

Silné heslo nestačí: Dnes je dôležité udržať si v bezpečí aj e-mail

16.7.2026 - Miroslav Mudroň | Zajtra studio spol.

Silné heslo samo o sebe nevyrieši bezpečnosť vášho účtu, ak útočník pozná váš primárny e-mail alebo v službe chýba druhý overovací faktor. Pri únikoch databáz sa totiž často nešíri len heslo, ale aj e-mailová vaša adresa, ktorá funguje ako univerzálny identifikátor naprieč službami. Informácie poskytol portál AndroidAuthority.

Bezpečnosť online účtov dáva väčší zmysel v troch vrstvách: e-mail, heslo a dvojfaktorové overenie. Ak zlyhá jedna časť, zvyšné dve majú zabrániť tomu, aby sa kompromitácia rozširovala ďalej.

E-mail je najčastejšie podceňovaný prvok

Primárna e-mailová adresa je pre väčšinu služieb kľúčom prístupu k účtu: používa sa na registráciu, obnovu hesla aj komunikáciu so supportom. Práve preto je problém, že ju bežne rozdáваме „všade“ a často bez väčšieho premýšľania.

Často sa spomínajú e-mailové aliasy. Ide o adresy, ktoré preposielajú poštu na váš hlavný e-mail, no samotnú primárnu adresu neodhalia. Ak alias unikne v databáze konkrétnej služby, dá sa jednoducho vypnúť a nahradiť novým, bez toho, aby ste museli meniť hlavný e-mail na všetkých účtoch. Aj takýmto štýlom môžete vašu adresu ochrániť.

Zdroj: Tomáš Kanálik

Hovorí sa tiež, že e-maily sú z povahy veci "verejnejšie" než heslá – často sa zadávajú a ukladajú ako bežný textový identifikátor. A keďže primárny e-mail sa mení ťažko (kvôli naviazaným účtom), jeho ochrana má vysokú hodnotu. Medzi príkladmi služieb pre aliasy patria platformy SimpleLogin a DuckDuckGo.

Heslá stále rozhodujú, ale len ak nie sú opakované

Aj keď sa dnes veľa hovorí o komplexnosti, ako napríklad využitie kombinácie veľkých/malých písmen, čísiel a špeciálnych znakov, v praxi zlyháva najmä opakované používanie rovnakého hesla alebo jeho drobných variácií. Únik z jednej služby sa potom ľahko zmení na reťazový prienik do ďalších účtov.

Riešením sú správcovia hesiel, ktoré vytvoria a uložia unikátne heslá pre každú službu. Používateľ si pamätá iba hlavné heslo, pričom kompromitácia jedného účtu automaticky neznamená ohrozenie všetkých ostatných. Ide tu aj o praktický bezpečnostný efekt: ak heslá nevypisujete ručne, znižujete šancu, že naletíte na phishingovej stránke, ktorá sa tvári ako originál.

Zaujímavým prepojením je, že niektorí moderní správcovia hesiel už vedia ponúknuť aj aliasy, takže pri registrácii kombinujete skrytý e-mail a unikátne heslo bez skákania medzi viacerými službami. A ak vás odrádza predstava zmeny stovky hesiel, odporúča sa takýto postup: meniť ich priebežne pri bežnom prihlasovaní do jednotlivých služieb.

Dvojfaktorové overenie je záchranná sieť pri úniku e-mailu aj hesla

Aj keď si dáte pozor na e-mail aj heslá, stále existuje scenár, keď sa oboje dostanú von na svetlo sveta. Práve tu dáva najväčší zmysel 2FA (dvojfaktorové overenie), ktoré pridáva ďalší krok pri prihlásení – jednorazový kód, TOTP alebo fyzický bezpečnostný kľúč.

Google Pixel 10a | Zdroj: Lenka Ivančíková

Bezpečnostné kľúče patria medzi najbezpečnejšie možnosti overenia druhým faktorom. Praktickejšou a dostupnejšou alternatívou sú autentifikačné aplikácie generujúce TOTP kódy v krátkych intervaloch. Ja osobne používam Authenticator od spoločnosti Google a ten funguje na jednotku.

SMS kódy sú vnímané ako slabšie riešenie, no stále lepšie než žiadne 2FA. Dôležité je mať overenie zapnuté, aby ste vedeli zastaviť prihlásenie aj v prípade, že útočník už pozná vaše prihlasovacie údaje, a zároveň získali čas na zmenu hesla.

Tri vrstvy, jeden cieľ: znížiť dopad únikov a útokov

Pointa je jednoduchá, jednotlivé nástroje riešia ten istý problém z rôznych strán. E-mail aliasy obmedzia šírenie vášho primárneho identifikátora, správca hesiel odstráni opakované heslá a 2FA pridá bariéru aj v situácii, keď prvé dve vrstvy zlyhajú.

Nemali by ste prehliadnuť:

- **Disney+ by mohlo nasledovať Spotify. Príští by mala verzia s reklamami**
- **Motorola Edge 70 Max: 7 100 mAh batéria a Snapdragon 8 Gen 5?**
- **Nepoužívate pri počítači okuliare s blokováním modrého svetla? Toto by ste mali vedieť**

Je potrebné podotknúť, že spoliehať sa len na jednu časť môže vytvoriť falošný pocit bezpečia. Ak sú však všetky tri vrstvy nastavené správne, fungujú ako záloha jedna pre druhú – keď jeden prvok padne pri úniku alebo phishingu, ďalší stále drží útočníka mimo účtu.

<https://www.mojandroid.sk/silne-heslo-nestaci-dnes-je-dolezite-udrzat-si-v-bezpeci-aj-e-mail>