Zveřejněno 14. 11. 2026

Nejčastější typy finančních podvodů a jak jim čelit

Podvodné e-maily, podvržená telefonní čísla, SMS zprávy i zprávy přes komunikátory (WhatsApp aj.) jsou v dnešním online prostoru na denním pořádku. Podvodníci dokáží vytvořit velký tlak, pocit naléhavosti a věrohodnou iluzi ohrožení, proti kterým běžná obezřetnost jednotlivce nemusí stačit a v praxi velmi často selhává.

S jakými podvody se můžete setkat?

Podvodníci neustále mění své scénáře, ale způsob, jakým vás kontaktují, a jejich hlavní cíl zůstávají stejné: vyvolat pocit naléhavosti, vyřadit vaše racionální uvažování (tzv. amygdalový únos) a donutit vás převést peníze nebo předat přístupové údaje.

Podvody nejčastěji probíhají těmito kanály:

Podvodné telefonáty (VISHING)

- **Jak to probíhá:** Volající se vydává za bankéře, bezpečnostního technika ČNB nebo policistu (často tyto role kombinuje). Díky tzv. spoofingu (technice podvržení telefonního čísla či identity odesílatele) se vám na displeji telefonu může zobrazit skutečné číslo infolinky banky či Policie ČR.
- **Typická záminka:** Varují vás, že váš účet je v ohrožení nebo že si na vás někdo bere úvěr. Přesvědčují vás, abyste peníze „zachránili“ okamžitým převodem na falešný záchranný/bezpečnostní účet, vybrali je do kryptoměnového bankomatu, nebo si do počítače nainstalovali aplikaci pro vzdálenou správu (např. AnyDesk, TeamViewer).
- **Pamatujte:** Žádná banka ani ČNB neprovozuje dočasné záchranné účty a Policie ČR nikdy neřeší přesuny peněz po telefonu!

Podvodné e-maily a podvržené stránky (PHISHING)

- **Jak to probíhá:** Dorazí vám e-mail, který vypadá jako oficiální zpráva od banky, úřadu, dodavatele energií nebo skautISu. Další častou formou je podvržená stránka ve vyhledávači – do vyhledávače (Google, Seznam) zadáte např. „Fio banka“ nebo „skautIS“, kliknete na první odkaz a ocitnete se na podvodném webu s mírně pozměněnou adresou, který vypadá k nerozeznání od toho pravého.
- **Typická záminka:** Výzva k úhradě podvržené faktury se změněným číslem účtu, nečekaný nedoplatek, nebo nutnost „přihlásit se“ na podvržené stránce banky/skautISu, čímž útočníkům předáte své přihlašovací údaje. Útočník je obratem zadá do skutečné banky a obratem vám pošle podvodnou SMS s výzvou, abyste mu přeposlali skutečný potvrzovací kód, který vám právě přišel.

- **Pamatujte:** Vždy si kontrolujte e-mailovou adresu odesílatele a přesnou URL adresu v prohlížeči. Do internetového bankovnictví a skautISu nechoďte přes vyhledávače ani odkazy v e-mailech, ale používejte přímou adresu uloženou v Záložkách / Oblíbených položkách.

Podvodné SMS zprávy (SMISHING) a zprávy v aplikacích (WhatsApp)

- **Jak to probíhá:** Zpráva na mobil s odkazem, která se tváří jako oznámení od doručovací služby (Česká pošta, Zásilkovna), banky či státního portálu.
- **Typická záminka:** Nezaplacené clo/poštovné za balíček, zablokovaný účet, nebo zpráva typu „Ahoj mami/tati, mám nové číslo a potřebuji narychlo zaplatit účet“.
- **Pamatujte:** Banka ani přepravci v SMS neposílají odkazy pro zadávání přihlašovacích údajů k účtu nebo kartě

Bazarové podvody (při nákupu vybavení)

- **Jak to probíhá:** Středisko nebo oddíl shání levnější vybavení na tábor či klubovnu (stany, vařiče, lodě, nábytek) přes inzertní portály (Bazoš, Sbazar) nebo Facebook Marketplace.
- **Typická záminka:** Podvodník nabízí kvalitní vybavení za velmi výhodnou cenu. Pod záminkou velkého zájmu požaduje platbu předem (či zálohu) na účet, případně pošle odkaz na falešnou platební bránu či přepravní službu pro „bezpečnou garanci platby“, kde z vás vymámí údaje z platební karty nebo přihlášení do banky. Zboží pak samozřejmě nikdy nedorazí.
- **Pamatujte:** Při nakupování od neznámých soukromých osob na internetu neposílejte velké částky předem bez ověření. Pro platby nikdy nevyužívejte odkazy na platební brány poslané prodávajícím v chatu nebo SMS.

Proč je tak snadné naletět?

Při sofistikovaném podvodu dochází k silnému psychologickému tlaku a manipulaci. Útočníci si vytvářejí vztah pomocí otázek, na které odpovídáte souhlasně, budují autoritu a často vás izolují od okolí (např. varováním, že o situaci nesmíte s nikým mluvit kvůli vyšetřování). V takovém stresu lidský mozek přirozeně jedná v panice a podléhá příkazům.

Nejlepší obranou proto není spoléhat se na chladnou hlavu jednoho člověka, ale **mít nastavený vnitřní kontrolní systém**. Jak správně nastavit vnitřní pravidla, dvoustupňovou autorizaci a limity na účtech, popisujeme v článku Kontrolní mechanismy a prevence podvodů.

Co dělat, pokud k podvodu dochází nebo již došlo?

Pokud máte podezření, že jste se stali obětí podvodu, **rozhodují minuty**:

1. **Ihned kontaktujte banku:** Zavolejte na oficiální infolinku banky (případně využijte tlačítko přímého volání v aplikaci mobilního bankovnictví). Požádejte o zablokování karet, zablokování přístupu do internetového bankovnictví a o pokus o stopnutí odchozích (zejména okamžitých) plateb.

   Tip: Uložte si oficiální číslo infolinky do telefonního seznamu v mobilu hned teď, ať ho v krizi nemusíte narychlo hledat!

2. **Informujte vedení:** Bezodkladně informujte druhou osobu s dispozičním právem / vedoucího střediska.

3. **Nahlaste událost na Policii ČR:** Podejte trestní oznámení na nejbližší služebně PČR. Připravte si výpisy z účtu, telefonní čísla, čísla účtů útočníků, e-maily/zprávy a časovou osu události.

4. **Informujte střediskovou radu, revizní komisi a ústředí:** Otevřenost je klíčová k tomu, aby se z události poučili i ostatní členové střediska a mohla se přijmout další preventivní opatření. Zároveň o útoku dejte vědět ústředí (kancelar@skaut.cz), aby mohlo včas varovat další organizační jednotky.