Budite na oprezu u sajber prostoru

Budite sajber svjesni

Budite na oprezu u sajber prostoru

Tehnologija je svuda. Postala je fundamentalni dio modernog života i zato je sada važnije nego ikad da budete oprezni u sajber prostoru.

Podaci koji čine svaki od naših digitalnih otisaka izuzetno su dragocjeni. Tužno, ali to je ono što ih čini glavnom metom sajber kriminala.

Sajber kriminalci i hakeri koriste mnoštvo različitih načina da dođu do naših podataka, pa može biti lako nasjesti na njihove lukave tehnike.

Iz tog razloga moramo biti na oprezu u sajber prostoru i praktikovati dobru sajber higijenu.

Pod sajber higijenom podrazumijevamo zaštitu od krađe i neovlašćenog pristupa uređajima koje koristimo, te podacima koje na njima čuvamo. Ovaj komplet korisnih alata pokazuje nam: kako da napravimo jače lozinke, kako da upravljamo svojim uređajima tako da nam pruže dodatnu sajber zaštitu, kako da održavamo svoje uređaje i ažuriramo najnoviji softver i kako da obezbijedimo svoje podatke izradom rezervnih kopija.

Sigurne lozinke

Snažne lozinke štite sve nas

Naše lozinke štite naše naloge i uređaje od štetnih sajber napada. One su važna bezbjednosna zaštita od potencijalnih prijetnji, tako da je važno odabrati jake lozinke.

Snažne lozinke ne moraju biti dugačke, niti komplikovane.

Često nam govore da naše lozinke moraju da sadrže različite informacije poput brojeva ili simbola kako bismo ih zaštitili od neželjenih napada. Problem sa ovim savjetom je to što se naši umovi bore da upamte nasumične nizove slova i brojeva koji za nas nemaju nikakvo značenje. Da bismo kreirali lozinku koju možemo da zapamtimo, mi koristimo predvidljive obrasce: na primjer, koristimo „0” umjesto „o”, ili „1” umjesto „i” ili koristimo „!” na mjestima na kojima ih je najlakše upamtiti. Iako nam ovo olakšava pamćenje lozinki, isto tako hakerima olakšava da pogode naše lozinke jer su svjesni obrazaca koje ljudi obično koriste.

Koristeći tehniku *Tri nasumične riječi*, možemo da kreiramo snažnije lozinke, koje se lako pamte i koje je teško hakovati.

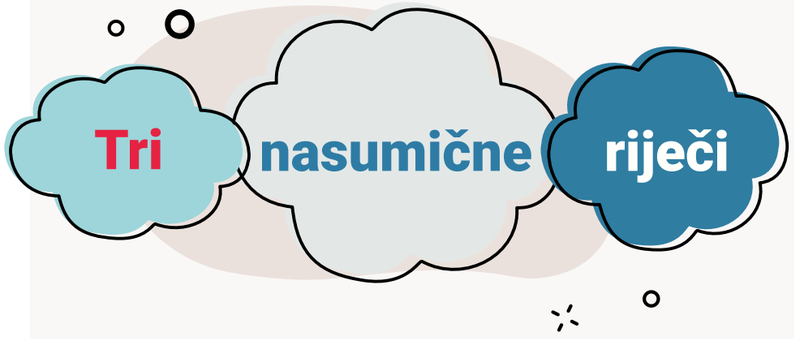
Zašto tri nasumične riječi?

Tehnika *Tri nasumične riječi* pomaže nam da kreiramo smislene lozinke koje ispunjavaju opšte zahtjeve.

Lozinke sastavljene od više riječi generalno će biti duže od lozinki sastavljenih od jedne riječi. Dužina je uobičajen (i preporučen) zahtjev za snažne lozinke, a korišćenje fraze stvorene kombinovanjem riječi omogućava da se to postigne bez oslanjanja na predvidljive obrasce.

Ključno je odabrati riječi koje se obično ne koriste zajedno, ali se pamte kada se sastave u jednu frazu. Tri nasumične, dobro izabrane riječi pružaju dodatnu zaštitu putem fraze koja za nas ima neko značenje i samim tim nam olakšava pamćenje, dok drugima otežava da je pogode.

