

Podvodníkům se na internetu stále daří!

Policisté Územního odboru Bruntál v současné době zaznamenávají stále více podvodů na internetu. V tomto směru má okres Bruntál jeden z největších nápadů této podvodné trestné činnosti v republice. Je až alarmující, jak jsou lidé z našeho okolí důvěřiví. Pachatelé k okrádání svých obětí používají stále sofistikovanější scénáře v online prostředí. Spoléhají na překonání lidského faktoru za použití časového nátlaku, vyvolání strachu o ztrátu finančních prostředků, a také na nezkušenost, nepozornost a důvěřivost. O tom, že se jim v této oblasti daří, svědčí i nemalé škody, které dosahují i stovek tisíc korun na osobu.

K nejčastějším online rizikovým situacím patří:

Podvodné telefonáty – pachatel se vydává za bankéře, který se snaží ve své oběti vyvolat strach o finanční prostředky legendou o napadení bankovního účtu. Pod tímto tlakem se snaží přimět volaného, aby své peníze převedl na „zabezpečený“ účet banky, či vložil peníze do vkladomatu na virtuální měny. Často je tento telefonát doplněn o telefonát falešného policisty, který má potvrdit věrohodnost volajícího bankéře. K této metodě je využíván tzv. spoofing – napodobení čísla banky či policie.

Novinkou je, že se pachatelé vydávají už při prvotním kontaktu místo bankéře za policistu. Uvádí, že neznámý pachatel se snažil v bance načerpat půjčku na doklady osoby, které policista volá. Pro zvýšení věrohodnosti, že volá policista, zasílá pachatel volané osobě skrze WhatsApp kopii služebního průkazu, případně předvolání k podání vysvětlení. Následně volaného nabádá ke sjednání půjčky a pod záminkou ochrany, k převedení všech financí na účet, který je v moci pachatele.

Podvodné phishingové SMS, emaily apod. – pachatelé rozesílají podvodné zprávy, jejichž předmětem je daňový přeplatek, refundace bydlení, zabezpečení bankovních účtů, zásilka zboží apod. Součástí zpráv je odkaz, který navádí na věrohodně vypadající, avšak podvržené - falešné stránky, snažící se vylákat přihlašovací údaje k online bankovníctví.

Novinkou jsou příchozí SMS či WhatsApp zprávy z neznámého čísla, s oslovením „Ahoj tati, ahoj mami, tohle je mé nové číslo...“, ve kterých se coby potomek osloveného snaží vylákat finance na uhrazení akutního problému s vysvětlením, že komunikuje z nového čísla, jelikož mu původní číslo nefunguje, apod. Zde do podvodu často vstupuje i umělá inteligence.

Investiční podvody – na internetu se často objevují reklamy a články o bezpečném investování do akcií a kryptoměn s vidinou zaručeného, velmi vysokého zisku. Bývají doplněné o doporučení veřejně známých osobností a pochvalné komentáře dalších lidí, kteří potvrzují pravdivost tvrzení. Při projevení zájmu o investice volá zájemci falešný investiční poradce, který se snaží pod legendou pomoci s první investicí vmanipulovat svou oběť do instalace softwaru pro vzdálený přístup s cílem dostat se do bankovníctví a následného odcizení peněz.

Prodeje na inzertních serverech – poškozený inzeruje zboží na prodej. Falešný zájemce reaguje a v rámci rychlého a zjednodušeného obchodu se snaží prodávajícího přesvědčit k vložení údajů o platební kartě do platební brány, jevící se na první pohled

jako pravé. Udává, že na tuto kartu poukáže finanční prostředky, avšak po získání údajů k platební kartě, dochází k jejímu zneužití.

Přihlášení do bankovníctví přes falešné stránky – poškozený se do svého bankovníctví přihlašuje zadáním názvu banky do vyhledávače. V prvních několika odkazech se objeví placená reklama – většinou falešné stránky s URL adresou podobnou originálu. Po zadání přihlašovacích údajů na těchto stránkách, tyto putují k pachateli, který jich obratem zneužívá a nabourá se do bankovníctví.

Podvodné eshopy – pachatel zneužívá známé, renomované značky e-shopu či výrobce například pneumatik a vytváří podvodný web, který je věrohodnou kopií originálních webových stránek. Nabízí ovšem zboží za mnohem výhodnější ceny. Po zaplacení zboží, typicky v nadcházející sezóně pneumatik, ovšem poškozený neobdrží svou objednávku a přichází o finance, které zaplatil.

Upozorňujeme, že toto je pouze výčet nejpoužívanějších podvodných lstí a praktik. Jelikož je vynalézavost pachatelů široká, existují i další a budou stále přibývat. Je tedy velmi důležité být na pozoru, nedělat rychlá a ukvapená rozhodnutí, případně nepodléhat vidině rychlého zbohatnutí! Lidé, kteří takovýmto podvodným jednáním přichází o své prostředky, už je zpátky nevidí.

Závěrem tedy pár preventivních rad:

- Nenechte se zastrašit výhrůžkou ztráty peněz pod časovým tlakem, raději hovor s takovým „bankéřem“ či „policistou“ ukončete a ověřte si informace u Vaší banky, případně se obraťte na Policii České republiky!
- Nevěřte klamavým reklamám o rychlém zbohatnutí a nic nesjednávejte po telefonu! Zadarmo Vám nikdo nic nedá.
- Neinstalujte si do svého zařízení cizí osobou doporučené aplikace a neumožňujte jim vzdálený přístup!
- Neposkytujte nikomu přihlašovací údaje k Vašemu bankovníctví ani platební kartě!
- Při prodeji zboží si domluvte osobní převzetí či zaslání financí předem na Vaše číslo účtu. Neklikejte na zasláné odkazy a nikam nevyplňujte přístupové údaje k bankovníctví či platební kartě!
- Neotevírejte odkazy v příchozích zprávách (sms, email, soc. sítě apod.) z neznámých zdrojů!
- Důsledně kontrolujte správnost adresy banky či e-shopů a neklikejte na reklamní bannery odkazující na nestandardní adresy!
- Nevěřte lidem z neznámých čísel, vydávajících se za Vaše blízké a v žádném případě jim nezasílejte finanční prostředky!

por. Bc. Miroslav Kolátek

nprap. Jaroslav Krpec

Oddělení prevence

Krajského ředitelství Policie ČR

ÚO Bruntál