Nepodceňte význam silného hesla

BEZPEČNOSŤ

Slovákom odcudzili účty na Facebooku aj Instagrame. Zmeňte si heslo a skontrolujte e-mail, využívajte dvojfaktorovú autentifikáciu.

Alžbeta Harry Gavendová ©hn
alzbeta.gavendova@mafraslovakia.sk

Overte si, či využívate platnú e-mailovú adresu na prihlasovanie do rôznych služieb. SNÍMKA: REUTERS

Opakovanie – matka múdrosti. Tak znie jedno z kategórie klišé príslovní, no treba si ho opäť pripomenúť. Je totiž načase oprášiť prihlasovacie údaje, teda meno a heslo k vašim sociálnym sieťam, e-mailom či iným službám. Len pred pár dňami obletela svet správa, že hackeri majú k dispozícii momentálne 3,2 miliardy e-mailov a hesiel na jednom mieste.

Únik COMB

Reč je o doteraz najväčšom kompiláte uniknutých prihlasovacích údajov Combination of Many Breaches, teda COMB. Tento súbor dát nazývali svetové médiá aj „matkou všetkých únikov“, keďže išlo o momentálne najväčší známy zoznam svojho druhu. Sú v ňom pekne pohromade doteraz uniknuté údaje. „V nových záznamoch je podľa vyjadrenia analytikov len približne 17 percent nových dát, ktoré sa podarilo decryptovať a ktoré ešte údajne neboli zverejnené,“ vysvetľuje bezpečnostný expert Lukáš Štefanko zo spoločnosti ESET. Na porovnanie, doteraz bol považovaný za najväčší únik hesiel Breach Compilation z roku 2017, keď sa na čiernom trhu objavilo 1,4 miliardy prihlasovacích údajov.

Nový COMB čerpá informácie aj z tohto úniku, plus pridáva milióny ďalších uniknutých informácií a spolu tak vznikla najväčšia databáza, aká je známa. Situácia sa podľa všetkého týka drvivej väčšiny používateľov a experti odporúčajú zmeniť si heslá vo vašich službách, kde využívate staré známe e-mailové adresy. Upozorňujeme, že únik hesiel neznamená okamžité hacknutie vášho účtu. Niekto by sa musel zamerať konkrétne na vás a skúšať heslo z databázy. Automatizované systémy by sa však o to mohli pokúsiť. Častým problémom navyše býva fakt, že používatelia využívajú rovnaké e-mailové adresy a heslá do rôznych služieb. V tom prípade sa napríklad pri získaní hesla od LinkedInu môže útočník dostať aj do Google a Gmail účtu.

Problém s Facebookom

Len krátky čas po zverejnení informácií o COMB sa na Slovensku aktuálne stretávame s odcudzovaním facebookových účtov, teda používateľských profilov na Facebooku. Zatiaľ nie je jasné, či tieto udalosti spolu súvisia, no opäť sme pri téme sile hesiel, aktualizácie prihlasovacích údajov i opatrnosti na sociálnych sieťach. Po tom, ako sa o svojej skúsenosti s pokusom odcudziť účet na Facebooku podelil so svojimi čitateľmi redaktor portálu MojAndroid.sk Miroslav Schwamberg, do diskusie sa mu začali ozývať čitatelia. Tých spája kuriózna záležitosť. Majú svoj e-mailový účet na Azete. Podstatou je, že množstvo používateľov ešte v čase zakladania profilu na Facebooku využilo e-mail Azetu. Medzitým však vo veľkej miere nastúpil na scénu Google, ktorý ponúkal svojho e-mailového klienta Gmail. Obrovské množstvo používateľov tak prešlo na Gmail, svoj facebookový účet však mali stále prihlásený pod registračnými údajmi v podobe e-mailu z Azetu. Ak sa však podľa podmienok prevádzkovateľa neprihlásili viac ako 36 mesiacov do účtu v Azete, ich e-mail sa po tomto čase stal neplatným.

