

Podvodníci nelení

Internetové podvody nejen přes Whatsapp stále na vzestupu. Za poslední čtyři červencové dny jsme na Rychnovsku zaevidovali desítku podvodů za téměř 2 miliony korun.

Policisté se problematikou podvodů v online prostředí zabývají již řadu let. S rozvojem digitálních technologií a komunikačních platforem se však mění i způsoby, jakými se pachatelé snaží oklamat veřejnost. Za prvních sedm měsíců letošního roku evidujeme na Rychnovsku již více než osm desítek trestných činů spáchaných v online prostředí, jejichž celková škoda dosahuje téměř 13 milionů korun. V loňském roce jsme přitom přijali necelou stovku těchto případů se škodou přesahující více než 22 milionů korun. Kromě těchto trestných činů zaznamenáváme další desítky oznámení na podvodná jednání na internetu, které jsou kvalifikovány jako přestupky.

V posledních dnech a týdnech evidujeme na Rychnovsku výrazný nárůst případů, kdy podvodníci s oběťmi komunikují prostřednictvím aplikace WhatsApp. Tito pachatelé využívají důvěryhodně působící zprávy, často se vydávají za rodinné příslušníky nebo známé, a snaží se vylákat finanční prostředky či jiné citlivé údaje. Podvodníci zpravidla nejdříve rozesílají poškozeným SMS zprávy, ve kterých je informují, že mají mít údajně rozbitý telefon či používají nové telefonní číslo. Díky oslovení „Ahoj mami/ tati...“ si tak poškození vydedukují, že se jedná o jejich děti, nová čísla si ukládají a poté společně písemně komunikují. Ti následně požadují rychlé zaslání finančních prostředků. V domnění, že poškození komunikují se svými potomky, vyhoví jejich požadavkům a bez ověření požadované platby provádí.

Pokud vám přijde tato zpráva: „Ahoj mami/tati, změnil/a jsem číslo/mám rozbitý telefon,...“ ZPOZORNĚTE!!!

Podvodníkům naletěla i 69letá žena z Rychnovska, jež zareagovala na zprávu od neznámé osoby z neznámého telefonního čísla, která se vydávala za její dceru. Té měl spadnout telefon do vody a po „své matce“ požadovala uhrazení 55.000 korun. Ty žena poslala na zaslání čísla bankovního účtu, bohužel bez předchozího telefonního ověření u skutečné dcery. Dceři zavolala až druhý den s tím, že peníze odeslala, ta ale o ničem nevěděla. Další podvodník oslovil zprávou také 79letého muže, vydával se za jeho dceru, která má rozbitý telefon a nutně potřebuje uhradit nějaké faktury. Přišel tak o více než 80.000 korun. O více než 40.000 korun přišla i 74letá žena, ve které podvodník vyvolal dojem, že si píše se svým synem. Další „dcera“ připravila 70letou ženu o 50.000 korun a tak bychom mohli pokračovat.

V posledních dnech jsme zaznamenali i případ, kdy se neznámý pachatel oznamovateli „naboural“ do aplikace Whatsapp a jejím prostřednictvím rozeslal svým známým zprávy s žádostí o půjčku ve výši 30.000 korun. Někteří z nich, bez předchozího ověření a v domnění, že komunikují se svým kamarádem, peníze na účet zaslali. Oznamovatel ale o žádné finanční prostředky ve skutečnosti nežádal.

Podvodníci kromě nových typů podvodů stále dokola využívají i osvědčené legendy, které opakují s drobnými obměnami. Bohužel se stále najdou lidé, kteří pod tlakem podlehnou, důvěřují neznámým osobám a nechají se zmanipulovat. Často tak přicházejí i o své celoživotní úspory. Jak vypadá autentická komunikace podvodníka s potenciální obětí, jaké metody podvodníci používají a jaký vyvíjejí nátlak na volaného, si můžete poslechnout zde: <https://t.co/SlsvswBjaD>.

Mluvte o této problematice se svými rodiči či příbuznými, známými i sousedy. Upozorněte je, že existují lidé, kteří mohou zneužít vaší identitu a obelstít je s cílem získat pro sebe finanční prospěch.

I přesto, že je objasňování této trestné činnosti s ohledem na nadnárodní přesah a důmyslnost pachatelů velice náročné, podařilo se vloni na jaře **na Ukrajině rozkrýt organizovanou skupinu**, která má na svědomí spáchání téměř 500 skutků se škodou více než 100 miliónů korun.

Nejčastější typy internetových podvodů:

- **Spoofing (phishing, vishing, smishing)**

Jedná se o podvodné e-maily, telefonáty nebo SMS, které se tváří jako komunikace od banky, úřadu nebo jiné důvěryhodné instituce. Cílem je získat přihlašovací údaje nebo PIN kód k internetovému bankovníctví.

