

Policisté apelují na občany, v kyberprostoru buďte ostražití!

V tomto roce policisté napříč republikou evidují nárůst případů, kdy lidé „naslepo“ obchodují s neznámými lidmi prostřednictvím internetových portálů a stávají se oběťmi podvodníků. Lidé v kyberprostoru ztrácejí obezřetnost a nechají s sebou manipulovat. Konec je většinou stejný, podvodník je obere o vysoké finanční částky, které převážně končí na neznámých účtech v zahraničí. Nutno podotknout, že obětí internetového podvodu se může stát každý. Mějte na paměti, že internet není bezpečné místo, kde můžete vypustit svoji obezřetnost a bezmyšlenkovitě dělat co vás napadne. Naopak je zde nutné mít všechny smysly v pohotovosti a vše si důkladně ověřovat.

Podvodníci přicházejí s různými legendami jako například:

- V současné době se policisté nejčastěji setkávají s podvody, kdy pachatelé své oběti obvykle kontaktují přes WhatsApp nebo Messenger s tím, že koupí zboží, které kontaktovaný nabízí k prodeji prostřednictvím inzertního portálu (Vinted, Bazoš apod.). Po krátké výměně zpráv svým obětem namluví, že peníze uložili u kurýrní služby, která si pro zboží přijede. Stačí kliknout na odkaz a vyplnit údaje. Prodávající se pak nestačí divit, jak rychle o své peníze přijde.
- Další legenda, kterou podvodníci používají je ta, že podvodník sdělí prodávajícímu, že peníze za zboží poslal prostřednictvím platební karty a pošle prodávajícímu odkaz. Jediné, co musí prodávající pro přijetí peněz udělat, je odkaz rozkliknout a vyplnit údaje z karty, na kterou chce peníze přijmout. S vidinou prodeje zboží tyto údaje prodávající vyplní. Podvodník má tak všechny informace o klientově kartě a tím i přístup k jeho bankovníctví. A peníze z účtu mizí.
- Dalšími častými případy podvodů jsou investice do kryptoměn. Iluze o snadném a rychlém zbohatnutí nahrává podvodníkům, kteří na internetové portály a sociální sítě umisťují reklamy, kterými ziskuchtivé občany lákají na velmi výhodné zhodnocení vkladů a investování do světových měn, včetně Bitcoinů. Vše většinou začíná velmi výhodnou nabídkou, např. v podobě internetové reklamy. Stránka, na kterou se zájemce po kliknutí na reklamu přeměruje, je plná odkazů na renomované články o známých osobnostech, kterým se podařilo svěřením se do péče reklamovaného finančníka peníze zhodnotit. Tyto podvodné stránky končí formulářem, který nabádá k registraci a vyzkoušení si možnosti investování. Pokud zájemce podlehne, vyplní a odešle registrační formulář, většinou následuje velmi brzy telefonát. Domnělí bankéři jsou velmi komunikativní a obratní. Často jim oběť poskytne kromě osobních údajů, snímků dokladů totožnosti či platebních karet také vzdálený přístup ke svému počítači. K vybití účtu pak už nebrání prakticky nic.
- Pachatelé získávají kryptoměny také cestou, při které není nic zastíráno. Šířením ransomware je do zařízení poškozených subjektů instalován škodlivý kód, který šifruje soubory na počítačovém systému nebo omezuje uživatele. Za dešifrování souborů nebo obnovení přístupu je požadováno výkupné, ve většině případů právě v kryptoměnách.
- Jsou i případy, kdy se podvodníci vydávají za bankéře a následně i policisty a pod legendou ohrožení finančních prostředků na bankovním účtu manipulují svoji oběť do provádění finančních transakcí. Nic netušící majitel bankovního účtu z obavy o své peníze převádí peníze přímo podvodníkům.

- „Láska přes internet, která stojí hodně peněz“. Stále se objevují případy a nejsou bohužel ojedinělé, kdy podvodníci vystupují v konverzaci jako lékaři na zahraničních misích, vojáci, námořníci apod. Na takové podvody už naletělo velké množství důvěřivých žen i mužů. Slibují, lásku, domov, šťastný společný život a bohatství. Zamilovaní podvedení jim posílají své peníze na vymyšlené poplatky a těší se, že už brzo budou mít svojí lásku u sebe. V drtivé většině případů přijdou mnohdy o statisíce někdy i miliony, než podvod prohlédnou.

A to je jen výčet těch nejčastějších legend, kterými může podvodník připravit o peníze kohokoliv, pokud nebude obezřetný.

Základní rady, jak nenaletět:

- Poznejte svého nepřítel. Seznamujte se s aktuálními hrozbami a trendy v online podvodech.
 - Zvažte, zdali přijmete nabízené přátelství od neznámého člověka na internetu.
 - Dávejte si pozor na sliby týkajícího se vážného vztahu, zejména s osobou ze zahraničí.
 - Protistrana dokáže velmi citlivě působit zejména na osamělé osoby, milá slova, komplimenty, lichotky, hraní na city...
 - Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete.
 - Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
 - Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze.
 - Když si nejste absolutně jisti, tak vždy raději vše ověřte jinou cestou.
 - Pamatujte si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
 - Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete.
 - Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z vaší platební karty.
 - Nesděluje své osobní údaje.
 - Nezasílejte ofoceně osobní doklady.
 - Nesděluje tištěné informace z platební karty.
 - Nesděluje kód, kterým by vzdáleně přistupoval k vašemu počítači.
 - Nesděluje bankovní autorizační SMS kódy.
 - Cizí osobě nikdy neautorizuje platbu.
 - V počítači mějte nainstalovaný stále aktualizovaný antivirový program.
 - V internetovém bankovníctví mějte nastaveny co nejnižší limity a zvyšujte je jen na aktuální potřebu zaplacení konkrétní platby.
- Vyzkoušejte si www.kybertest.cz a zjistěte, kde máte mezery.

Bud'te připraveni, protože kdo je připraven, není překvapen.

por. Bc. Lenka Pokorná ta.pis@pcr.cz
 tisková mluvčí a preventistka
 PČR ÚO Tábor
 24. října 2022