4.

ZAŠTITITE SVOJE VIRTUALNE VRIJEDNOSTI

Baš kao što brinete o vrijednim predmetima u svom domu, tako biste trebali postupiti i s podacima koje virtualno pohranjujete - bilo da se radi o vašoj financijskoj evidenciji, skeniranju putovnice ili čak adresi ili telefonskom broju, važno je gdje pohranjujete svoje najcjenjenije osobne podatke i kako ih možete zaštititi.

Spot clean izvrstan je ako želite napraviti nekoliko brzih poboljšanja uz kavu. Potražite određene podatke koji se nalaze u vašoj e-pošti ili na drugim računima i izbrišite ih: skenove osobne iskaznice, bankovnih podataka ili podataka o zdravstvenom osiguranju, da nabrojimo samo neke. Ako vam kasnije zatreba nešto od spomenutog, uvijek isto možete ponovno preuzeti ili isprintati prije brisanja s računa e-pošte.

Dubinsko čišćenje temeljitije je i dobro ga je raditi jednom godišnje. Arhivirajte sve na svom računu e-pošte ili na društvenim mrežama, preuzmite podatke na računalo i izbrišite sadržaj računa da biste započeli iznova.

Savjet: Nemojte samo brisati - također ispraznite kantu za smeće i privremene datoteke!

Na vama je želite li sigurnosnu kopiju arhiva i dokumenata napraviti u oblaku ili ih spremiti na vanjski tvrdi disk ili USB. Bez obzira na to kako čuvate svoje podatke, pripazite da ih ne izgubite te da ih čuva snažna lozinka koja za vas ima smisla.

5.

PROSLIJEDI DALJE

Često se i lako zaboravlja da se web s razlogom naziva "mreža". **Svi smo povezani na mreži** putem različitih mreža, ne samo kao „prijatelji“ na društvenim mrežama, već i putem kontakata na našim računima e-pošte i fotografija koje dijelimo na mreži. Kada osigurate svoje račune, ojačate lozinke i očistite podatke, niste samo vi u prednosti - **svi s kojima ste povezani pomalo su sigurniji upravo zbog vašeg truda.**

Kada čistite račune e-pošte i društvenih mreža, razmislite što još možete preuzeti i izbrisati što bi moglo pomoći vašim prijateljima ili suradnicima: bankovni podaci vaše sestre, ključni kôd vašeg ureda ili sken putovnice vašeg sina samo su neke od evidencija koje bi vam mogle izazvati glavobolju ukoliko dođu u pogrešne ruke.

Prenesite dalje! Povećavanje vaše digitalne sigurnosti može biti jednostavno kroz slijeđenje nekoliko osnovnih koraka. Podijelite ovaj Komplet sa svojim prijateljima, obitelji ili suradnicima kako biste im pomogli u promijeni navika na načine koji za njih imaju smisla.

DATA DETOX KIT

POMAKNITE POSTAVKE

za zaštitu podataka

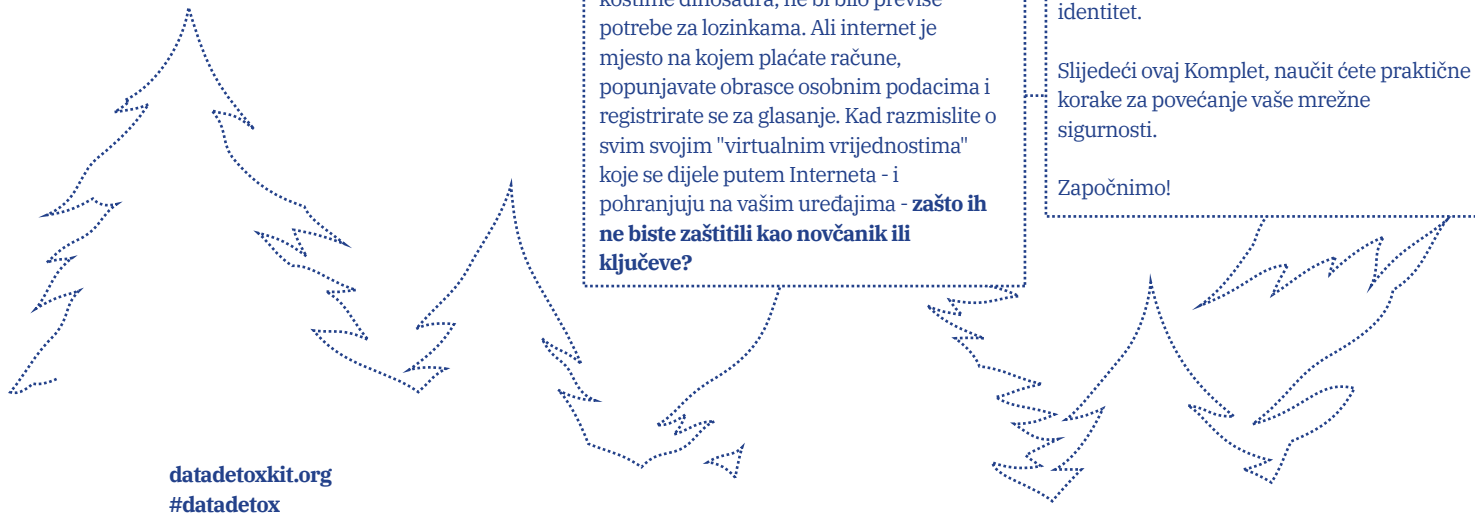
Kad bi internet bio samo mjesto na kojem se razmjenjuju slika pasa koji nose kostime dinosaura, ne bi bilo previše potrebe za lozinkama. Ali internet je mjesto na kojem plaćate račune, popunjavate obrasce osobnim podacima i registrirate se za glasanje. Kad razmislite o svim svojim "virtualnim vrijednostima" koje se dijele putem Interneta - i pohranjuju na vašim uređajima - **zašto ih ne biste zaštitili kao novčanik ili ključeve?**

