CESTUJTE (KYBER)BEZPEČNĚ:

NÚKIB

DOPORUČENÍ PRO CESTY NA LETNÍ OLYMPIJSKÉ HRY V PAŘÍŽI 2024

1. DBEJTE ZVÝŠENÉ POZORNOSTI PŘED PHISHINGEM

Vzhledem k významnosti akce lze předpokládat škodlivé aktivity v kyberprostoru, jež mohou směřovat mimo jiné vůči účastníkům akce. V minulosti byly obdobné události zneužívány k zasílání phishingových zpráv s cílem zisku citlivých informací. Je proto třeba dbát zvýšené opatrnosti při stahování dokumentů či otevírání příloh v rámci internetové komunikace.

CO JE TO PHISHING?

Phishing je typ kybernetického útoku pomocí technik sociálního inženýrství, kdy se útočník snaží získat citlivá data oběti nebo na jejím zařízení spustit škodlivý kód. Nejčastěji tyto útoky probíhají za využití e-mailů či SMS zpráv (smishing), které napodobují legitimní komunikaci. Na vzestupu jsou však případy vishingu, během kterého útočník provádí podvodné volání.

2. MINIMALIZUJTE VYUŽÍVÁNÍ VEŘEJNÝCH WI-FI SÍTÍ

Veřejné sítě na letištích, v hotelech či různých restauracích a na dalších veřejných místech velmi často nedisponují dostatečným zabezpečením. Útočníkům tím poskytují potenciální příležitost sledovat vaši komunikaci a zachytávat tak kromě potenciálně citlivých informací například také přihlašovací údaje a hesla. Je tudíž doporučeno, pokud možno tyto sítě využívat pouze okrajově, případně se skrze ně alespoň nepřihlašovat například do internetového bankovnictví nebo dalších obdobných služeb a nesdělovat skrze ně citlivé informace. Pokud přece jen potřebujete připojení skrze takovou Wi-Fi, tak využívejte VPN služby. Ty zajišťují šifrování provozu a vytváří bezpečnější „tunel“ pro vaše internetové aktivity.

3. PRO MAXIMALIZACI ZABEZPEČENÍ PREFERUJTE DATOVÝ ROAMING SPOLU S VPN A END-TO-END ŠIFROVÁNÍM

Nejvíce bezpečnou variantou internetového připojení je využití datového roamingu. Dodatečně lze využít také některou z VPN služeb a komunikovat skrze aplikace s end-to-end šifrováním. V takovém případě se riziko narušení důvěrnosti vaší komunikace výrazně minimalizuje.

4. NENECHÁVEJTE SVÁ ZAŘÍZENÍ BEZ DOZORU A NEZAMČENÁ

Dále je doporučeno za žádných okolností nenechávat svá elektronická zařízení bez dozoru, a to primárně s ohledem na možnost dalších typů kompromitace ze strany útočníka. Pokud je to však potřeba, je velmi důležité dané zařízení uzamknout, čímž se významně snižují možnosti kompromitace útočníkem. Nebezpečné může být také používat darované flash disky, kabely, ale i veřejné nabíječky či jiné doplňky, které mohou na vašem zařízení spustit škodlivý kód.

5. ZABEZPEČTE SVOJE SLUŽBY DVOUFÁZOVÝM OVĚŘENÍM

Je vhodné mít nastavenu dodatečnou úroveň ochrany vámi používaných služeb ve formě dvoufázové autentizace (2FA). Tu podporuje většina služeb jako jsou e-mailové aplikace, účty na sociálních sítích či internetové bankovnictví. Použití 2FA významně minimalizuje škody, jež může útočník napáchat i v případě, že dojde ke krádeži vašich přihlašovacích údajů.