Znaky spoofingu:

- Nátlak na uživatele, snaha vyděsit a nedat čas na rozmyšlenou. Výzva k okamžité reakci, jinak se „něco“ stane, nejčastěji hrozba ztráty finančních prostředků.
- Vyžadování citlivých údajů po telefonu nebo žádost o poskytnutí přístupu do zařízení.
- Velké množství kontrolních otázek osobního charakteru nad rámec data narození, rodného čísla apod.
- Neodpovídající e-mailová adresa, telefon či webová adresa.

Policie radí a doporučuje:

- Phishing: buďte obezřetní a používejte selský rozum, neklikejte na odkazy v nevyžádané poště nebo sociální síti, např. Whatsapp apod., neotvírejte přílohy nevyžádaných e-mailů, nikomu nesdělujte citlivé údaje.
- Vishing: nedůvěřujte neověřeným a podezřelým telefonním číslům, neposkytujte volajícímu citlivé informace, používejte dvoufaktorovou autentizaci (ověření).
- Smishing: u každé zprávy posuzujte obsah (kdo a co po mě chce), SMS s pravopisnými chybami naznačuje strojový nebo automatický překlad, neklikejte na odkazy obsažené v SMS zprávách - jejich pravost si můžete ověřit u jejich odesílatele.

- **Falešné investiční nabídky**

Nabídky rychlého zhodnocení peněz, často v kryptoměnách. Pachatelé slibují vysoké výnosy, ale ve skutečnosti jde o podvod.

Znaky falešné investiční nabídky:

- Poškozený sám reaguje na nabídku k velmi výhodné investici, která je sama o sobě podezřelá, např. nereálné zhodnocení investovaných finančních prostředků.
- Podvodník kontaktuje zájemce o investování či osobu, která již v minulosti takto investovala.
- Nátlak, aby si poškozený naistaloval program pro vzdálený přístup, např. AnyDesk.
- Časté sjednání úvěrů pachatele v účtu poškozeného.

Policie radí a doporučuje:

- Nic nesjednávejte po telefonu.
- Nikdy neinstalujte doporučené aplikace a programy umožňující vzdálený přístup k vašemu PC či telefonu.

- **Reverzní inzertní podvody na bazarech a inzertních portálech**

Falešní kupující nebo prodávající požadují platbu předem nebo zasílají odkazy na falešné platební brány. Často bývá zaslán i odkaz s adresou některé přepravní společnosti zajišťující dopravu zboží.

Policie radí a doporučuje:

- Všímejte si formátu webových stránek, pokud něco neodpovídá, může se jednat o podvod.
- Všímejte si koncovek webových stránek, koncovka neznámé země apod.
- Falešné stránky se mohou lišit v podrobnostech lišit od originálu, např.: navíc tečka, pomlčka apod.
- Nikdy neklikejte na zaslané odkazy a nikam nevyplňujte přístupové údaje ke svému účtu či platební kartě.
- Kupujícímu vždy poskytněte jen číslo vašeho účtu.

- **Romantické podvody**

Pachatelé navazují vztah přes sociální sítě a po čase žádají o finanční pomoc. Mohou se tvářit jako úspěšní manažeři, právníci, lékaři, sportovci nebo dokonce astronauti, např. podvody typu „americký voják“.

Policie radí a doporučuje:

- V případě, že jste dotyčného, se kterým komunikujete on-line, do současné doby neviděli, tak si představte, že ten s kým komunikujete, může být někdo úplně jiný, než za koho se vydává.
- Důrazně varujeme, abyste komukoli, koho osobně neznáte, neposílali jakékoli finanční prostředky!

Co platí v obecné rovině a jak se chránit?

- **Nikdy nesdělujte PIN, hesla ani přístupové údaje** – banka je po vás nikdy nebude požadovat telefonicky ani e-mailem.
- **Ověřujte si změny čísel** – zavolejte zpět nebo se zeptejte na něco, co ví jen daná osoba.
- **Ověřujte si informace z více zdrojů** – zejména pokud jde o investice nebo výhodné nabídky.
- **Neposílejte peníze neznámým osobám** – ani pokud se vydávají za známé nebo autority.
- **Používejte dvoufázové ověření** – zejména u bankovníctví a e-mailu.
- **Buďte obezřetní při online komunikaci** – zvláště pokud druhá strana žádá o peníze nebo přístup k zařízení.

Policie ČR se aktivně zapojuje do **preventivních kampaní**, které mají za cíl zvýšit povědomí veřejnosti o rizicích v online prostředí a naučit občany, jak se účinně bránit. Tyto aktivity zahrnují přednášky, tvorbu informačních materiálů, spolupráci se školami a veřejnými institucemi. Jen na Rychnovsku proběhlo v letošním roce více než dvacet přednášek na téma Digitální bezpečnost, a to jak na základních a středních školách, tak i pro veřejnost.

Policisté budou i nadále věnovat zvýšenou pozornost kybernetické kriminalitě a pokračovat v preventivních aktivitách zaměřených na ochranu občanů před podvodným jednáním v online prostředí.

To nejdůležitější je ale na vás!

4. srpna 2025

por. Mgr. Andrea Muzikantová

por. PhDr. Jaroslav Matoušek, MBA, LL.M.