Postoji jedan jednostavan način da drugima otežate pristup vašim virtualnim vrijednostima: **nemojte im olakšati pogađanje vaših lozinki.** Većini ljudi nisu potrebne posebne tehničke vještine da bi ušli na vaše račune - to mogu učiniti samo nagađanjem lozinki ili pokretanjem automatiziranog programa.

A nakon što uđu na jedan račun, mogu isprobati tu kompromitiranu lozinku na drugim računima, prikupiti podatke o vama i vašim navikama, preuzeti račune u vašem vlasništvu ili čak koristiti vaš digitalni identitet.

Slijedeći ovaj Komplet, naučit ćete praktične korake za povećanje vaše mrežne sigurnosti.

Započnimo!



Proizvod
TACTICAL TECH

Podržan od
Firefox

datadetoxkit.org
#datadetox

1.

ZAKLJUČAJ SVOJA DIGITALNA VRATA

Zaključavanje zaslona: lozinka, uzorak, otisak prsta ili ID lica koji upotrebljavate za pristup uređaju neke su od **najboljih obrana** protiv nekoga tko bi možda želio ući u vaš uređaj. Ali postoji puno različitih vrsta zaštite i možda će biti teško znati koja je prava za vas.

Ukoliko imate bilo kakvu bravu na telefonu, tabletu ili računalu, ona vam pruža veću zaštitu nego da nemate nikakvu bravu. I baš kao i različite vrste brava koje biste mogli staviti na vrata, **neke su brave zaslona jače od drugih.**

Od svih brava koje postoje, duge, jedinstvene lozinke su najjače. To znači da ako otključavate uređaj lozinkom, ona bi trebala sadržavati slova, brojeve i posebne znakove.

Recimo da koristite osnovni potez za otvaranje telefona. Možete polako povećati svoju sigurnost postavljanjem duge lozinke. Ili sada koristite zaključavanje uzorkom? Što kažete na to da svoj uzorak učinite dužim? Upotrebljavate 1234 kao svoj PIN? Što kažete na to da umjesto ove kombinacije, sedam puta bacite kockice i zapamtite taj PIN? **Mala promjena može uvelike doprinijeti zadržavanju kontrole nad vašim uređajima.**

2.

PUSTITE ONOG PRAVOG

Stvaranje vrhunskih lozinki je jednostavno. Sve što trebate je slijediti nekoliko osnovnih principa. Vaše lozinke trebaju biti:

Dugačke: **lozinke trebaju imati najmanje osam znakova. Još bolje? 16-20 znakova**

Jedinstvene: **svaka lozinka koju upotrebljavate - za svaku web stranicu - treba biti različita**

Nasumične: **vaša lozinka ne bi trebala slijediti logičan obrazac niti bi je trebalo lako moći pogoditi. Tu upravitelji lozinki postaju vrlo korisni.**

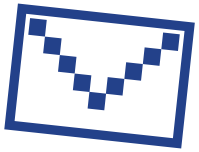
Najjače lozinke koriste kombinaciju slova, brojeva i posebnih simbola. Ovaj provjereni savjet čini jaču lozinku koju je teže pogoditi. Neki sustavi lozinki nažalost ne dopuštaju upotrebu posebnih simbola (poput @ # $% - = +), ali dovoljno duga kombinacija slova i brojeva ipak je bolja od kratke.

U idealnom slučaju, trebali biste koristiti namjenski upravitelj lozinki za generiranje i spremanje svih lozinki. Upravitelj lozinki - poput 1Password i KeePassXC, koje često preporučuju sigurnosni stručnjaci - u osnovi je aplikacija čija je jedina svrha zaštititi vaše vjerodajnice za prijavu i druge osjetljive podatke.

3.

DODAJ DRUGI KLJUČ

Postavljanje dvofaktorske autentifikacije (2FA) ili više faktorske autentifikacije (MFA) znači da čak i ako netko pronađe vašu lozinku, **vjerojatno neće imati dodatni faktor koji treba za ulaz.**



Pregledajte sigurnosne postavke svojih najčešće korištenih web lokacija i aplikacija da biste vidjeli možete li postaviti ovaj dodatni ključ. Započnite s najvažnijim - bilo kojim financijskim aplikacijama ili uslugama poput e-pošte koje upotrebljavate za oporavak ostalih računa.

Google:
Prijavite se na myaccount.google.com → Sigurnost → Potvrda u 2 koraka → Započnite

Facebook:
izbornik → Postavke → Sigurnost i prijava → Upotrijebi dvofaktorsku autentifikaciju

Savjet: Kada postavljate sljedeći sloj provjere, morat ćete odabrati drugi način potvrde da ste to vi. Pokušajte izbjegavati korištenje SMS-a (tekstualnih poruka poslanih na vaš telefonski broj) kao drugog čimbenika, samo u slučaju da izgubite telefon. E-pošta je obično pouzdanija opcija.