Kyberkriminalita se stále rozšiřuje

KARLOVARSKÝ KRAJ – Přežijete v online světě?

Policisté Karlovarského kraje upozorňují, že se rozmohla nová forma trestné činnosti týkající se kyberprostoru, kdy pachatelé napodobují různá telefonní čísla, jejichž prostřednictvím pak své oběti kontaktují jakožto pracovníci klientské linky určité banky s tím, že je nutné z různých důvodů zprostředkovat převod jejich peněz.

Právě na tuto problematiku má upozorňovat celorepubliková „kyberkampaň“, v rámci které proběhly v Karlovarském kraji preventivní akce, kterých se účastnily policistky z oddělení tisku a prevence. Na těchto akcích preventistky poskytovaly veřejnosti preventivní rady týkající se dané problematiky, jako např. jakým způsobem mají lidé chránit své úspory, aby se nemohli stát obětí útočníka nebo také jak chránit své osobní údaje.

Kyberkampaň upozorňuje především na problematiku týkající se bankovnictví. Česká bankovní asociace a Policie ČR varují před pachateli, kteří mohou po oběti chtít jménem banky přístupové údaje do internetového bankovnictví, údaje o platební kartě nebo provedení platební transakce z důvodu hrozícího útoku na její účet. Důrazně upozorňujeme, aby lidé na tyto požadavky nereagovali, neboť jde o podvodníka.

Na základě výše uvedeného je potřeba připomenout 5 rad pro bezpečí vašich peněz:

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. 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 kroky pro jejich záchranu. **Kdyby byly vaše peníze v ohrožení, banka by zareagovala dávno už bez vás.**
3. Pány svého účtu jste jen vy. NEZADÁVEJTE ani v aplikaci NEPOTVRZUJTE PLATBY, které vám někdo bude diktovat po telefonu, ani nikomu NESDĚLUJTE či NEPŘEPOSÍLEJTE potvrzovací kódy z SMS. Stejně tak NEDÁVEJTE nikomu VZDÁLENÝ PŘÍSTUP DO vašeho POČÍTAČE.
4. MĚJTE AKTUALIZOVANÝ SOFTWARE a ANTIVIRUS. A to i na telefonu!
5. **V případě pochybností vždy kontaktujte svou banku či volejte 158**. Myslete na to, že útočník dokáže napodobit jakékoli telefonní číslo (tzv. spoofing) či e-mail včetně těch vaší banky.

V rámci kampaně si můžete vyzkoušet i kybertest, který naleznete na internetové stránce [www.kybertest.cz](http://www.kybertest.cz) . Test obsahuje 10 obrázků představující běžné situace, do kterých se jako uživatel internetu a klient banky může dostat. Můžete si tak vyzkoušet, zda byste podvodná jednání poznali.

prap. Mgr. Lucie Machalová

kpt. Bc. Zuzana Týřová

13.9.2021