I Google i Microsoft imaju dostupne smjernice o tome kako da promijenite lozinke za e-mail naloge, kao i za Microsoft i Google uređaje. Ako nijeste sigurni kako da promijenite svoje lozinke, posjetite Microsoft i Google stranice podrške za više informacija.



Zaštita naših lozinki pomoću Menadžera lozinki (Password Manager)

Često nam govore da su nam potrebne različite lozinke za različite naloge. Problem s toliko različitih lozinki može biti u njihovom memorisanju, čak i sa tehnikom *Tri nasumične riječi*.

Važno je da zapišemo svoje lozinke ili da ih sačuvamo u nezaštićenom dokumentu, ali zbog toga postajemo ranjivi na sajber napade jer hakeri lako mogu pronaći ove informacije. Tu nam može pomoći siguran menadžer lozinki.

Menadžer lozinki predstavlja koristan softver (obično je to aplikacija ili dio veb-pretraživača) koji može čuvati sve naše različite lozinke na bezbjedan i siguran način. To znači da ne moramo da brinemo o pamćenju naših različitih lozinki i smanjujemo rizik od nenamjernog dijeljenja.

Jednom kada se prijavimo u menadžer lozinki koristeći *glavnu* lozinku, on će zapamtiti naše lozinke za sve naše onlajn naloge. Mnogi menadžeri lozinki takođe mogu automatski da unesu naše lozinke na veb-lokacije i u aplikacije, tako da ne moramo da ih unosimo svaki put kada se prijavljujemo.

Šta to menadžeri lozinki rade?

Menadžeri lozinki nam omogućavaju da:

- Upravljamo zasebnim lozinkama za sve svoje važne naloge.
- Sinhronizujemo lozinke na različitim uređajima, time omogućavajući prijavljivanje gdje god da se nalazimo i koji god uređaj da koristimo.
- Pomažu u otkrivanju lažnih veb-sajtova, što će nas zaštititi od napada.
- Obavještavaju nas ako ponovo koristimo istu lozinku na različitim nalozima.
- Obavještavaju nas ako se naša lozinka pojavi u okviru poznatog kršenja privatnosti podataka, kako bismo znali da treba da je promijenimo.
- Funkcionišu na različitim platformama, tako da, na primjer, možemo koristiti jedan menadžer lozinki koji radi i za naš iPhone i za naš Windows desktop računar.

Kada se prijavljujemo na svoje onlajn naloge, većina veb-pretraživača (kao što su Chrome, Safari i Edge) će ponuditi da sačuva naše lozinke za nas. Za nas je bezbjedno da ovo uradimo na sopstvenim uređajima. Veb-pretraživači kao što su Safari i Chrome uvijek će pitati prije nego što sačuvaju naše lozinke.

Kako bismo bili sigurni da su naše lozinke bezbjedne, uvijek treba da budemo sigurni da koristimo najnoviju verziju veb-pretraživača.

Izbor snažne *glavne lozinke*

Menadžeri lozinki čuvaju sve naše važne lozinke, tako da je važno da imamo jedinstvenu, snažnu *glavnu lozinku* kako bismo zaštitili svoj menadžer lozinki.

Za kreiranje jake glavne lozinke (koja se teško zaboravlja) preporučljivo je koristiti tehniku *Tri nasumične riječi*. Zapamtite da menadžer lozinki ne čuva glavnu lozinku, tako da je važno da izaberete tri jedinstvene riječi koje će imati neko značenje za vas (pri tome nemojte koristiti lične podatke).

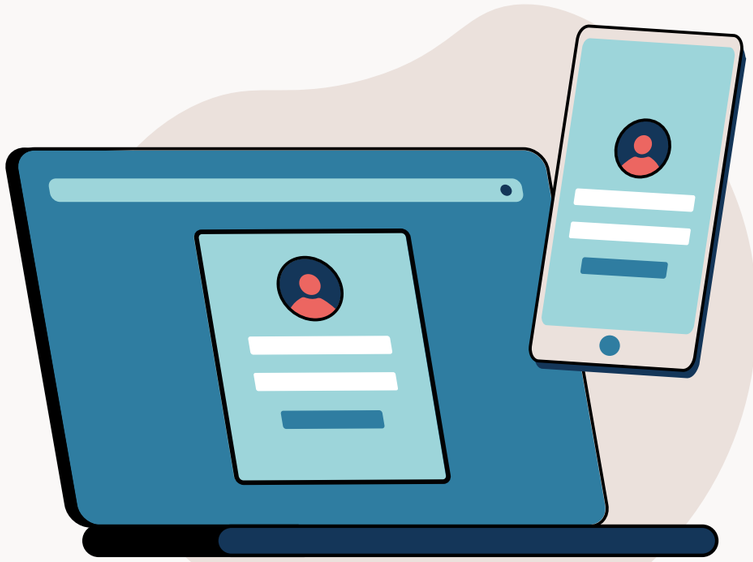
Takođe možemo dodati još jedan sloj zaštite pomoću verifikacije u dva koraka.

