**Zašto je potrebno imati snažnu lozinku?**

Snažna lozinka jedan je od glavnih sustava zaštite vaših podataka. Ako ste jedni od onih koji vole postaviti jednostavnu lozinku, ostaviti lozinku koja je došla s uređajem ili možda volite adrenalin pa ostavljate sustave dostupne bez lozinke, ne čudite se ako postanete žrtva: **gubitka kontrole nad svojim računalom, krađe podataka i/ili identiteta, gubitka privatnosti ili pak ucjene.**

Prema izvješću [Verizona](https://www.verizon.com/business/resources/reports/dbir/%22%20%5Ct%20%22_blank) o povredi podataka, **80% povreda uzrokovano je lošim ili ponovno korištenim lozinkama.** Ovaj podatak će vas manje čuditi kad pročitate statistike o ljudskim navikama vezanim uz lozinke. [IDAgent](https://www.idagent.com/blog/10-facts-about-passwords-that-you-need-to-see-now/) navodi da: čak 60% ljudi koristi jednake lozinke za prijavu u različite sustave, 13% ljudi koristi jednaku lozinku za sve svoje sustave i uređaje, 48% zaposlenika koristi jednaku lozinku za privatne i poslovne račune, a gotovo polovica prilikom promjene lozinke promijeni ili doda samo jedan znak.

**Kako onda kreirati kvalitetnu i snažnu lozinku?**

Da odmah naglasimo**, ne postoji savršeni recept za lozinku** i 100% usuglašeno mišljenje oko pravila dobre lozinke, stručnjaci imaju različita mišljenja i stavljaju naglasak na različite elemente lozinke. Tako jedni kažu da je najbitnija duljina lozinke, drugi se fokusiraju na složenost i korištenje različitih znakova kako bi se izbjeglo korištenje riječi iz rječnika, treći smatraju da je bitna duljina lozinke, ali da se mogu koristiti fraze koje su lako pamtljive i tako se rasprava nastavlja i vi možda u cijeloj toj priči više ne znate koga poslušati.

Kod odabira lozinke i zaštite u kibernetičkom prostoru uvijek se vodi bitka između komocije (lakoće korištenja i pristupa sustavu) i razine zaštite. **Što je viša razina zaštite to je manje komocije.** Zato sami morate odlučiti na koju stranu vage želite pomaknuti težište, tj. procijeniti „koliko vam je važno spriječiti pristup određenim podacima ili sustavima osobama koje taj pristup ne bi trebale imati?“

Kako bismo vam olakšali odluku, donosimo vam par savjeta za kreiranje dobre lozinke:

**Kako onda kreirati kvalitetnu i snažnu lozinku?**

**Stavite prioritet na duljinu lozinke, minimalni 10 znakova (bolje 14 ili 16 znakova).**

**Kombinirajte slova (velika i mala), brojeve i znakove.**

**Ne koristite iste lozinke za različite sustave, pogotovo ne za osobne ozbiljne račune.**

[**Ne koristite česte fraze ili slijedove znakova (123456789, qwertz, asdfgh i sl.)**](https://www.naivci.hr/#Galerija)**.**

**Ne dijelite lozinke sa prijateljima.**

**Ne šaljite lozinke mailom, porukama i drugim nesigurnim kanalima komunikacije.**

**Ako već zapisujete lozinke na papir, ne ostavljajte takve zapise na vidljivim mjestima.**

**Ako možete, ne koristite prave riječi (lozinke nasumičnih znakova su ipak malo sigurnije).**

**Izbjegavajte povezivanje na javni WiFi.**

**Koristite password managere / upravitelje lozinkama.**

**Često mijenjajte lozinke.**

**Ako imate mogućnost, uključite dvostruku autentifikaciju!**

**Provjerite je li vaš račun već hakiran.**

Već neko vrijeme dobra lozinka nije nužno samo jedna riječ – možete upotrijebiti cijelu rečenicu koju ćete lakše pamtiti: DanasJeLijepDan9. **Recept**: Uzmite samo prva slova rečenice ili stiha koja ćete lako zapamtiti, a dodajte brojeve i velika slova. Primjer: Na planinama sunce sja, 20Npss13.

