... AKTUÁLNÍ PŘÍPADY INTERNETOVÝCH PODVODŮ V KRNOVĚ

• Dvaapadesátiletý muž z Krnova oznámil, že v odpoledních hodinách 6. února 2023 byl z přesně neustanoveného místa telefonicky kontaktován na jeho mobilní telefon ze strany mu neznámé osoby s nabídkou pomoci při úspěšném obchodování na burze, přičemž mu následně po dohodě zaslal na jeho e-mail jistý internetový odkaz s doporučením, aby tento otevřel a vyplnil požadující informace. Výše uvedený muž se kromě zadání údajů ke své osobě přihlásil přes tak zvaný George klíč i do svého internetového bankovnictví a měl sledovat připisování finančních prostředků. Místo toho však během velmi krátké chvíle došlo v několika případech k odčerpání finančních prostředků z jeho účtu na jiné mu neznámé bankovní účty a těmito neoprávněnými transakcemi neznámého pachatele mu byla odcizena finanční hotovost ve výši 300 tisíc korun.

• V dopoledních hodinách dne 6. února letošního roku byl několikráte telefonicky kontaktován neznámou osobou i 80letý muž z Krnova s tím, že by mu ráda převedla nějaké finanční prostředky získané předchozím investováním do kryptoměn a požádala jej o přihlášení se nejen do e-mailové schránky ale rovněž i do jeho internetového bankovnictví, což důvěřivý muž seniorského věku učinil. Následně sledoval, jak mu na jeho spořicí účet přišla finanční částka ve výši 50 tisíc korun, která však po chvíli byla opět odebrána a z tohoto jeho účtu byly několika rychlými transakcemi neoprávněně odčerpány na jiné účty i jeho finance ve výši 200 tisíc korun.

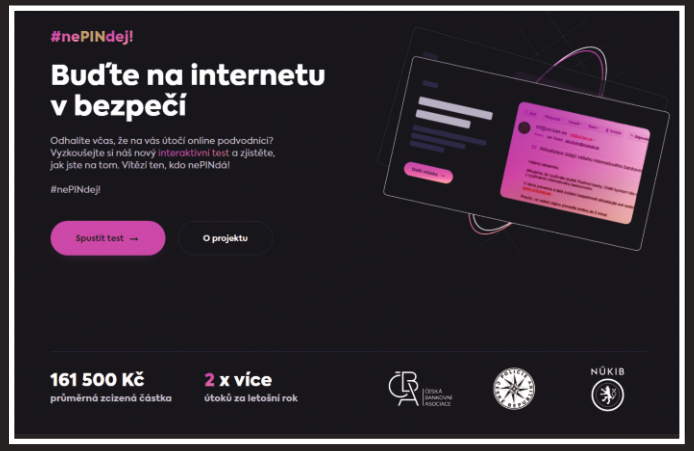
• V průběhu dne 6. února tohoto roku byla v místě bydliště telefonicky kontaktována 32letá žena z Krnova ze strany jí neznámého muže, který se představil jako pracovník společnosti Microsoft a nabídl jí vyčištění jejího notebooku s následnou autorizovanou aktualizací, s čímž výše uvedená žena souhlasila. Na základě telefonicky dávaných pokynů si do svého příručního počítače nainstalovala aplikaci Teamviewer a do svého mobilního telefonu aplikaci Anydesk, následně zadala své přístupové údaje ke svému internetovému bankovnictví, přičemž bez jejího vědomí došlo k neoprávněné expresní platbě v euro měně a na blíže neupřesněný zahraniční účet byly převedeny její finanční prostředky v celkové výši téměř 52 tisíc korun.

ZÁKLADNÍ DESATERO BEZPEČNOSTI

- **Starejte se o bezpečí svého počítače**
- **Zabezpečte si mobilní telefon**
- **Ověřujte si původ aplikací**
- **Chraňte své přihlašovací údaje**
- **Svůj PIN chraňte jako oko v hlavě**
- **Mějte bezpečné heslo**
- **Pozor na neznámé přílohy**
- **Nakupujte jen u prověřených on-line prodejců**
- **Čtěte upozornění banky**
- **Informujte banku**

Cílem kyberpodvodníků jsme **všichni, od teenagerů po seniory.**
Vyzkoušejte si proto interaktivní vzdělávací kybertest,
který upozorňuje na aktuální kyberpodvody a současně vás
naučí, jak je rozpoznat a jak jim nenaletět:

www.kybertest.cz



Městská policie Krnov - prevence kriminality

V KRNOVĚ

PREVENCE SE VYPLATÍ

NA INTERNETU BEZPEČNĚ

Statistická data a zejména špatné zkušenosti mnohých občanů nám ukazují, že množství protiprávních činů v kyberprostoru stále narůstá a je tedy větší pravděpodobnost, že se s nějakou hrozbou setká každý. Je proto na nás, jak budeme připraveni a jestli dokážeme včas rozpoznat, že se jedná o podvodné jednání a nenecháme se **nachytat, obelhat, okrást**.

**Kyberpodvodníci jsou dobře organizovaní,
velmi často s mezinárodním přesahem,
působí profesionálně
a jednají naprosto bez zábran.**

JAK POZNAT PODVODNÉ JEDNÁNÍ?

