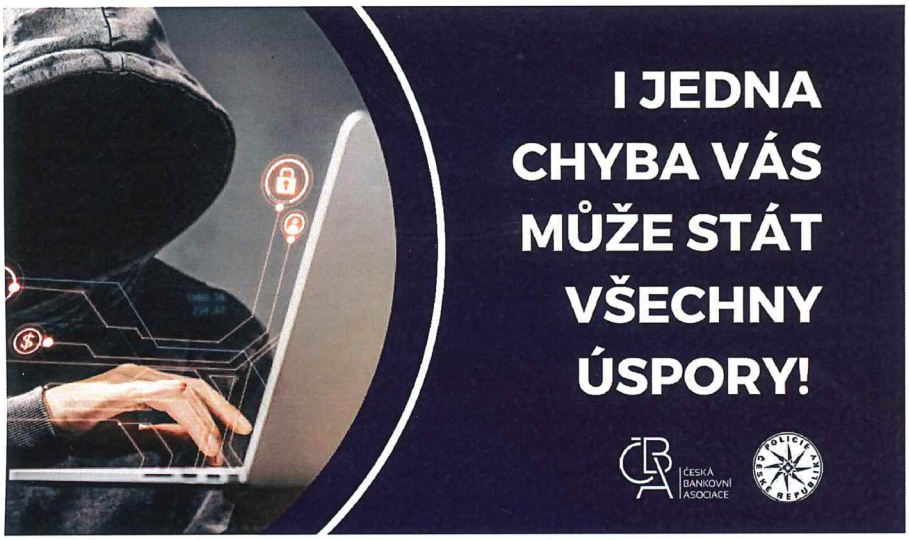
Varování před podvody přes internet!

Kyberkriminalita na Rychnovsku zaznamenala nárůst v řádu několika set procent!

Oddělení hospodářské kriminality Územního odboru Policie ČR Rychnov nad Kněžnou je v současné době zahlceno internetovou kriminalitou. Ve spolupráci s Oddělením analytiky a kybernetické kriminality PČR od počátku roku 2022 policisté zaznamenali obrovský nárůst případů, a to v řádu několika set procent. To obnáší velké zvýšení počtu prověřovaných případů, zvýšení počtů poškozených a jim způsobené škody přesahující milionové částky.



Internetová kriminalita tu byla i v letech minulých, ale neměla tak silné zastoupení, jednalo se o jiné způsoby páchání této trestné činnosti a zaevidovaných případů bylo znatelně méně. Bohužel v současné době pachatelé zneužívají „volný trh" a jejich působení v kyberprostoru je markantní.

U internetové (kybernetické) kriminality se jedná o majetkovou trestnou činnost, hlavně o podvody. Již od počátku jejího nárůstu bylo evidentní, že za vším stojí organizované zločinecké skupiny, které se takto vcelku snadno obohacují o obrovské zisky. V republikovém měřítku se jedná o desítky podvodů denně a o miliardy korun ročně. Pachatelé nemají důvod přestat, naopak stále mění své způsoby trestné činnosti, vymýšlejí nové varianty komunikace, vylepšují své legendy a přizpůsobují se změnám na trhu.

U INTERNETOVÉ KRIMINALITY PŘEVAŽUJÍ ČTYŘI ZÁKLADNÍ ZPŮSOBY PÁCHÁNÍ PODVODŮ.

1 Falešní zájemci o inzerované zboží

Prvním jsou podvody s falešnými zájemci o inzerované zboží. Oběti inzerují na různých portálech, v poslední době často na Vinted.cz, Bazoš.cz, Marketplace apod., kde nabízejí své zboží k prodeji, přičemž portály s tím nemají nic společného. Zpravidla cestou WhatsAppu se ozve falešný zájemce o zboží s tím, že je z jiného města a má o zboží obrovský zájem. Podvodník nabídne, že zaplatí dopravu a platbu předem a přes Whatsapp podvrhne odkaz na podvodné stránky tvářící se jako stránky přepravce typu DPD, PPL či Zásilkovna. Pak z oběti vyláká přihlašovací údaje do bankovnictví nebo i kompletní údaje k platební kartě včetně CVC kódu, který je na její druhé straně. Toto je nesmyslný požadavek, k prodeji není třeba číslo vaší karty, její platnost či CVC kód. Stejně jako požadavek přihlášení se do svého internetového účtu a následná autorizace. Správně kupujícímu poskytněte maximálně své číslo účtu, kam má peníze zaslat.

Poskytnutí všech ostatních osobních údajů a citlivých informací připravují prodávajícího o peníze, často v řádech deseti tisíců až statisíců korun. V tomto tak zvaném Phishingu jsou podvodníci bohužel velice úspěšní a prodejci naivní.

