

Ako odhaliť, kto predal váš e-mail a zastaviť spam skôr, než príde

30.6.2026 - Lenka Ivančíková | Zajtra studio spol

Primárna e-mailová adresa je často rovnaká roky a postupne ju zaregistrujete v banke, na úradoch či vernostných programoch. Problém je, že tú istú adresu zároveň bežne zadávame aj pri jednorazových nákupoch, pri registrácii do verejnej Wi-Fi a podobne, čím ju zbytočne vystavujeme ďalším databázam.

E-mail dnes funguje aj ako identifikátor, cez ktorý môžu uniknúť citlivé dáta, je použitý na marketingové zoznamy a profilovanie. Riešením je systém e-mailových aliasov. Teda samostatných adries, ktoré preposielajú poštu do vašej schránky, no v prípade potreby ich viete jednoducho vypnúť bez zásahu do hlavného účtu.

Spam sa dá zastaviť skôr, než sa dostane do schránky

Bežná ochrana proti spamu je najmä reaktívna: poskytovateľ filtruje prichádzajúce správy a snaží sa odhadnúť, čo sú legitímne a čo nie. Výsledkom býva kombinácia dvoch problémov. Dôležité e-maily občas skončia v spame a naopak, lepšie pripravený phishing sa môže dostať priamo do doručenej pošty.

Ak sa vaša hlavná adresa dostane do spamovej siete, čaká vás nekonečné blokovanie odosielateľov a tvorba pravidiel, ktoré sa dajú obísť drobnými zmenami domén. Pri aliasoch sa dá hra otočiť: na každú službu alebo typ registrácie použijete samostatnú adresu (napríklad pre odbery, newslettery či konkrétny e-shop).

Keď sa konkrétny alias začne zneužívať, dá sa deaktivovať jedným prepínačom v správe aliasov. Správy poslané na vypnutú adresu sa zahodia na úrovni servera, nedostanú sa do inboxu ani do spamu, a odosielateľovi príde informácia o nedoručení. Namiesto čistenia jedného kompromitovaného "potrubia" tak vypínate iba ten vstup, ktorý "začal tiecť".

Nastavenia aliasov v Google Workspace | Zdroj: Lenka Ivančíková

Alias pomôže vystopovať únik dát ku konkrétnej službe

Pri náhlom náraste podozrivých marketingových e-mailov alebo phishingu je v klasickom nastavení prakticky nemožné zistiť, odkiaľ sa adresa dostala do nesprávnych rúk. Po rokoch používania jedného e-mailu totiž môže ísť o desiatky až stovky rôznych aplikácií, obchodov a služieb.

Ak má každá firma unikátny alias, zdroj problému sa dá identifikovať okamžite. Stačí pozrieť, na ktorú adresu podvodná alebo nevyžiadaná pošta prišla. Ak bol alias vytvorený výhradne pre konkrétneho predajcu a neskôr naň začnú chodiť cielené podvody, máte jasný signál, že dáta sa z tejto strany posunuli ďalej (predaj dát alebo neohlásený únik).

V praxi to vytvára aspoň základnú mieru zodpovednosti. Alias môžete vypnúť a zároveň máte konkrétny podklad na to, aby ste problém nahlásili priamo danej službe.

Menší dosah incidentov a slabší základ pre profilovanie

Únik databázy neznamená len riziko pre jeden účet. Útočníci bežne skúšajú uniknuté kombinácie e-mailov a hesiel naprieč ďalšími službami (credential stuffing), vrátane finančných a poisťných portálov. Aj keď používate unikátne heslá, univerzálna e-mailová adresa im stále dáva polovicu prihlasovacích údajov pre celý váš online život.

S aliasmi sa dopad zúži: ak unikne databáza konkrétneho e-shopu, unikne len e-mail, ktorý existuje iba pre tento e-shop. Útočník ho nevie použiť na hľadanie vašich účtov inde, pretože rovnaká adresa sa v ďalších službách nenachádza. Kľúčové účty (napríklad hlavný e-mail alebo banka) sa tak dajú držať mimo dosahu menej bezpečných registrácií na fórach, hrách či drobných službách.

Podobný efekt má alias aj voči reklamnej personalizácii. Reklamný ekosystém sa opiera o spájanie identity naprieč aplikáciami a platformami a e-mail sa používa ako stabilný identifikátor, ktorý sa dá prepájať aj cez databázy sprostredkovateľov. Ak však pri každej interakcii používate inú adresu, databázy sa nevedia jednoducho zlúčiť cez rovnaký e-mail, čím sa profilovanie výrazne oslabí.

Proton mail aliasy | Zdroj: Proton.me

Ako s aliasmi začať a ako ich použiť na poriadok v inboxe

Prechod na aliasy nemusí znamenať vlastný mail server ani zložitú konfiguráciu. Je viac možností:

- vlastná doména + služba na maskované adresy (SimpleLogin, AnonAddy)
- Google Workspace: natívne aliasy (v zdroji spomínaný limit 30)
- Proton Mail a Apple: aliasy ako súčasť prémiových služieb

Štandardný Gmail podporuje len tzv. "plus adresovania", teda pridania **+text** za meno účtu (napríklad vasemenom+eshop@gmail.com). Pošta dorazí do rovnakej schránky, no nejde o skutočný alias, pretože vaša hlavná adresa zostáva viditeľná.

Spoločným menovateľom je, že alias vytvoríte rýchlo v administrácii. Priradíte mu popis a začnete ho používať pri registráciách bez toho, aby ste museli naraz meniť e-mail na všetkých existujúcich účtoch.

Pri nových registráciách si vždy vytvorte nový alias a existujúce účty meňte priebežne, keď sa do nich najbližšie prihlásite. Odporúčame začať kritickými službami, ako sú bankové aplikácie a hlavné sociálne siete. Okrem bezpečnosti sa aliasy dajú využiť aj na poriadok v pošte. Napríklad presmerovať newslettery a promo do separátnej, nízkoprioritnej schránky, zatiaľ čo osobné a pracovné aliasy necháte padať priamo do hlavného inboxu.

<https://www.mojandroid.sk/ako-odhalit-kto-predal-vas-e-mail-a-zastavit-spam-skor-nez-pride>