PODVODNÉ TELEFONÁTY

V poslední době se rozmáhá volání falešných bankovních úředníků, investičních poradců, pracovníků technické podpory a následně třeba i nepravých policistů. Tito podvodníci se snaží vystrašit informací o ohrožení bankovního účtu a manipulovat volaného k provádění finančních transakcí, jako jsou převody peněz, výběry hotovosti, platby pomocí QR kódů, apod. Vystrašená oběť dostává přesné instrukce ke stahování aplikací, klikání na odkazy v SMS, e-mailech nebo na falešných a důvěryhodně vypadajících webových stránkách, k zadávání údajů z platebních karet nebo bankovní identity. Takové transakce nemůže banka zablokovat, ani prostředky vrátit.

Preventivní rady a doporučení:

Pamatujte, že **banky** případné ohrožení účtů svých klientů **řeší samy**, nikdy ne prostřednictvím urgentních telefonátů nebo dokonce SMS zpráv. Potřebné citlivé údaje mají k dispozici.

- **Nikdy se nenechávejte přesměrovat do internetového bankovnictví prostřednictvím klikání na odkazy v e-mailech nebo SMS zprávách**.
- Buďte na pozoru, jestliže je e-mail psán **špatnou gramatikou**.
- Nesdělujte nikomu **údaje ke své platební kartě**.

PODVODNÉ E-SHOPY

Při online nákupech můžete velmi snadno narazit na falešný internetový obchod, proto zejména při prvním nákupu ověřujte jeho věrohodnost. Vyhnete se tak pořízení nekvalitního nebo i nevyžádaného zboží, nebo že vaše objednávka vůbec nedorazí.
Podvodné e-shopy také například stahují z vašeho účtu vyšší částky nebo dlouhodobě drobné obnosy.

Preventivní rady a doporučení:

- Ověřte si **věrohodnost prodejce** v seznamu rizikových e-shopů na stránkách České obchodní inspekce.
- Cenové nabídky porovnejte u více prodejců a **vyhněte se podezřele nízkým cenám.**
- Buďte obezřetní při online platbách, **chraňte si údaje k platební kartě a pro přihlášení do internetového bankovnictví**.
- Pokud nakupujete v e-shopu poprvé, nechte si zboží zaslat na dobírku.
- Až k vám balíček dorazí, co nejdříve **zkontrolujte jeho obsah** pro případnou reklamaci.
- **Pokud obsah neodpovídá vaší objednávce, kontaktujte Policii ČR, jednejte co nejrychleji.**

INVESTIČNÍ PODVODY

Vše může začít zdánlivě výhodnou nabídkou v podobě internetové reklamy. Podvodníci nabízejí pomoc s nákupem kryptoměn, pochopitelně s příslibem vysokého výnosu. Oběť je utvrzována o důvěryhodnosti transakce například přístupem na falešné portfolio či do falešných virtuálních peněženek na profesionálně působících webových stránkách. Pro zvýšení důvěryhodnosti jsou někdy vyžadovány pravidelné vklady s tím, že výnosy budou vyplaceny až po delším časovém úseku. Oběť také bývá vyzývána k poskytnutí osobních a bankovních údajů, nebo ke vzdálenému přístupu k svému počítači. Krádeži už pak nic nestojí v cestě.

Preventivní rady a doporučení:

- Nevěřte lákavým reklamám o pohádkových výnosech.
- Ke každé investici do kryptoměny přistupujte jako k riziku.
- Nikdy neinvestujte všechny své úspory.
- Pokud chcete investovat, obraťte se přímo na bankéře.
- Pokud vás osloví bankér či investiční poradce první, pečlivě si ověřte jeho věrohodnost.
- Nikdy nikomu neposkytujte vzdálený přístup k vašemu počítači ani informace o vašem internetovém bankovnictví.

INZERTNÍ PODVODY

Podvodníci se objevují i mezi kupujícími, tedy reagují jako zájemci o inzerované zboží. Následně sdělují, že platbu zaslali kurýrní službou, která zboží převezme. Prodávající obdrží v SMS odkaz, který je údajně nutno pro vyzvednutí peněz vyplnit. Podvodník tak získá informace k platební kartě a může s ní manipulovat.
Velmi často k podvodům dochází při prodejích v online bazarech, jako je Aukro, Bazoš, Sbazar, Vinted nebo Marketplace.
Podvodníci lákají své oběti na atraktivní položky, jako je elektronika nebo značkové zboží za výhodné, až podezřele nízké ceny. Při komunikaci se vyhýbají osobnímu předání a zaslání zboží na dobírku. Aby získali peníze co nejrychleji, tvrdí, že má o zboží zájem jiný kupující a získá ho ten, kdo zaplatí dříve. Jakmile získá podvodník vaše peníze, komunikaci ukončí.

Preventivní rady a doporučení:

- **Nepodléhejte nátlaku**, koupi si promyslete.
- Při realizaci obchodu se domluvte na **osobním předání nebo na zaslání na dobírku**.
- U online plateb si hlídejte, aby probíhaly na zabezpečených protokolech (htpps, tls/ssl), na zabezpečené platební bráně nebo aby bylo využito aktivní zabezpečení 3D Secure.
- **S nikým nesdílejte údaje o své kartě**, zejména CVV/CVC ověřovací kód z druhé strany karty.