Máme případy, kdy firmy přišly o finanční částku přesahující v jednom případě 10 milionů a v druhém 13 milionů korun.

U občanů jsme evidovali největší škodu při investování do akcií, a to přes 2 miliony korun v jednom případě a v dalším případě přesahující 1 milion korun.

2 Falešní bankéři a policisté

Druhým příkladem je tzv. „falešný bankéř nebo policista", kteří volají s následující legendou. Váš účet je v ohrožení, proto musíte zajít do své banky, ale zde nikomu nic neříkat, protože pracovník banky je v této akci rovněž zapletený. Nutné je tedy peníze vybrat a vložit je do bitcoinmatu podle instrukcí, které podvodník „ohrožénému klientovi" dá. Při komunikaci používají pachatelé tzv. spoofované telefonní číslo, které může napodobit skutečné číslo banky či policie. Finanční prostředky převedené na kryptoměnu se okamžitě přesouvají jinam a stávají se nedobytné. Jakkoliv se může zdát legenda pachatelů úsměvná, evidujeme bohužel případy, kdy se pachatelé projevují jako zdatní manipulátoři a přivedou tak oběť k jednání, které s odstupem času sám nechápe.

3 Investování do kryptoměn a akcií

Třetím příkladem internetové kriminality je investování do kryptoměny či akcií známých firem. Oběť reaguje na reklamu, kterou mají pachatelé na sociálních sítích nebo zpravodajských serverech, ale oběť bývá často i přímo oslovena telefonicky. Když oběť zareaguje a projeví zájem o investování, pachatel ho manipulativními technikami přiměje vyplnit dotazník s osobními údaji a zaregistrovat se na podvržených stránkách. Následuje počáteční vklad v řádech tisíců korun jako ověření, že má oběť skutečný zájem. Následně ji přimějí k tomu, v rámci pomoci a zjednodušení, aby si do počítače nainstalovala software pro vzdálenou zprávu počítače, například program AnyDesk. Tím podvodníci získají správu počítače oběti a vidí vše, co na něm dělá, aniž to tuší. Dál už jejich trestná činnost funguje poměrně jednoduše. Přímo před obětí podvodníci zadávají vlastní platební příkaz, které jim oběť potvrzuje pomocí autorizace, které oběť obdrží od banky.

Jakkoliv to zní neuvěřitelně, lidé jsou tak zmanipulovaní, že podvodníkům autorizační kódy předávají. Pachatelé díky vzdálenému přístupu do počítače oběti a přihlášení se do internetového bankovnictví mohou zcela převzít její účet, když oběť autorizuje i změnu autorizačního zařízení. Pak si již podvodníci autorizace provádějí sami a na účtu oběti si sjednají i půjčku, kterou následně odcizí. Kvůli tomu, že jim oběť umožní pod jejich smyšlenou legendou vzdálený přístup do svého počítače a přihlásí se do svého internetového bankovnictví, přijde oběť o všechny své finance a často jí ještě vzniknou dluhy.

4 Firma mění číslo účtu

Čtvrtým příkladem podvodu je situace, kdy pachatel překoná bezpečnostní opatření a tím získá přístup k počítačovému systému, a tak je schopen sledovat e-mailovou komunikaci mezi dvěma firmami. Ve správný okamžik vystoupí jako jedna ze stran a kontaktuje podvrženým e-mailem obchodního partnera s tím, že mění své číslo účtu a podvrhne pozměněné faktury k zaplacení. Aby vystupoval jako obchodní partner mu stačí nepatrná změna v podvrženém e-mailu, třeba v přidání tečky.

Obecně lze říci, že internetová kriminalita je cílena na všechny, neexistují rozdíly mezi městy, obcemi či vzdělaností. První část komunikace s obětí je vytvořena počítačovým programem, který automaticky posílá např. hromadné zprávy. Takto obešle stovky lidí s tím, že někdo jistě zareaguje. Komunikace pak probíhá telefonicky či přes Whatsapp.

Ztráty jdou do milionů korun

V minulém roce jsme evidovali případy, kdy oběť přišla o finanční částku přesahující v jednom případě 10 milionů a v druhém 13 milionů korun, a to v případě firem. U občanů jsme evidovali největší škodu při investování do akcií, a to přes 2 miliony korun v jednom případě a v dalším případě přesahující 1 milion korun. V desítkách dalších případů pak začínají částky od několika desítek tisíc korun až po několik set tisíc korun.

Například při prodeji litých kol na auto přišel prodejce o více jak sto tisíc korun. Při podvodném napadení účtu přišel majitel účtu o více jak tři sta tisíc korun, při investování do akcií přišel zájemce o půl milionu korun a tak dále.

Kdo je „legalizátor"?