Ak sa útočníci dostali k takémuto zoznamu starých facebookových účtov s Azetom, mohli napríklad už iba vytvoriť nový e-mail s rovnakým názvom pred zavináčom – a pri prihlásení na Facebooku stlačiť „Zabudol som heslo“. Odoslalo ho jednoducho na tento staronový e-mail, avšak už s novým majiteľom. Tento poskytovateľ totiž dáva možnosť vytvoriť po určitom období nový e-mail s rovnakým menom. A tak útočník mohol dostať do schránky e-mail na obnovenie hesla a stal sa majiteľom účtu na Facebooku. Celý problém s odcudzovaním účtov na Facebooku či Instagrame sa však, samozrejme, neviaže na Azet. Navyše Schwamberg mal napríklad e-mailový účet na Azete aktuálny, a tak vďaka linke podpory problém nakoniec vyriešil.

Žiadosť o priateľstvo

Redaktor HN Radoslav Petrík sa tiež stal obeťou. Má však inú skúsenosť a na prihlásenie do Facebooku a Instagramu využíva Gmail. „Prišlo mi upozornenie, že moju žiadosť o priateľstvo potvrdil neznámy muž na Facebooku, a pritom som žiadne žiadosti neposielal. Po kliknutí na toto upozornenie som zistil, že z Facebooku som odhlásený,“ vysvetľuje. Následne sa ukázalo, že jeho účet bol zablokovaný z dôvodu porušenia podmienok používania. „Na svoj Facebook som pritom už pekný piatok nič nepridával. Podal som odvolanie na preskúmanie, na čo mi bolo pomerne rýchlo zo strany sociálnej siete automaticky odpísané, že účet bol natrvalo zablokovaný s tým, že aj po preskúmaní nie je možné účet odblokovať.“

Dvojfaktorové overenie

Zatiaľ nevieme s istotou povedať, či sme svedkami súvisiacich systematických útokov. Faktom však je, že aktualizáciou svojich prihlasovacích údajov nič nepokazíte. Štefanko odporúča navštíviť stránky Haveibeenpwned.com alebo Cybernews.com, kde si môžete skontrolovať, či bola nejakým spôsobom vaša e-mailová adresa kompromitovaná. Ak áno, odporúča zmeniť si heslo i heslá k ďalším službám, ktoré v spojení s ňou využívate. V lepšom prípade vám môžu chodiť na e-mail spamy či pokusy o phishing, v horšom prípade by sa niekto mohol zmocniť vášho účtu. Tiež sa uistite, či v službách a na sociálnych sieťach používate platné e-mailové adresy. Ak nie, čím skôr si tieto údaje aktualizujte a nezabudnite ani na nové heslo.

„Viacero používateľov svoje heslo nechce meniť, pretože ho používa na viacerých účtoch už roky a modifikuje časom len minimálne,“ vysvetľuje základnú chybu Vladimír Palečka, expert na kyberbezpečnosť spoločnosti Aliter Technologies. „Heslo by sme z bezpečnostných dôvodov mali meniť minimálne raz za pol roka. Silné a unikátne heslo je kľúčom k zabezpečeniu svojich dát.“ Ideálom je v kombinácia veľkých a malých písmen, znakov a čísel. Zrejme najrozumnejším riešením je však dvojfaktorová autentifikácia. Je to nástroj, ktorý rozširuje tradičné využitie hesla. „To znamená, že okrem bežného stupňa overenia cez heslo pridávate ďalší stupeň overenia. Tento druhý faktor pritom môže byť náhodne vygenerovaný kód, ktorý vám príde esemeskou na mobil a je ho potrebné zadať pri prihlásení.“ Využiť však môžete aj mobilnú aplikáciu, ako je napríklad Google Authentificator, ktorý je k dispozícii pre mobilné zariadenia s operačným systémom Android aj iOS.

Dvojfaktorové zabezpečenie sa používa aj pri internet bankingu či online nakupovaní, no nájdete ho už dávno aj práve v rámci prihlasovania na Facebook, Instagram či do vášho Google účtu a Apple ID. Ak útočník zistí vaše prihlasovacie údaje, stále mu bude chýbať „druhý faktor“ na overenie totožnosti a vpustenie do vášho účtu. Mobilný telefón, prostredníctvom ktorého sa vďaka náhodnému kódu autorizujete dodatočne, máte pri sebe len vy. Bohužiaľ, vo svete sú i prípady, keď bolo obídené aj dvojfaktorové overenie. To už by ste sa však museli stať terčom poriadneho útoku či vírusu. Momentálne je to stále rozumné riešenie a vyšší stupeň zabezpečenia ako len heslo.

