství. Zavolejte nám, napište nebo nás osobně navštivte.

kontakt:

e-mail: **poradna@sos-msk.cz**

telefon: **608 722 582, 607 398 511** (pracovní dny 9:00 - 16:00)

www.sos-msk.cz

Abychom vám byli blíží, poskytují pracovníci SOS MaS, z.s. osobní poradenství nejen v poradně v Ostravě, ale také ve výjezdních poradnách na území Moravskoslezského, Olomouckého a Zlínského kraje.

Otvírací dobu jednotlivých poraden najdete na stránce <https://www.sos-msk.cz/pro-spotrebitele-nove/poradny/>



Sdružení obrany spotřebitelů
Moravy a Slezska

Publikace je financována z rozpočtu Moravskoslezského kraje - Programu na podporu komunitní práce a neinvestičních aktivit z oblasti prevence kriminality na rok 2025

