

KYBER RÁDCE

„Internetové podvody současné doby“



Pomáhat a chránit

Terčem KYBER útoku může být opravdu každý

- Do prostředí online podvodů se přesouvá organizovaný zločin s mezinárodním přesahem.
- Nikdo z nás není v úplném bezpečí.
- Naletět „šmejdům“ z online světa může každý. Ať už jde o děti, studenty, pracující či důchodce.
- Už to není o tom, že se nechá napálit jen „hlupák“. Sofistikovanost a kvantita útoků neustále stoupá. Je to jen o tom, kdy vás podvodníci **zastihnou nepřípraveného**.

A CO PORADIT?

Nenechte se uchlácholit tím, že vám na účtu nezbývá moc peněz.

Pachatel si převede peníze z vašeho spořicího účtu, či si na vás sjedná půjčky - a to vše s vaším přispěním.



Podvodné NAVOLÁVÁNÍ

- Pachatel se vydává například za bankéře, policistu anebo pracovníka technické podpory a snaží se z lidí pomocí vyvolání strachu vylákat peníze nebo je přesvědčit k tomu, aby si do svého zařízení nainstalovali program, pomocí kterého dokáže na dálku ovládat váš počítač.
- Vše začíná telefonátem, který probíhá velmi profesionálně. Volající „pracovník banky“ se představí, vysvětlí problém (nejčastěji jde o právě probíhající transakci, blokace karty, napadení účtu apod.) a na závěr od vás chce vědět či potvrdit osobní údaje pod zástěrkou vaší identifikace a informace k vašemu bankovnímu účtu.
- Pokud falešnému operátorovi vše sdělíte, stáváte se obětí podvodu a z vašeho účtu již v tu chvíli mizí leckdy i vaše celoživotní úspory, včetně toho, že si na vás podvodník vezme úvěr.

A CO PORADIT?

Nikdy nesdělujte informace o svém bankovním účtu, o přístupových údajích k němu ani vaše údaje k platební kartě. Banky tyto informace mají a nepotřebují je od vás slyšet.



Nabídka výhodných investic – akcie, kryptoměna

- Většinou jde o možnost nákupů akcií úspěšných společností, tedy ČEZ, Agrofert, Škoda Auto apod. V přesvědčivé reklamě, která se většinou objevuje na sociálních sítích investice vychvalují i známé osobnosti (jde o sportovce, politiky či velmi bohaté a úspěšné lidi).

Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků, k tomu využívá přirozenou ziskuchtivost každého z nás.

- V prvopočátku jde o drobnou investici v řádu stovek korun, které slouží k založení investičního účtu, případně k instalaci jiných investičních aplikací (Revolut, Binance apod.).
- Dalším krokem je spuštění programu ve vašem počítači, který umožní „poradci“ vzdálený přístup do vašeho zařízení (např. AnyDesk, TeamViewer) s příslibem, že za vás bude vše vyřizovat a obchodovat tak s větším výdělkem. Vše s příslibem rychlého zbohatnutí.
- V dalším kroku vás pachatelé přesvědčují vzít si půjčku, aby váš výdělek byl o to větší.



Podvody při prodeji vašeho zboží

VINTED, BAZOŠ, SBAZAR

- Pachatel zareaguje na váš inzerát (nejčastěji přes e-mail, či WhatsApp) a projeví zájem o koupi zboží, které se snažíte prodat. Poté následuje komunikace s vyžádáním vaší emailové adresy, na kterou podvodník pošle falešný odkaz pro přijetí peněz. Zde máte vyplnit údaje o vaší platební kartě, případně přihlašovací údaje do vašeho internetového bankovníctví.
- To nedělejte! K přijetí peněz přeci stačí jen číslo vašeho bankovního účtu.
- Pokud na podstrčeném odkaze zadáte údaje a potvrdíte platbu, už pachatelé ovládají váš účet. Vaše peníze pak pravděpodobně zamíří do zahraničí ...

A CO PORADIT?

Nikdy nevyplňujte žádné údaje v odkazech, které vám někdo zašle, ani když má kupující věrohodnou záminku. Pokud čekáte platbu – uvádějte jen číslo vašeho účtu.



Podvodné m-platby

- Podvodníci nejčastěji napodobí profil vašeho kamaráda např. na Messengeru nebo se do tohoto profilu neoprávněně nabourají a následně jeho jménem rozesílají zprávy všem přátelům z adresáře a chtějí získat vaše telefonní číslo s vymyšlenou pohádkou o soutěži, večeři apod. Po obdržení vašeho telefonního čísla pak žádají ověřovací kód, který vám přišel v SMS zprávě. Pod vaším telefonním číslem již totiž něco zaplatili.
- Mobilní **m-platby** fungují jako platební karty s rozdílem, že vám nejsou peníze strženy z bankovního účtu, ale z měsíčního tarifu u mobilního operátora.

A CO PORADIT?

Nikomu nesdělujte kód z SMS zprávy, protože tímto způsobem potvrzujete transakci, tj. m-platbu.



Podvody přes seznamky - voják, lékař na misi...

- Pachatelé hledají své oběti obvykle na internetových seznamkách a snaží se svoji oběť zlákat a zmanipulovat. Nějakou dobu si s obětí dopisují přes e-mail, chat, posílají si vzájemně své fotografie či videa. Oběť zjišťuje, že má s pachatelem (lékařem či vojákem na misi) společná témata a zájmy, až se zrodí láska na dálku. Pachatel slibuje budoucí společný život.
- Pak přichází zádrhel. Pachatel by rád přijel, ale finanční prostředky na zakoupení letenky nemá na misi k dispozici a chce poslat peníze. Nebo si rovnou řekne o finanční půjčku s legendou pořízení společného bydlení. Slibuje, že všechny peníze vrátí hned, jakmile to bude možné.
- Dalším způsobem může být i cenný balíček (šperky, zlato), který pachatel oběti posílá. Ta musí „jen“ zaplatit poplatky k proclení, pojištění či dopravě. Tuto částku může pachatel postupně navyšovat až do milionových hodnot.

**Pozor na internetových seznamkách – nikdy totiž neznáte
skutečnou totožnost vašeho ideálu!**



Jak NENALETĚT on-line „šmejdům“

- Nenechte se od pachatele do ničeho tlačit a vše si raději pečlivě promyslete.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát například ohledně napadení vašeho bankovního účtu neočekávaný, tak je podezřelý.
- Vždy se zamyslete nad tím, kam vypisujete vaše osobní data, údaje k platební kartě, k bankovnímu účtu, nebo kam posíláte své peníze.
- Když si nejste absolutně jistí, tak vždy raději vše ověřte jinou cestou (telefonicky, osobně).
- Nikdy neumožňujte vzdálený přístup cizím osobám do svého zařízení.
- Nikdy nesdělujte kupujícímu na inzertních portálech údaje o své platební kartě nebo o vašem bankovním účtu.
- Pokud je možnost, aktivujte si dvoufázové ověřování účtů u služeb, které používáte.

A CO PORADIT NA ZÁVĚR?

Mějte bezpečné heslo - doporučuje se 12 znaků, promíchat malá a velká písmena, číslice a použít speciální znaky (*, /, _ apod.).



Děkujeme za pozornost

Kontakt

Tel.: 974 221 207

Email: krpc.pio@pcr.cz