To znači da su naše lozinke, čak i ako zaboravimo glavnu lozinku ili je neko pogodi, i dalje zaštićene od napada.

Šta je to verifikacija u dva koraka?

Aktivacija verifikacije (koja je takođe poznata kao dvofaktorska autentifikacija ili višefaktorska autentifikacija) u dva koraka jedan je jedan od najefikasnijih načina da zaštitite svoje naloge na mreži od sajber kriminalaca. Može se koristiti za sve vaše naloge, a ne samo za menadžer lozinki.

Krađa vaše lozinke se izvodi lakše nego što mislite, pa se preporučuje da odvojite vrijeme kako biste podesili verifikaciju u dva koraka na svim svojim važnim nalozima, čak i na onim koje ste zaštitili jakim lozinkama.



Udvostručite svoju zaštitu

Aktivirajte verifikaciju u dva koraka
i dodatno zaštitite svoj nalog

Upoznajte se sa „Budite sajber svjesni“ alatima kako biste mogli da podesite opciju verifikacije naloga u dva koraka

Vlada
Crne Gore

Britanska ambasada
Podgorica

Kako da podesite verifikaciju u dva koraka

Ako je verifikacija u dva koraka dostupna za nalog, opcija za njenu aktivaciju se obično nalazi u bezbjednosnim podešavanjima naloga.

Kada postavimo verifikaciju u dva koraka, šalje nam se PIN ili kod, često putem SMS-a ili e-mail adrese. Zatim, moramo da unesemo ovaj PIN kako bismo dokazali svoj identitet i bili sigurni da samo mi možemo da pristupimo nalogu ili uređaju, budući da samo mi možemo da pristupimo našim SMS porukama ili e-mail nalogu.

Postoje različite vrste verifikacije u dva koraka. Dakle, umjesto da unesemo PIN ili kod, možda ćemo moći da unesemo otisak prsta ili skeniranje lica ili da koristimo aplikaciju za autentifikaciju (kao što su one koje pružaju Microsoft ili Google).

Nećemo morati da unosimo PIN (ili dajemo otisak prsta) svaki put kada koristimo uslugu; u zavisnosti od toga kako je nalog podešen, ovo ćete morati da uradite samo kada se otkrije „sumnjiva“ aktivnost (kao što je pokušaj prijave sa drugog uređaja ili zahtjev za promjenu lozinke).

Važno je zapamtiti da je, koju god vrstu verifikacije u dva koraka odaberemo, potrebno samo nekoliko minuta da je podesite. Jednom kada to uradimo, odmah smo mnogo bezbjedniji na mreži.

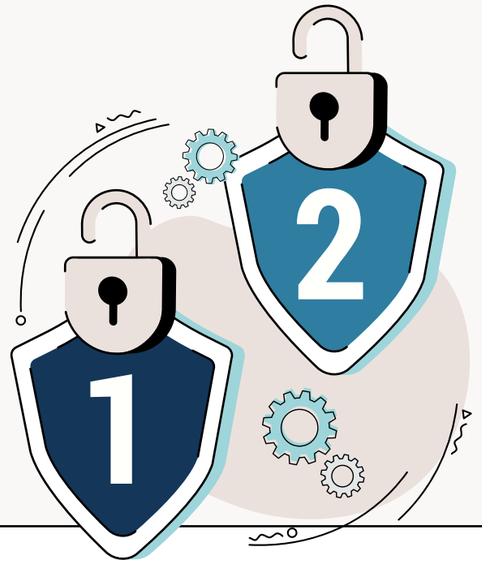
Microsoft i Google imaju dostupne smjernice i podršku za pomoć pri postavljanju verifikacije u dva koraka.

