Kyberšmejdi dovolenou nemají. Buďte obezřetní i o prázdninách!

Internetová kriminalita je stále na vzestupu a ani o prázdninách tomu není jinak, ba naopak, kyberšmejdi ve velké míře využívají tento dovolenkový čas ke svým nekalým praktikám.

Policie ČR proto důrazně upozorňuje na tyto aktivity a všechny vybízí k velké obezřetnosti i třeba v souvislosti s pořizováním dovolenkových pobytů.

V současné době se můžeme často setkat s phisingovými stránkami, které se snaží z důvěřivé veřejnosti vytáhnout citlivé osobní údaje, peníze, či přístupová data k účtům.

Podvodné webové stránky často napodobují stránky známých cestovních značek s cílem oklamat uživatele a přimět je k zadání přihlašovacích údajů a osobních informací. Především pak při hledání dovolených na poslední chvíli je nezbytná velká obezřetnost. Stejně tak při rezervování letenek, popř. ubytování je nutné mít toto riziko na paměti a být velmi opatrný a pečlivý. Podvodníci mohou číhat i na legitimních webech, kdy se jim podařilo proniknout do administrativních systémů jednotlivých hotelů, které tyto portály využívají. Probíhá to tím způsobem, že podvodníci přesvědčí personál hotelů ke stažení škodlivého softwaru, který je jim zaslaný prostřednictvím e-mailu. V něm se mohou vydávat např. za bývalého hosta, který si v hotelovém pokoji zapomněl cestovní doklad, následně posílají personálu odkaz na Disk Google s tím, že obsahuje obrázek pasu. Místo toho vede odkaz na škodlivý software, který automaticky prohledá hotelové systémy a získá přístup k účtům na legitimních portálech. Poté se již podvodníci po přihlášení do daného portálu probírají jednotlivými zákazníky i s aktuálními informacemi k rezervacím. Po získání těchto informací přes oficiální aplikaci portálu posílají zákazníkům zprávy, kde je vyzývají k platbě. Peníze však nejdou na účet hotelu, ale kyberpodvodníkům.

Apelujeme tedy na všechny, aby byli velice opatrní a kontrolovali si, kam posílají peníze. Určitě v takových případech je bezpečnější kontaktovat přímo vybraný hotel a platbu a informace k platbě ověřit.

Přes letní měsíce jsou také velmi aktuální podvody související s nabídkou práce. Podvodníci velmi často nabízejí jednoduchou práci v on-line prostředí nejčastěji prostřednictvím chatovací aplikace. Ve zprávě informují o podmínkách a náplni práce (často se jedná o lajkování videí na sociálních sítích). Lajkujete tedy videa a opravdu vám na účet chodí drobné částky. Dále dochází k tomu, že vás podvodník požádá o přeposlání části financí na jiný účet nebo o předkoupení kreditu, abyste mohli pokračovat v práci. Pokud postupujete dle těchto pokynů, přeposíláte peníze z trestné činnosti (pravděpodobně jde o peníze některé z obětí, kterou podvodníci okradli před vámi). Stáváte se tak bílým koněm a dopouštíte se protiprávního jednání.

Stejně obezřetní buďte i v případě nyní poměrně častých phishingových útoků nazývaných **quishing**. Jedná se o podvod, který využívá QR kódy, v současné době velmi často využívaná metoda nejen pro sdílení kontaktů, stahování aplikací, ale i např. k platbám. Ze samotného QR kódu nepoznáte, zda je nebezpečný či nikoli. Za QR kódem se může skrývat odkaz, pomocí kterého dojde k přesměrování na stránky, jejímž cílem jsou krádeže přihlašovacích údajů.

Při využívání QR kódů buďte velmi ostražití a dávejte pozor zejména na to, zda není původní QR kód překrytý jiným. Používejte pro skenování QR kódu takovou aplikaci, která nabízí bezpečnostní prvky, jako je předchozí zobrazení URL adresy před přesměrováním na webovou stránku. Tímto způsobem můžete zkontrolovat, zda adresa vypadá důvěryhodně, než se na ni rozhodnete přejít.

Kounicova 24
611 32 Brno

www.policie.cz

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

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.
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. Při skenování QR kódů zkontrolujte, zda není překrytý původní kód tím falešným. Používejte při skenování QR kódů takové aplikace, které nabízí bezpečnostní prvky, jako je předchozí zobrazení URL adresy před přesměrováním na webovou stránku. Tímto lze zkontrolovat důvěryhodnost stránky před jejím rozkliknutím.
11. Mějte aktualizovaný software a antivirus. A to i na mobilním telefonu.
12. V případě pochybností vždy kontaktujte svou banku či volejte 158.

Důležité odkazy:

- www.kybertest.cz
- www.policie.cz
- www.saferinternet.cz
- www.nukib.cz
- www.hoax.cz
- www.csob.cz/BranteSeRozumem
- www.jaknainternet.cz

Kounicova 24
611 32 Brno

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