ZÁKLADY BEZPEČNÉHO POUŽÍVANIA SOCIÁLNYCH SIETÍ OD SPOLOČNOSTI ESET:

1. Majte vždy aktualizovaný operačný systém a bezpečnostný softvér.
2. Vytvorte si silné dlhé heslo a pre každú platformu používajte jedinečné heslo.
3. Chráňte svoje kontá dvojfaktorovou autentifikáciou.
4. Používajte sociálne siete cez zabezpečený prehliadač alebo oficiálne aplikácie a cez zariadenia a siete, ktoré poznáte.
5. Nastavte si čo najstriktnejšie nastavenia súkromia.
6. Zverejňujte minimum súkromných informácií o sebe a svojich blízkych.
7. Nepridávajte si medzi priateľov ľudí, ktorých nepoznáte.
8. Neklikajte na všetko, čo sa objaví na sociálnych sieťach. Riaďte sa pravidlom dvakrát meraj, raz rež.
9. Nezapájajte sa bezhlavo do akýchkoľvek aktivít promovaných online. Sledujte len overené stránky a predajcov.
10. Hlavné pravidlo: „Ak narazíte online na niečo, čo vyzerá až príliš dobre na to, aby to bolo skutočné, tak to pravdepodobne skutočné nebude.“

(Zdroj: ESET)

MOBILNÉ TECHNOLÓGIE

Nefunkčný fotoaparát pod displejom ukryjú do rámčeka

Nový patent značky OnePlus ukazuje ďalší spôsob, ako vyriešiť predný fotoaparát tak, aby nerušil plochu displeja. Zmenšia ho natoľko, že sa zmestí aj do tenkého rámika. Výrobca OnePlus si nedávno totiž nechal patentovať dizajnovú metódu, ako umiestniť prednú selfie kameru do tenkého rámika nad displejom. Jeho riešenie je údajne lacnejšie ako priestrel displeja či nová integrácia fotoaparátu pod displej telefónu. Zatiaľ je to len patent a na prípadnú praktickú ukážku si však musíme počkať.

Samozrejme, ponúka sa otázka – nikomu inému to ešte nenapadlo? Keď sa v minulosti spustila honba za čo najtenšími rámčekmi okolo displeja, tak by sa z logiky veci mal zmenšovať aj fotoaparát, aby sa stále vošiel a „nezacláňal“ v displeji. Realita je iná.

Snímač v displeji

Optika fotoaparátu a jeho snímač potrebujú určité miesto na to, aby robili to, čo majú. Výrobcovia radšej vymysleli spôsob, ako jeho súčasné rozmery napasovať do plochy displeja, než sa pokúsiť ho zmenšiť.

Jediný, kto pri fotoaparáte v klasickom rámčeku (nie výreze či priestrele) zostal, je výrobca Sony. Avšak jeho modely majú predsa len na dnešnú dobu citeľne širší rámček nad displejom. OnePlus oproti tomu dúfa, že kompletný hardvér fotoaparátu prispôsobia tak, aby sa vošiel do súčasných, asi milimeter až dva milimetre tenkých rámčekov.

Nastolenie trendu

Ak sa to firme podarí, možno sa strhne trend čelných fotoaparátov skôr týmto smerom. Selfie snímače integrované pod displej už síce v prvej generácii dorazili na trh v podobe ZTE Axon 20 5G, avšak stále robia kompromisy napríklad v hustote pixelov v mieste, kde je fotoaparát, aby bolo cez ne lepšie vidieť. Výsledky nie sú ani v tomto prípade také dobré ako v prípade klasických fotoaparátov vo výrezoch. Navyše je takéto riešenie aj drahé na výrobu.

Poddisplejové fotoaparáty majú byť však jedným z hlavných trendov tohto roka. Je tak otázne, nakoľko ich výrobcovia dokážu zlepšiť a zároveň tiež zlacniť ich produkciu. Ak sa však po nich aj tento rok zľahne zem, je možno OnePlus na správnej ceste.

iDnes.cz/oma

OnePlus sa netrápi s fotoaparátom pod displejom. SNÍMKA: LETSGODIGITAL.COM