Na Microsoft nalozima:

- Idite na stranicu *Osnove bezbjednosti* (‘Security basics’) i prijavite se sa svojim Microsoft nalogom.
- Izaberite *Više bezbjednosnih opcija* (‘More security options’).
- U odjeljku *Verifikacija u dva koraka* (‘Two-step verification’) izaberite *Podesi verifikaciju u dva koraka* (‘Set up two-step verification’) kako biste je uključili.

Na Google nalozima:

- Idite na *Stranicu o bezbjednosti* (‘Security page’) na svom Google nalogu.
- Izaberite *Verifikacija u dva koraka* (‘Two-step verification’) u odjeljku *Prijava na Google* (‘Signing into Google’).
- Pratite uputstva kako biste podesili verifikaciju u dva koraka.



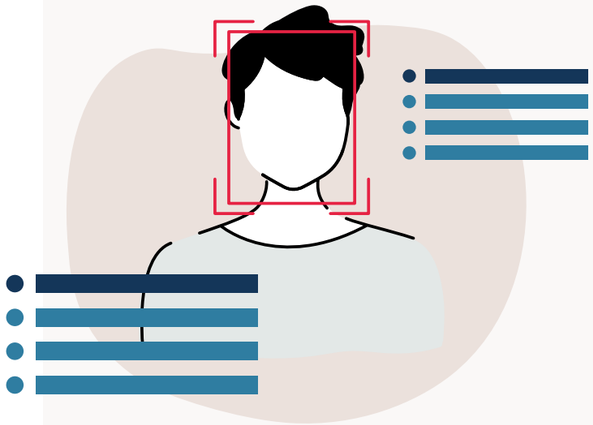
Upravljanje našim uređajima

Upravljanje našim uređajima

Obezbjeđivanje mobilnih telefona, tableta, laptopova, desktop računara i drugih povezanih uređaja suštinski je dio zaštite naše organizacije od sajber prijetnji.

Dobra vijest je da postoji podrška koja nam pomaže da upravljamo svojim različitim uređajima i da ih učinimo bezbjednim. Svaka platforma, bilo da je to Apple, Google ili Microsoft, ima stranice namijenjene za podršku, koje pružaju detaljnije informacije o specifičnim funkcijama uređaja (koje nam pomažu da ostanemo bezbjedni) i o načinima kako da upravljamo različitim uređajima.

Postoji nekoliko jednostavnih i brzih funkcija koje možemo da koristimo kako bismo zaštitili svoje uređaje, kao što je korišćenje biometrije (otisak prsta ili prepoznavanje lica) za verifikaciju u dva koraka, automatsko zaključavanje uređaja i omogućavanje praćenja lokacije.



Korišćenje biometrije

Biometriju čine biološke karakteristike pojedinca kao što su lice ili otisci prstiju i ona pruža bezbjednu i pogodnu alternativu upotrebi lozinki ili PIN-ova. Može se koristiti za verifikaciju identiteta i uvjeravanje da smo jedina osoba koja može da pristupi našim uređajima.

Na pametnim telefonima, tabletima, laptopovima i desktop računarima biometrija je primarni metod za provjeru identiteta korisnika i zaštitu od neovlašćenog pristupa. Upotreba otiska prsta ili prepoznavanja lica za autentifikaciju uređaja sada je uobičajena funkcija na pametnim telefonima i tabletima. Mobilni uređaji imaju najmanje jednu ugrađenu funkciju za verifikaciju identiteta korisnika putem otiska prsta ili prepoznavanja lica. Ova funkcija takođe postaje sve više dostupna i na laptop računarima.

Možemo da podesimo prepoznavanje lica ili otiska prsta u podešavanjima našeg uređaja, a mogu se naći i u *podešavanjima ekrana* (‘display settings’) ili *bezbjednosnim podešavanjima* (‘security settings’) u zavisnosti od uređaja. Preporučuje se da se takođe koristi i šifra (lozinka), tako da postoje dva sloja zaštite za naše uređaje, u slučaju da, iz bilo kog razloga, prepoznavanje lica ili otiska prsta ne radi.

