BUĎTE OBEZŘETNÍ I VE VIRTUÁLNÍM SVĚTĚ.

Neustále se objevují nové případy kybernetických podvodů, kdy útočníci využívají manipulativní komunikaci a nátlak na své oběti. Internetoví podvodníci pořád hledají cesty, jak napálit důvěřivce a své techniky stále zdokonalují. A právě v tomto předvánočním čase, v době nákupů se bude jejich aktivita zvyšovat, proto apelujeme na všechny, buďte obezřetní.

Nejčastěji využívanými technikami internetových podvodníků jsou phishing, vishing a smishing.
Phishing – rozesílání e-mailových zpráv, které adresáta vyzývají k zadání osobních údajů. Útočník se vydává za důvěryhodnou autoritu.
Útočníci rozesílají e-maily, které vypadají, že přicházejí od důvěryhodné firmy, banky, úřadu. Pomocí této komunikace se útočníci snaží vylákat citlivé informace, které se týkají bankovních kont, platebních prostředků apod. Získaná data využívají poté k odčerpání financí z účtu oběti.
Vishing – oklamání oběti prostřednictví telefonního hovoru.
Podvodníci se představují jako pracovníci bank či policisté, kteří zjistili napadení bankovního účtu, popř. jako bezpečnostní experti, kteří chtějí zabezpečit Váš počítač.
Cílem útočníků je vylákání různých citlivých informací, které mohou být následně zneužity (informace k osobní identitě, k platební kartě, k bankovnímu účtu...).
Smishing – forma phishingového útoku prováděná prostřednictvím SMS.
Podvodníci se snaží vylákat citlivé údaje k účtům nebo platebním kartám.
Prostřednictvím SMS může být zaslána naléhavá výzva, informace o hrozbě napadení účtu i s nabídkou řešení v podobě odkazu, kam má oběť kliknout. Po otevření odkazu je ve většině případů oběť vyzvána k zadání citlivých údajů k bankovnímu účtu či k platebnímu prostředku.

Základní pravidla bezpečnosti:

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.
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.

Kounicova 24
611 32 Brno

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

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

Krajské ředitelství policie Jihomoravského kraje přeje všem klidné vánoční svátky a mnoho sil do dalšího roku.

Kounicova 24
611 32 Brno

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