SMISHING

Znáte už nový trik podvodníků? Citlivé údaje jako rodná čísla nebo přístupová hesla k bankovním službám lákají prostřednictvím SMS.

Telefonní číslo odesílatele může připomínat nebo přímo napodobovat například banku, úřad, doručovací společnost. U každé zprávy proto pečlivě posuzujte hlavně obsah.

Nevyžádané SMS, např. o výhře v soutěži, do které jste se nikdy nepřihlásili, jsou podezřelé. SMS s chybami naznačuje strojový nebo automatický překlad.

Odkazy často vybízejí k vyplnění osobních údajů, potvrzení přístupových hesel nebo poskytnutí přístupu do vašeho telefonu.

Pamatujte, že banky, úřady ani poskytovatelé doručovacích služeb po vás nikdy nebudou chtít osobní informace prostřednictvím SMS.

Pokud z odkazu v SMS nepoznáte, na jaké stránky vás navedou, neklikejte na něj.

Pravost SMS můžete ověřit u odesílatele. K tomu ale využijte kontakty z oficiálních zdrojů banky, úřadu, pošty atd. Ty v SMS mohou být opět zavádějící.

Pokud v návaznosti na popisované jednání přijdete o peníze na účtu, řešte vše obratem s bankou, která může v některých případech peníze ještě zachránit. Pokud je vám způsobena škoda, oznamte to také Policii ČR.

SMISHING
ZNÁTE NOVÝ TRIK PODVODNÍKŮ, PŘI KTERÉM OKRÁDAJÍ LIDI PŘES SMS. NEOTVÍREJTE BEZ UVÁŽENÍ ODKAZY V SMS, MŮŽE VÁS TO STÁT SPOUSTU PENĚZ.

FALEŠNÉ VÝHODNÉ INVESTICE

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

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.

FALEŠNÉ VÝHODNÉ INVESTICE
DOSTALI JSTE SUPER VÝHODNOU INVESTIČNÍ NABÍDKU? ZBYSTŘETE A HLAVNĚ NIKOMU NESVĚŘUJTE VLÁDU NAD SVÝM POČÍTAČEM. O SVÝCH PLATBÁCH SI VŽDY ROZHODUJTE SAMI.

VISHING

Vishing nebo také podvodné navolávání patří mezi další triky podvodníků. Není už úplnou novinkou, ale raději si připomeneme, v čem spočívá.

Pachatelé se vydávají za bankéře a policisty, oslovují oběť s legendou napadení jejího účtu a vybízejí k rychlému zálohování peněz, včetně přesných instrukcí, kam finanční prostředky ukrýt.

Oběť je zmanipulována k převodu finančních prostředků, k výběru a vložení finančních prostředků do vkladomatu na virtuální měnu nebo k vyzrazení citlivých údajů a případně k umožnění vzdáleného přístupu do svého zařízení.

Útočník často používá tzv. spoofing, to znamená, že telefonní číslo volajícího se tváří jako regulérní telefonní číslo banky, Policie ČR nebo jiným důvěryhodných institucí. Podvodníci v těchto případech dokáží napodobit jakékoliv telefonní číslo.

Nezapomínejte, že banka dokáže vaše peníze ochránit sama, pokud zjistí podezřelou aktivitu. Nikdy proto nebude požadovat, aby klient prováděl jakýkoliv převod nebo aby poskytl vzdálený přístup do mobilního telefonu nebo počítače.

Banka nikdy po klientovi nevyžaduje telefonicky citlivé údaje, kopie dokladů a platební karty. Všechny tyto údaje už o svých klientech má.

V případě podezření na podvod okamžitě kontaktujte svou banku. Hodně pomůže, pokud se vám podaří nahrát hovor s pachatelem.

VISHING

VOLÁ VÁM BANKOVNÍ ÚŘEDNÍK A TVRDÍ, ŽE JE VÁŠ ÚČET V OHROŽENÍ, A ŽE MÁTE OKAMŽITĚ SVÉ PENÍZE POSLAT JINAM? ZBYSTŘETE. SKUTEČNÍ BANKOVNÍ ÚŘEDNÍCI TAK NIKDY NEPOSTUPUJÍ.

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 z prodejce různými způsoby manipulovat k provedení různých 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 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, který 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 se 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).

PODVOD PŘES INZERÁT

PRODÁVÁTE ZBOŽÍ PŘES INTERNET? ZBYSTŘETE VŽDY, KDYŽ SE VÁS KUPUJÍCÍ SNAŽÍ PŘESVĚDČIT K NESTANDARDNÍM POSTUPŮM. NEPŘISTUPUJTE NA PLATBU NEDOPLATKŮ, PŘEPLATKŮ ČI KAUCÍ A NIKAM NEZADÁVEJTE SVÉ PLATEBNÍ ÚDAJE. KUPUJÍCÍ MÁ PLATIT VÁM, NE VY JEMU!