Kyberkriminalita: Na co si dát pozor na internetu?

Policie v poslední době zaznamenává obrovský nárůst podvodného jednání v oblasti kyberkriminality. Kriminalisté řeší případy podvodů založených na principech manipulace lidí za účelem provedení určité akce nebo získání informace s milionovými škodami. Na co si dát pozor?

Podvod přes inzerát

Prodáváte zboží přes inzerát na prodejních serverech nebo sociálních sítích? Dejte pozor na falešné kupující. Můžete přijít o peníze

Podvodníci využívají kontaktních údajů z inzerátů, vydávají se za kupující a snaží se prodejce různými způsoby manipulovat k provedení plateb nebo poskytnutí údajů k platební kartě apod. Nejčastěji pracují pachatelé s podvodnými platebními bránami, fiktivními přepravními společnostmi nebo falešným příjemcem.

Podvodná platební brána:

Cílem je nasměrovat oběť na předem připravený phishingový web (phishing je druh internetového podvodu, který se snaží z oběti vylákat citlivé údaje) v podobě platební brány. Pro takový web jsou často ke zvýšení důvěryhodnosti zneužita loga, grafika nebo názvy reálných ověřených doručovacích společností nebo poskytovatelů služeb. Příkladem je smyšlená služba Bazoš-pay.

Podvodná přepravní společnost:

Cílem je opět manipulace k zaslání peněz na účet podvodníků. V komunikaci často figuruje smyšlená přepravní společnost s věrohodnými webovými stránkami s obvyklými funkcionalitami jako sledování zásilky, chat s technickou podporou apod. Fiktivní dopravce se snaží navodit iluzi, že jsou peníze za prodávané zboží již na cestě, ale je nutné vyrovnat přeplatek, nedoplatek, zaplatit kauci k uvolnění částky apod. Pokud prodávající manipulaci podlehne a peníze odešle, přicházejí pod různými záminkami další a další výzvy k dalším doplatkům za dopravu, přeplatkům aj. Podvodníci v tu chvíli již cílí na sunk cost fallacy, tedy snahu oběti dotáhnout v tomto případě prodej do konce, když už do něj vložil peníze.

Podvodný příjemce:

V těchto případech se podvodníci snaží vylákat odeslání zboží, které nikdy nezaplatí. Adresa pro doručení bývá často v zahraničí anebo na adrese, kde zboží může bezpečně převzít relativně anonymní osoba (doručovací společnost u běžných zásilek neřeší, komu je zboží předáno).

V některých popisovaných případech figurují platby v kryptoměnách, např. cestou legitimní platební brány, kde oběť "nakoupí" krypto ve prospěch cizí peněženky nebo je oběť navedena k vytvoření účtu u směnárny.

Co signalizuje pravděpodobný podvod?

- Na inzerát reaguje cizinec. Není moc pravděpodobné, že si někdo ze zahraničí najde český inzerát s relativně běžným zbožím.
- Kupující požaduje nestandardní způsob dopravy, např. prostřednictvím neznámé zahraniční přepravní společnosti, nebo vyzvednutí zástupcem společnosti.

- Kupující navrhuje nestandartní způsob platby. Příkladem je zajištění jeho platby "přepravní společností", která peníze uvolní, až bude složena záloha nebo bude zboží na cestě nebo platební brána, která vyžaduje údaje z platební karty prodávajícího.
- Kupující požaduje platbu přes neznámé služby různých nebankovních platebních společností nebo chce platit v kryptoměně.
- Pro připsání zaslaných peněz má být složena jednorázová platba ze strany prodávajícího, nebo se objeví komplikace, které vyžadují zaslání platby.
- Zboží má být odesláno ještě před tím, než prodávající obdrží platbu.
- Zbystřete tedy vždy, když prodej vybočuje ze standardního modelu: podám inzerát -> ozve se zájemce -> zaplatí -> zašlu zboží (popř. zašlu na dobírku).

Falešné výhodné investice

Dostali jste nabídku výhodně investovat, která se nedá odmítnout? Zbystřete, je tu nový trik podvodníků.

Jak to funguje?

Hlavním cílem podvodníků je získat vzdálený přístup na plochu vašeho počítače a odcizit vaše peníze.

- Útočník na internet umístí lákavou reklamu slibující zaručené zisky. V reklamě se pro zvýšení důvěryhodnosti mohou objevovat známé osobnosti a významné společnosti.
- Reklama vybízí k vyplnění kontaktního formuláře. Po odeslání údajů je oběť oslovena například telefonicky podvodníky, kteří se vydávají za pracovníky různých investičních společností.
- Roztáčí se kolotoč intenzivní manipulace. Oběť poskytne osobní údaje, snímky osobních dokladů, údaje o platební kartě, a nakonec umožní i vzdálený přístup na plochu svého počítače (na základě telefonických instrukcí nainstaluje do svého počítače software, který vzdálený přístup umožnuje).
- Pod dojmem regulérní investice odesílá oběť své peníze přímo pachateli nebo je díky poskytnutým nástrojům provádí sám pachatel.
- Podvodníci využívají profesionálně vypadající investiční platformy. Vše vypadá velmi věrohodně a slouží k prodlužování nevědomosti či vylákání dalších finančních prostředků.

Jak se nenechat okrást?