Sad kad ste pročitali savjete za dobru lozinku na vama je da ih primijenite u praksi. Ne želite se dovesti u situaciju gdje osoba koja ne bi trebala imati pristup vašim podacima po njima „njuška“ i potencijalno vam može naštetiti, bilo to financijski ili na neki drugi način.

**Bonus savjet:** iako na internetu postoje mnogi **servisi koji će vam izračunati snagu vaše lozinke nikako ne savjetujemo da svoju lozinku testirate na taj način.** Upisivanjem svoje lozinke u nepoznati servis riskirate da ona bude pohranjena u običnom tekstualnom obliku te bi tako jednog dana mogle biti prodane na crnom tržištu i iskorištene za zlonamjerne radnje. Ono što možete, je upisivanjem svoje mail adrese [provjeriti nalazi li se lozinka vašeg računa](https://www.cert.hr/cit0day) u nekoj od baza podataka koje su postale javno dostupne. Ako je tome slučaj svakako savjetujemo da promijenite lozinku tog računa.

Istraživanje je pokazalo da prosječan haker čak i lozinku od osam znakova – sastavljenu od brojeva, velikih i malih slova te posebnih znakova –  može probiti u roku od 39 minuta. Prije dvije godine za to mu je trebalo osam sati. Sve kraće ili manje složene lozinke može bez problema probiti bilo koji haker koji zna što radi, čak i ako koristi samo osnovnu opremu.

Za probijanje lozinke od 10 znakova sastavljene od brojeva, velikih i malih slova te posebnih znakova prije dvije godine trebalo je 5 godina, a danas je dovoljno 5 mjeseci.

S druge strane, prosječnom hakeru trebalo bi 438 bilijuna godina da probije lozinku od 18 znakova koja koristi kombinaciju brojeva, malih i velikih slova i simbola, tvrdi Hive Systems.

**Trik kako najlakše zapamtiti lozinku**

**Najčešće greške**

Korisnici čine nekoliko grešaka koje hakerima olakšavaju posao.

Osim što ne mijenjaju lozinke, odnosno koriste istu lozinku za više računa, često te lozinke zapisuju na papir i ostavljaju ga pored računala. Također, lozinke često čuvaju u mailovima na svojim e-mail računima.

Budući da je naporno pamtiti puno različitih lozinki, korisnici pokušavaju pronaći lozinke koje su im logične. Tako kao lozinke koriste imena članova obitelji, kućnih ljubimaca, datume rođenja, brojeve telefona ili jednostavno riječ 'lozinka'.

Često se koriste i programi koji nude korisnicima da umjesto njih pamte lozinke, poput [KeePassa](http://keepass.info/%22%20%5Ct%20%22_blank). Umjesto da pamte desetak različitih lozinki, korisnici moraju zapamtiti samo jednu - tog programa. Međutim, unatoč svim naporima, šanse su da će vam barem jednom u životu netko 'ukrasti' lozinku i 'upasti' u račun.

**Zlatna pravila dobre lozinke**

I što vam je onda činiti?

Stručnjaci za sigurnost dijele brojne savjete kako se zaštititi, osmisliti lozinku koju je teže 'probiti' odnosno kako spriječiti hakere da uopće pokušaju ući u račun.

1) **Zaboravite normalne riječi** - ako se vaša lozinka može pronaći u rječniku, zaboravite je. Većina programa koristiti velike baze riječi iz rječnika i pomoću njih pokušava otkriti lozinku.

2) **Nikad ne koristite istu lozinku dva puta** - zbog istog razloga zbog kojeg svaka brava ima svoj ključ, i svaki račun trebao bi imati vlastitu lozinku. Možda vam se ne čini bitnim to što imate istu lozinku na e-mailu i serveru za igrice, ali čim hakeri otkriju pukotinu u sigurnosti, zasigurno će je iskoristiti da dođu do što više podataka.

3) **Osmislite frazu** - neka vam lozinka bude fraza logična samo vama. Što dulja to bolje. Idealna bi bila dulja od 14 znakova. Prisjetite se omiljene rečenice iz knjige, filma ili pjesme i kao lozinku iskoristite samo prva ili posljednja slova pojedinih riječi.

