Policisté znovu upozorňují na sílící vlnu podvodů, která se odehrává ve virtuálním světě. Denně jsou to desítky nových případů, kdy způsob podvodů bývá velmi podobný.

Nejčastější způsoby podvodů na internetu zacílené na kryptoměnu jsou následující:

1) Výhodná nabídka – investice do kryptoměn – pachatel opět vyláká od poškozeného platební údaje či získá neoprávněný přístup k počítači a poté následuje neoprávněná transakce ze strany pachatele.
2) Falešný bankéř – podvodník telefonicky zkontaktuje svoji oběť s tím, že si ověřuje její žádost o úvěr. Zde se většinou oběť ohradí, že žádný úvěr nemá a ani nemá účet u uvedené banky. Podvodník se omluví a sdělí, že informaci předá do její banky. Poté následuje další telefonát, kdy se podvodník vydává za bankéře banky oběti. Podvodník sdělí, že došlo k napadení účtu a je nezbytně nutné vybrat veškerou hotovost. Následuje nabídka převodu peněz na bezpečný účet a zaslání QR kódu na telefon. Tento kód má poté oběť načíst u bitcoinového bankomatu při vkládání peněz.

Na všechny způsoby podvodů však platí stejné rady a doporučení, jak se nestát obětí kyberpodvodníků:

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovnictví ani čísla ze své platební karty. **Banky se na ně neptají, ani zprávami či e-mailem neposílají odkazy na weby, kde jsou vyžadovány!**
2. Při každém vstupu do internetového bankovnictví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje.
3. Sledujte a pečlivě čtěte informace od vaší banky v internetovém bankovnictví.
4. Nereagujte na telefonní hovory, e-maily ani zprávy, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další krok pro jejich záchranu.
5. Nezadávejte ani v aplikaci nepotvrzujte platby, které vám bude diktovat někdo po telefonu, ani nikomu nesdělujte či nepřeposílejte potvrzovací kódy z SMS. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.
6. Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.
7. Podvodnou platbu co nejdříve ohlaste na PČR a co nejdříve reklamujte u svého bankovního subjektu.
8. Jakoukoli komunikaci ze strany podvodníka nemažte do doby, než bude zajištěna policejním orgánem.
9. Buďte obezřetní při využívání inzertních portálů. Pečlivě volte způsob platby a ani v těchto případech neklikejte na zaslané odkazy.
10. Mějte aktualizovaný software a antivirus. A to i na mobilním telefonu.

Kounicova 24
611 32 Brno

www.policie.cz

Tel.: +420 974 624 486
Email: krpb.prevence@pcr.cz

11. V případě pochybností vždy kontaktujte svou banku či volejte 158.

Odhalíte včas, že na vás útočí online podvodníci? Vyzkoušejte si test a poměřte své výsledky s ostatními na: www.kybertest.cz.

por. Mgr. Zdeňka Procházková
oddělení tisku a prevence
Krajské ředitelství policie Jihomoravského kraje