10 SPÔSOBOV, AKO SI CHRÁNIŤ OSOBNÉ ÚDAJE

1

Neklikajte na odkazy

Neklikajte na internetové odkazy v e-mailových správach. Adresu webstránky ktorú chcete navštíviť prepíšte do adresného riadka internetového prehliadača.

Prečo? Odkaz v e-maili môže byť falošný a pod ním môže byť skrytý podhodený odkaz na phishingovú stránku.

2

Používajte viacstupňové overenie

Ak to aplikácia umožňuje, nastavte si viacfaktorové overenie (autentizáciu) pri ktorej musíte na dvoch alebo viacerých stupňoch preukázať dôkazy (faktory) na potvrdenie vašej totožnosti, napríklad heslo a kód, ktorý sa zasiela na váš mobilný telefón.

Prečo? Viacnásobné overenie poskytuje ďalšiu vrstvu bezpečnosti, čo výrazne znižuje šancu útočníka prihlásiť sa do aplikácie vo vašom mene.

3

Vymazávajte staré konverzácie

Pravidelne vymazávajte uložené rozhovory v diskusných fórach, SMS-kách a chatovacích aplikáciách. Väčšinou obsahujú citlivé osobné informácie.

Prečo? Nemá zmysel držať históriu rozhovorov, najmä ak sú známe prípady, keď sa k takýmto starším konverzáciám dostali útočníci.

4

Obmedzte požiadavky poskytovateľov

Znížte množstvo informácií, ktoré o sebe poskytnete v nastaveniach internetových služieb. Dôkladne zvážte, aké osobné údaje uvádzate na svojom profile. Zvoľte len také nastavenia, ktoré vyhovujú vám.

Prečo? Aj samotné platformy poskytovateľov internetových služieb mnohokrát požadujú informácie, ktoré im vôbec nie ste povinní poskytnúť. Ak si nie ste istí, rozmyslite si, či si profil u danej spoločnosti vôbec vytvoríte.

5

Nezdieľajte svoju polohu

Vypnite sledovanie geografickej polohy vo všetkých aplikáciách, ktoré to nepotrebujú ku svojej funkčnosti.

Prečo? Je verejným tajomstvom, že aj veľkí poskytovatelia služieb radi speňažia vaše údaje za účelom zisku z reklamy. Nečudujte sa, ak vám chodia ponuky z obchodov, okolo ktorých práve kráčate. Ale je tu aj oveľa vážnejší problém: moderní zlodeji si najprv zistia, kde sa nachádzate a váš byt alebo dom pohodlne vykradnú v čase, keď ste čo najďalej.

6

Nedôverujte správam, ktoré sľubujú výhody

SMS správy alebo e-mail, ktoré sľubujú cenové zľavy, zisk, alebo akékoľvek iné finančné výhody, sú samozrejme lákavé. Nesmiete im však naletieť.

Prečo? Zvyčajne ide o podvod, najmä ak je nárokovanie výhod podmienené zaslaním osobných údajov.

7

Neverte súrnym správam

Jednou z techník sociálneho inžinierstva je snaha o vyvolanie časovej tiesne. Na také správy nereagujte.

Prečo? Ak je nejaký e-mail označený ako urgentný, alebo si v texte vyžaduje vašu okamžitú reakciu, takmer s istotou je falošný. Podvodníci sa snažia vyvolať dojem naliehavosti, aby ľudí zaskočili a vylákali od nich osobné údaje.

8

Používajte silné heslá

Vytvárajte heslá, ktoré majú aspoň 15 znakov a obsahujú kombináciu veľkých a malých písmen, číslic a symbolov, ak to aplikácia umožňuje.

Prečo? Čím silnejšie je vaše heslo, tým ťažšie je hacknúť váš účet. Ľahko zapamätateľné heslá dokážu útočníci ľahšie uhádnuť.

9

Neinštalujte zbytočnosti

Pred inštaláciou dôkladne zvážte, či príslušnú aplikáciu naozaj potrebujete, alebo vás len ovládla zvedavosť, či presvedčila reklama. Nepotrebné aplikácie odstráňte. Zároveň jediný bezpečný spôsob, ako získať aplikácie, je stiahnuť ich priamo z oficiálneho obchodu (Google Play, Apple App Store atď.). Rozmýšľajte aké údaje a súhlasy poskytujete pri potvrdení softvérovej licencie.

Prečo? Kliknutím na náhodný odkaz na stiahnutie aplikácie by ste si mohli infikovať vaše zariadenie. Ak je aplikácia zadarmo, znamená to, že produktom ste vy sami.

10

Plátajte a aktualizujte

Váš počítač, smartfón, wifi router a všetky IT zariadenia musia mať vždy nainštalované posledné verzie aktualizácií a záplat operačného systému. Týka sa to aj internetového prehliadača a všetkých aplikácií.

Prečo? Hackeri ako prvé hľadajú známe zraniteľnosti v neaktualizovaných systémoch, čiže bezpečnostné diery, a tie treba plátať.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

www.dataprotection.gov.sk

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

www.cybercompetence.sk

ISBN 978-80-69011-19-9

Verzia V.1