4) **Zaboravite na gramatiku** - gramatički točne riječi, kao i one iz engleskog jezika najčešće su korištene kao lozinke. Radije izaberite riječ iz nekog manje raširenog jezika (hrvatski je dobar primjer) i krivo je napišite. Primjerice, umjesto 'obitelj' pišite 'obitlej'.

5) **Prepustite se slučaju** - za posebno osjetljive račune, poput bankovnih, potrebno je osmisliti lozinku koja će biti veoma komplicirana. Najjednostavniji način? Otvorite prazan dokument, položite ruke na tipkovnicu, ispraznite misli, zatvorite oči i udarajte kako vas je volja. Šanse su da će krajnji rezultat biti potpuno nesuvisao niz znakova, koje možete kopirati kao lozinku. Naravno, nemojte zaboraviti spremiti lozinku na sigurno mjesto, jer je zasigurno nećete moći ponoviti bez pomoći originalnog zapisa.

6) **Ignorirajte generička sigurnosna pitanja** - većina servisa nudi opciju podsjećanja na lozinku ako je zaboravite. Ponudit će vam nekoliko generičkih pitanja, na koja vi prilikom prve registracije odgovorite, a prilikom postupka obnove lozinke, oni tim odgovorima provjeravaju vaš identitet. No zbog brojnih društvenih mreža, do takvih je odgovora sve lakše doći. Puno je bolja solucija sam zapisati neko pitanje ili na generičko pitanje poput 'Ime vašeg prvog kućnog ljubimca?' odgovoriti frazom koja je samo vama poznata.

7) **Uključite dvostupanjsku verifikaciju** - kod nekih e-mail providera moguće je uključiti dvostupanjsku verifikaciju. To znači da će vam provider, nakon što ukucate lozinku, na mobilni telefon poslati niz brojeva (poput bankovnog tokena), koji je potrebno upisati kako bi se pristupilo računu. To je izvrsna zaštita ako vam netko otkrije lozinku i pokuša ući u račun.

8) **Koristite različite pretraživače (browsere**) - na taj ćete način otežati krađu lozinki za sve račune. Tako koristite jedan za neformalno surfanje, drugi za e-mail, treći za sigurne transakcije poput online kupnje ili e-bankinga.

9) **Pazite gdje upisujete svoje e-mail adrese** - tretirajte svoju e-mail adresu kao što biste tretirali svoju kućnu adresu. Ne ostavljajte je po forumima ili za različite natječaje. Radije otvorite e-mail adresu koja će vam koristiti samo za to. Na taj ćete način spriječiti da hakeri dođu do osjetljivih podataka koje možda imate na svojoj 'glavnoj' e-mail adresi.

I na kraju najvažniji savjet - mijenjajte lozinke redovito. To ne mora biti svaki tjedan ili svaki mjesec. Ali preporučuje se da barem svaka tri mjeseca promijenite lozinku na svom računu.

Zlu ne trebalo.

**Digitalni tragovi i elektroničko nasilje**



 **Kako onda kreirati kvalitetnu i snažnu lozinku?**

**Stavite prioritet na duljinu lozinke, minimalni 10 znakova (bolje 14 ili 16 znakova).**

**Kombinirajte slova (velika i mala), brojeve i znakove.**

**Ne koristite iste lozinke za različite sustave, pogotovo ne za osobne ozbiljne račune.**

[**Ne koristite česte fraze ili slijedove znakova (123456789, qwertz, asdfgh i sl.)**](https://www.naivci.hr/#Galerija)**.**

**Ne dijelite lozinke sa prijateljima.**

**Ne šaljite lozinke mailom, porukama i drugim nesigurnim kanalima komunikacije.**

**Ako već zapisujete lozinke na papir, ne ostavljajte takve zapise na vidljivim mjestima.**

**Ako možete, ne koristite prave riječi (lozinke nasumičnih znakova su ipak malo sigurnije).**

**Izbjegavajte povezivanje na javni WiFi.**

**Koristite password managere / upravitelje lozinkama.**

**Često mijenjajte lozinke.**

**Ako imate mogućnost, uključite dvostruku autentifikaciju!**

**Provjerite je li vaš račun već hakiran.**