6 korakov, kako dodatno poskrbeti za varnost svojega Google računa

Uporabniki spleta imamo pomembne račune, ki jih moramo zaščititi in imamo POMEMBNE račune. Vaš Googlov račun zagotovo spada pod to drugo kategorijo. Samo pomislimo, koliko stvari je vezanih na dotični "sign-in": vaša elektronska pošta, dokumenti, vaše fotografije, datoteke, mogoče celo kontakti, tekstovna sporočila, zgodovina lokacij itd. Če torej uporabljamo Android, lahko milo rečeno označimo Googlov račun za "občutljivega". Ne glede na to, ali uporabljate Google v poslovne ali privatne namene, poskrbeti morate, da zaščitite karseda vse informacije, ki so vezane na ta račun.

Pomembno se je zavedati, da geslo, ki ste si ga pred nekaj leti izmislili v nekaj sekundah, ni dovolj, da lahko povemo, da smo popolnoma varni. Dejstvo je, da za Googlovim računom stoji ogromna količina osebnih podatkov in zgolj zaščita z geslom je prvi korak na poti do večje varnosti. Vzemite si 10 minut časa in preglejte spodaj opisane korake, ki nam lahko pomagajo pri povečanju varnosti Googlovega računa.

1. korak: Preverite moč gesla Google računa

Začeli bomo z nečem, kar se zdi samoumevno, vendar še kako pomembno - zgoraj omenjeno **geslo računa**.

- Ali uporabljate geslo, ki bazira na vašem imenu, imenu partnerja ali otrok, vašeg rojstnega datuma, naslova bivanja, ali na čemerkoli drugem, kar je vezano na vas?
- Ali je vaše Google geslo enostavna beseda, ali vzorec črk, ki ga je lahko uganiti?
- Je vaše Google geslo kratko - krajše od osem znakov?
- Ali uporabljate geslo Google računa (ali kakšno variacijo tega) za vpis v katerokoli drugi aplikacijo, spletno stran, ali storitev?

Če je odgovor na katero od zgornjih vprašanj pritrdilen, uporabite to POVEZAVO in takoj spremenite vaše geslo - kot verjetno veste je za gesla vedno najbolje, če so ta dolga, kompleksna in ne vsebujejo nobenih osebnih podatkov, ki jih lahko odkrijemo na hiter in enostaven način.

2. korak: Vašemu Google računu dodajte dodatno plast zaščite

Ne glede na to, kako zaščiten je vaš Google račun, vedno obstaja možnost, da pride do zlorabe. S pomočjo dvofaktorske avtentikacije lahko stopnjo zaščite precej povečate, s tem pa povzročite potencialnim hekerjem kar nekaj težav. Dvofaktorska avtentikacija je zelo učinkovit način, da zavarujete svoje digitalne račune. Predstavlja dodatno raven zaščite, saj združuje geslo (nekaj, kar poznate) in drugi faktor, npr. enkratno geslo ali obvestilo, ki ga storitev pošlje na vaš mobilni telefon (nekaj, kar imate v lasti).

Ne glede na izbran način dvofaktorske avtentikacije je to dodatna zaščita vašega računa, ki močno oteži kakršenkoli poizkus vdora, tudi, če ta oseba pozna vaše geslo. Če dvofaktorske avtentikacije pri Googlovem računu še ne uporabljate, obiščite to POVEZAVO in sledite navodilom.

*(**se nadaljuje**)*

6 korakov, kako dodatno poskrbeti za varnost svojega Google računa (2. del)

3. korak: Pripravite se na dokazovanje vaše identitete

Če Google kdajkoli zazna potencialno sumljivo aktivnost pri uporabi vašega računa, lahko od vas zahteva verifikacijo identitete, preden vam dovoli vpis v račun. Če že dolgo časa (ali še nikoli) niste pogledali v nastavitve verifikacije računa, obstaja velika verjetnost, da potrebni podatki manjkajo oz. so že potekli. Vzamite si minuto in odprite Googlovo stran z varnostnimi nastavitvami in odprite sekcijo "Načini preverjanja, da ste to res vi". Tam boste videli različne načine reverjanja, ki jih lahko uporabijo, če se morajo prepričati, da ste to res vi:

- Telefonska številka za obnovitev;
- e-poštni naslov za obnovitev;
- varnostno vprašanje.

Če pri kateri od opcij številka oz. podatek ni pravilen, ga čim prej spremenite.

4. korak: Preglejte "third-party" storitve, ki imajo dostop do vašega računa

Ko namestite oz. začnete z uporabo aplikacije, ki je na kakršenkoli način povezana z Googlom - na vašem telefonu, računalniku, ali znotraj Googlovih storitev, kot sta Gmail in Docs - ta aplikacija dobi določeno raven dostopa do podatkov na vašem Googlovem računu.

Odvisno od primera, vendar to lahko pomeni, da lahko aplikacija vidi nekatere aktivnosti znotraj specifičnih Googlovih storitev; recimo vidi lahko pošto v Gmailu, zapiske v Google Drivu, ali Google Calendar; ali pa lahko vidi čisto vse znotraj Googlovega računa. Torej naš nasvet je, da skrbno pregledate vse "third-party" storitve, ki imajo dostop do vašega računa in se seznanite z informacijami, do katerih imajo dostop. Na tej POVEZAVI lahko vidite vse povezane storitve.

Če izbranim aplikacijam zaupate in jih poznate, seveda lahko imajo dostop do določenih podatkov, vendar vam svetujemo, da seznam "third-party" storitev obiskujete redno in ga tudi redno posodabljate s pravicami dostopa do vaših podatkov.

5. korak: Preglejte vse naprave, ki imajo dostop do vašega računa

Poleg zgoraj izpostavljenih aplikacij, v katere smo se z Google računom vpisali preko večih fizičnih naprav, so ravno te tiste, na katere moramo biti prav tako pozorni. Pogosto se zgodi, da ko se enkrat vpišemo na sistemski ravni, naprava ostane povezana z našim računom in ima do njega dostop ne glede na to, koliko časa je minilo od takrat, ko smo napravo in aplikacijo dejansko zadnjič uporabili.

Nadzor na napravami, ki imajo dostop do Google računa, lahko ponovno prevzamemo na tej POVEZAVI. Če na seznamu naprav opazite kakšno, katero ne uporabljate več, ali je celo ne prepoznate, kliknite na ikono s tremi pikami in račun iz naprave izpišite.

6. korak: Preglejte dovoljenja aplikacij na vašem telefonu

Za vas imamo še eno pomembno napotilo glede uporabe aplikacij: Če uporabljate Android, nekatera dovoljenja na ravni sistema - kot so tista povezana s kontakti in koledarjem - lahko močno vplivajo na upravljanje dostopov do podatkov vezanih na Google račun. Zapomniti si je potrebno, da storitve, kot sta Google Contacts in Google Calendar sinhronizirajo podatke med telefonom in oblakom. Na vašem telefonu najdete sekcijo Zasebnost, ki se po navadi nahaja v sistemskih nastavitvah in poiščete "Upravitelj dovoljenj" (ali nekaj podobnega, odvisno od verzije Androida, ki jo uporabljate). Tam lahko najdete različne tipe dovoljenj in pogledate, katere aplikacije imajo avtorizacijo za dostop.