Podvodně získané finance končí na tuzemských či zahraničních účtech, jsou převáděny na krytpoměnu nebo vybrány z bankomatu tzv. legalizátory, což jsou lidé například najímání přes inzeráty na tzv. rychlou brigádu. Legalizátor buď poskytne svůj účet, na který podvodník pošle pod různými nesmyslnými legendami peníze a chce, aby je přeposlal dále, vybral či vložil do bitcoinů. Legalizátor může být i zmanipulovaný člověk, který si myslí, že investuje a při tom legalizuje jinde odcizené finanční prostředky a zároveň přichází i o svoje finance. Někteří legalizátoři mají za úkol zakládat bankovní účty a přihlašovací údaje předávat podvodníkům, kteří pak účty zneužívají pro trestnou činnost. Pachatelé podnikají všechny kroky, aby se peníze ztratily a byly nedohledatelné.

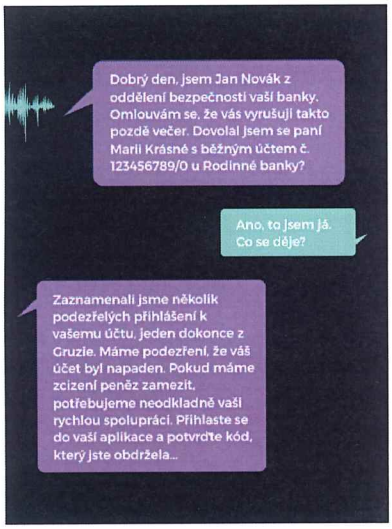
Na co si dát pozor?

- **Při prodeji nikdy nereagujte na zaslaný odkaz a nepřihlašujte se v něm do své banky.** Prodejci maximálně pošlete své číslo účtu. Všechny jiné požadavky jsou nesmyslné (proč bych se při prodeji přihlašoval do svého internetového bankovnictví) a směřují k jedinému – podvodu a zisku vašich peněz.

- **Pokud volá bankéř či policista s výstrahou, že máte napadený účet a musíte vybrat peníze, jedná se o podvod!**
Vždy si ověřte stav svého účtu ve své bance. Zajděte na kamennou pobočku nebo zavolejte na linku své banky. A když už si peníze vyberete a máte je v bezpečí u sebe, jaký je důvod vkládat je pak ihned do bitcoinmatu?

- **Osloví-li vás někdo k investici do kryptoměny či nákupu akcií, nikdy mu neumožněte vzdálený přístup ke svému počítači.** Máte-li potřebu investice či nákupu akcií, řešte to se svojí bankou na kamenné pobočce nebo s ověřenou společností s referencemi.

- **Změnu čísla bankovního účtu si ověřte.** Jestliže vám obchodní partner sdělí e-mailem, že mění číslo svého účtu, kam máte zaplatit za odebrané zboží, vždy si pro jistotu ověřte, zda komunikujete se skutečným obchodním partnerem, a že skutečně mění své číslo účtu pro platby!



Internetová kriminalita skýtá spoustu nástrah, proto buďte obezřetní a vše si pořádně rozmyslete anebo se před úkonem informujte u dotčených institucí nebo u někoho zkušeného. Jeden špatný klik vás může připravit o vše.
Pokud se přihlašujete do své banky, nikdy to nedělejte přes vyhledávač. Evidujeme případy, kdy se oběť přihlásila na stránky banky, které si našla cestou vyhledávače, ale ten ji nenašel oficiální stránky skutečné banky, nýbrž stránky podvržené, falešné s malou nepatrnou změnou v doméně. Při takovém přihlašování se tyto falešné podvržené stránky začnou „aktualizovat" a následně vyzvou k opakované autorizaci. A to proto, aby šlo pokračovat, avšak provedenou autorizací majitel účtu pustí pachatele na svůj účet a pak i potvrdí odchozí platby z účtu.

Všechny podvržené stránky jsou vytvořeny velice kvalitně a běžný uživatel je jen stěží na první pohled rozliší. Domnívá se tedy, že jde skutečné stránky, jako například v případech odkazů z MPSV (ministerstvo práce a sociálních věcí), třeba s informací, že vám posílají peníze, ovšem s podmínkou, že až se přihlásíte do své banky, pošlou vám příslušnou platbu na váš účet. Tento požadavek je nesmyslný a jeho účelem je také odcizení všech peněz z vašeho bankovního účtu.

Při autorizaci své platby v internetovém bankovnictví vždy a raději dvakrát zkontrolujte, co autorizujete. Z případů je zřejmé, že lidé se nedívají, co autorizují a výsledkem jsou odcizené peníze, často všechny životní úspory, případně i statisícové dluhy a oči pro pláč.

PŘIPRAVILI: ALENA KACÁLKOVÁ, MIROSLAV HOFMANN