- Nikdy neposkytujte vzdálený přístup k vašemu počítači nikomu, koho neznáte.
- Pachatelé Vás mohou oslovovat například telefonicky, e-mailem, nebo lákavou reklamou.
- Nevěřte bezhlavě telefonním číslům volajících, protože i ID volajícího může být podvržené.
- Neposkytujte ani žádné vaše osobní informace, nebo informace o vašem bankovnictví.
- Pamatujte, že v případě investování je riziko výhradně na straně investora. Volte proto pro zhodnocování svých peněz jen ověřené a renomované investiční společnosti.
- Nikdy plně nedůvěřujte recenzím, ty může napsat kdokoliv.
- Nepodléhejte manipulativnímu jednání, fiktivnímu doporučení celebrit, falešným novinovým článkům a už vůbec ne slibům zaručených investic bez rizika.
- Pokud údaje o svém bankovním účtu pod vlivem manipulace poskytnete podvodníkovi, ihned kontaktujte svou banku.

POZOR na falešné bankéře!

Dnešní moderní doba nahrává podvodníkům, kteří se svou obětí nemusí přijít do fyzického kontaktu. Stačí jim pouze telefon a věrohodný scénář, aby svou oběť připravili o několik desítek či stovek tisíc korun!

K velmi častým scénářům takových podvodníků patří vydávání se za bankovního úředníka. Pachatel volá se smyšleným příběhem o napadení bankovního účtu, snaží se ve své oběti vyvolat strach o její finanční prostředky a pod tímto tlakem donutit volaného, aby neodkladně převedl své peníze na zabezpečený účet a nepřišel tak o své úspory. K tomuto pachatelé používají tzv. spoofingu. To znamená, že používají napodobeninu čísla banky, případně policie. Během telefonního hovoru pachatel nabádá volaného, aby vybral veškerou finanční hotovost, případně si ještě sjednal úvěr a celý tento finanční obnos následně vložil do bitcoinmatu. Před vložením hotovosti zašle své oběti QR kódy, na základě kterých je zapotřebí peníze do vkladomatu vložit. Tyto kódy mají údajně zajistit vklad na zabezpečený účet. Pro zvýšení věrohodnosti svého tvrzení pachatel, coby bankovní úředník, přepojí poškozeného na falešného policistu, který doporučí s bankéřem spolupracovat dle sdělených informací. Poškozený pak v obavě o své peníze pachateli vyhoví, peníze vkládá v dobré víře do bitcoinmatu, avšak tímto krokem se připraví o vloženou finanční hotovost.

Policisté v této oblasti mimo jiné věnují velkou pozornost preventivním aktivitám, aby se tyto informace dostaly k nejvíce občanům a ti se následně nestávali dalšími podvedenými. Jednou z těchto aktivit je i umisťování preventivních letáků s varováním přímo na bitcoinmaty. Největší dosah informovanosti však zajišťuje spolupráce s médii a bankovními ústavy.

Vishing a spoofing jsou aktuálním trendem v nezákonných postupech podvodníků, jejichž cílem je získat neoprávněně cizí finanční prostředky nebo osobní data.

Kriminalisté zaznamenávají případy podvodů s milionovými škodami. Pachatelé přicházejí s novým způsobem vylákání peněz, který je pro oběť velmi obtížné odhalit. Podvody jsou páchány prostřednictvím jedné z metod sociálního inženýrství, tzv. vishingu.

Kromě peněz získávají podvodníci také citlivé osobní údaje, které mohou kdykoliv zneužít. Setkáte-li se tedy s podvodným jednáním s popisovaným průběhem, neváhejte kontaktovat Policii ČR, ale také svojí banku. Včasné kroky ještě mohou zvrátit ztrátu peněz.

Co dělat, pokud jste se Vy nebo někdo z Vašeho okolí s takovým podvodem setkali?:

- Nereagujte na podobné hovory a v žádném případě nesdělujte k Vaší osobě žádné citlivé údaje ani bezpečností údaje z vaší platební karty, nebo přístupové údaje k online bankovnictví.
- Nikdy nikomu nesdělujte a ani nepřeposílejte bezpečnostní / autorizační kód, který Vám přišel formou SMS zprávy.
- Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.
- Nikdy nikomu podezřelému neumožňujte vzdálený přístup do Vašeho počítače.
- Sledujte a pečlivě čtěte informace od Vaší banky v internetovém bankovnictví.
- Při každém vstupu do internetového bankovnictví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje.
- Aktualizovat software, antivirový program, firewall.
- Buďte neustále ostražití, protože i vy se můžete stát cílem podobného podvodného jednání.

- Během, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které Vám útočník sdělil (jména, e-mailové adresy, čísla účtů, odkazy na webové stránky, apod.)

Zároveň varujeme:

Nereagujte na telefonní hovory, SMS zprávy, e-maily, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich záchranu. Kdyby byly vaše peníze v ohrožení, tak banka sama zareaguje a učiní další opatření. V případě pochybností vždy kontaktujte svou banku. Pokud Vás shora naznačeným způsobem již někdo kontaktoval, neváhejte se rovněž obrátit na tísňovou linku Policie České republiky na čísle 158 a celou záležitost oznamte.

Další informace o možných postupech podvodníků, včetně rad, jak se jim bránit, můžete získat v dalších již zveřejněných varováních Policie ČR nebo u své banky.

Dávejte pozor na Vaše citlivé údaje, právě ty útočníka zajímají! To jsou informace, které mají být důvěrné pouze vám, nikomu jinému. Pokud je sdílíte s cizí osobou, vystavujete se velkému nebezpečí.

Které údaje nesmí padnout do cizích rukou?

- hesla do e-mailu, mobilního telefonu, internetového bankovnictví, profilů na sociálních sítích, apod.
- PIN kód platební karty
- PIN kód mobilního telefonu
- celé číslo platební karty
- autorizační kódy
- rodné číslo, číslo občanského průkazu, a další