# Čelíme rekordnímu nárůstu kyberpodvodů

**12.5.2026 - Zuzana Pidrmanová | Policie ČR**

**Útočníci míří hlavně na ženy a využívají strach, časový tlak a manipulaci.**

Kyberkriminalita v České republice prudce roste a stává se jednou z nejzávažnějších bezpečnostních hrozeb současnosti. Online podvody tvoří již **tři čtvrtiny veškeré kyberkriminality**, přičemž jejich skutečný rozsah je ještě vyšší, protože řada obětí případy nehlásí. I podle závěrů Global Fraud Summitu OSN jde celosvětově o nejrychleji rostoucí formu kriminality. Podvody jsou často propojené s další trestnou činností, například vydíráním nebo legalizací výnosů z trestné činnosti. Účinný boj proti této kriminalitě je možný pouze prostřednictvím mezinárodní spolupráce, sdílení informací a posilování prevence napříč veřejným i soukromým sektorem. *„Nejde už jen o jednotlivé pachatele, ale o **organizovaný mezinárodní zločin**, který funguje jako propracovaný byznys,“* uvedl **plk. Vladimír Lukášek,** ředitel Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR. **Enormní nárůst** jsme zaznamenali v průběhu měsíce března letošního roku, a to **o více než 37 %** v meziročním srovnání stejného období.

Nejrychleji rostoucí formou útoků jsou telefonáty, při nichž se pachatelé vydávají za pracovníky bank nebo Policie ČR. *„Oběťmi těchto podvodů jsou v 80% případů ženy. Falešní bankéři a falešní policisté využívají strach, práci s emocemi a časový tlak. Průměrná škoda u telefonních podvodů dosahuje **744 000 Kč**, u romantických podvodů **513 000 Kč**. V některých případech lidé přijdou o **miliony korun**,“* doplňuje **pplk. Ondřej Kapr** z Úřadu služby kriminální policie a vyšetřování.

**Útočníci oběť**:

- **vystraší** („váš účet je napaden“, „někdo si na vás bere úvěr“),
- **izolují** („nikomu nic neříkejte, jinak budete stíhána“),
- **manipulují** k převodu peněz na údajně „bezpečný účet“,
- **nutí** instalovat aplikace pro vzdálený přístup nebo sdílet obrazovku,
- **přimějí** k výběru hotovosti a předání obnosu kurýrovi či vkladu do vkladomatu na virtuální měnu.

„Hovory trvají klidně i 12 hodin, střídá se v nich několik lidí, v přestávkách hraje hudba nebo volají za sebou z několika českých telefonních čísel. Přitom celou dobu hovoru poškozeného drží ve strachu, že když neuposlechne jejich instrukce a jimi nabízené řešení, přijdou o své veškeré peníze nebo se sami dopustí trestného činu,“ dodává **pplk. Ondřej Kapr**. V tomto kontextu žádný bezpečný účet neexistuje stejně jako výhodný investiční produkt slibující nestandardně vysoké zúročení v krátké době.

Stejně tak jsou děsivé romantické podvody, které patří k nejzávažnějším formám kyberkriminality vzhledem ke značným citovým vazbám, které jsou součástí celého podvodného scénáře. Až **87 % obětí tvoří ženy**, jejichž průměrný rok narození je **1967**.

**Pachatelé vědomě útočí na emoce**:

- **budují dlouhodobý vztah**,
- **izolují oběť**, aby se s láskou nikomu nesvěřovala, protože by jí okolí záviděl,
- **vyznávají lásku** během několika dní,
- **žádají peníze** na „cestu“ za obětmi, neodkladnou „operaci“ vedoucí k uzdravení, „kauci“ na vyvázání se ze služby, aby mohl začít nový vysněný společný život,

- **často se vydávají za vdovce** pečující o dítě, aby citový nátlak umocnili,
- **používají falešné identity včetně fotografií** (lékař OSN, voják, pilot, inženýr),
- **vytvářejí falešné weby bank a přepravních společností**,
- **posílají fiktivní balíky s movitým majetkem**, které nikdy nedorazí a k jejichž doručení požadují zaplacení celních poplatků.

Podvodníci navazují důvěryhodný vztah i několik měsíců. Prvotní kontakt vyhledají přes seznamovací aplikace či jiné sociální sítě, kde vystupují pod falešnou identitou. Rychle budují důvěru, vyznávají lásku a žádají o diskrétnost. Následně vyvolají v oběti strach o jejich život formou nebezpečné válečné operace či mise, vážného lékařského zákroku apod. Často se na několik dní zcela odmlčí. Pakliže je oběť citově podchycena a na situaci emotivně reaguje, začnou po ní požadovat různé finanční výpůjčky či poplatky s příslibem, že vše vrátí. Oběť může být manipulována i k převodům peněz přes vlastní účet na jiné účty, což pachatelé využívají k legalizaci výnosů z trestné činnosti.

*„Z dostupných statistik vyplývá, že nejvíce ohrožení jsou lidé ve středním věku, tedy ti, kteří se starají o děti i rodiče a často mají pocit, že **„jim se to stát nemůže“**. Jenže pachatelé neútočí racionalitou. Pracují zásadně s emocí, kterou je strach, takže všichni mohou být zaskočeni nečekaným telefonátem nebo zprávou, která působí naléhavě a důvěryhodně. Proto žádáme veřejnost o pomoc se šířením prevence. Sdílení informací může ochránit vaše peníze i peníze vašich blízkých,“* vysvětluje **plk. Zuzana Pidrmanová**, vedoucí odboru prevence Policejního prezidia ČR.
Stačí si pamatovat několik jednoduchých zásad: **nikdy neposílat peníze na údajný bezpečný účet**, vědět, že **policie ani banka nevyžaduje převody peněz po telefonu**. Věděli jste, že podezřelá čísla falešných bankéřů či falešných policistů můžete telefonním operátorům hlásit na čísle **7726?** Nenechte se vmanipulovat do nekomfortní situace, o to pachatelům jde. Vždy si vezměte čas na rozmyšlenou tím, že zavěsíte a necháte odejít ten strach, který ve vás pachatel vyvolal.

Připravili jsme **jednoduché pravidlo 3Z**, které je vhodné se naučit, aby nám vyvstalo na mysli pokaždé, když zvedneme telefon s naléhavou informací o napadení účtu.

1. **ZASTAV** – nenechte se vtáhnout do paniky.
2. **ZAVĚS** – policie ani banky nikdy nepožadují převody peněz.
3. **ZKONTROLUJ** – ověřte si situaci přímo u své banky.

Pamatujme, že součástí útoků falešných bankéřů či policistů může být i odkaz nebo SMS s falešnou přihlašovací stránkou banky. Vypadá identicky jako ta skutečná, má pouze jinou URL adresu. V takových případech mohou pomoci k ochraně každého jednotlivce i technologická řešení, která hrozbu zachytí dříve, než se uživatel vůbec dostane na stránku. To může být rozhodující moment pro každého, kdo pod vyvolaným strachem z neočekávaného telefonátu v danou chvíli a ve stresu jedná impulzivně. *„**Kyberbezpečnost není jen o softwaru. Je to kombinace tří věcí: informovanosti, zdravého úsudku a dobré technologie**. To vše pečlivě nastavené může kyperpodvodníkům znesnadnit jejich úspěšnost,“* uzavírá **Ondřej Novotný,** specialista kyberbezpečnosti ESET.

Praha 12. května 2026
plk. Zuzana Pidrmanová

https://policie.gov.cz/clanek/celime-rekordnimu-narustu-kyberpodvodu.aspx