Automatsko zaključavanje

Većina mobilnih uređaja, poput pametnih telefona i tableta, ima funkciju automatskog zaključavanja, koja će automatski zaključati uređaj nakon određenog perioda neaktivnosti. Podešavanje automatskog zaključavanja brzo je i jednostavno. Potrebno je da odete u podešavanja uređaja i izaberete *podešavanja displeja* (‘display settings’). Ovdje možemo izabrati dužinu vremena prije nego što se uređaj automatski zaključa, čiji je raspon obično od 30 sekundi do 5 minuta neaktivnosti.

Važno je da se postaramo da na uređaju takođe imamo podešenu i biometriju, tako da možemo bezbjedno da otvorimo uređaj koristeći lice ili otisak prsta nakon što se ekran automatski zaključa.

Funkcija praćenja lokacije

Praćenje lokacije ili GPS funkcija takođe nudi još jedan sloj zaštite za naše uređaje. Ako je naš uređaj ukraden ili izgubljen, praćenje lokacije nam pomaže da ga pronađemo. Držanje podešavanja lokacije uključenim, što se može uraditi u podešavanjima uređaja (ili *podešavanjima privatnosti*), omogućiće praćenje uređaja u slučaju gubitka ili krađe.

Većina proizvođača nudi onlajn uslugu lociranja izgubljenih ili ukradenih uređaja, a ova funkcija se može omogućiti unaprijed, tako da se uređaj može daljinski zaključati ili obrisati.

I Apple i Android uređaji nude ovu uslugu, pa se isplati provjeriti njihove zvanične stranice podrške za više informacija o tome kako možete da locirate, zaključate ili obrišete svoj uređaj.

Održavanje uređaja ažuriranim putem instaliranja bezbjednosnih ažuriranja pomaže u zaštiti naših uređaja i naloga od sajber kriminalaca.

Bezbjednosna ažuriranja obično uključuju zaštitu od virusa i drugih vrsta zlonamjernih softvera osmišljenih da naškode našim uređajima i nalozima. Oni će često podrazumijevati poboljšanja i nove funkcije, tako da treba da vršimo ažuriranja čim postanu dostupna.

Ako dobijemo poziv da ažuriramo svoj uređaj (ili aplikacije), ne bi trebalo da ga ignorišemo. Primjena ovih ažuriranja je jedna od najvažnijih i najbržih stvari koje možemo da uradimo kako bismo ostali bezbjedni na mreži.

Instalacija ažuriranja softvera može potrajati i obično zahtijeva pouzdanu internet vezu, tako da je najbolje da to uradite na bezbjednoj lokaciji, na primjer, na poslu ili kod kuće, gdje možete da pristupite svojoj wi-fi vezi (i da vaš uređaj dobije napajanje).

Ako u podešavanjima svog uređaja izaberemo opciju *automatsko ažuriranje*, nećemo morati da se sjetimo da instaliramo ažuriranja kako bi naši uređaji duže ostali zaštićeni.

Ne odlažite instalaciju ažuriranja. Ažuriranja sadrže zaštitu od virusa i drugih vrsta zlonamjernih softvera.

Šta ako naši uređaji više ne primaju ažuriranja?

Proizvođači će na kraju prestati da pružaju ažuriranja za starije uređaje.

Ako nastavimo da koristimo uređaj koji više nije podržan, on neće primati ažuriranja koja sadrže nove funkcije i poboljšanja performansi i neće primati bezbjednosna ažuriranja od proizvođača (bez njih je naš uređaj podložniji sajber napadima).

Trebalo bi da razmotrimo zamjenu uređaja koje proizvođači više ne podržavaju novijim modelima, ali možemo provjeriti onlajn da vidimo koliko dugo će naš trenutni uređaj imati zvaničnu podršku od strane proizvođača.

Rezervne kopije naših podataka

Većina nas u nekom trenutku nije mogla da pristupi važnim podacima kao što su dokumenti, fotografije, video-snimci, kontakt podaci ili neke druge lične informacije. Kada napravimo rezervnu kopiju svojih podataka, osiguravamo da se našim informacijama i fajlovima i dalje može pristupiti ako nešto krene naopako.

Zakazivanje izrade rezervne kopije podataka moglo bi da nas poštedi mnogo stresa. Pravljenje rezervne kopije podataka ne traje dugo i obično se može podesiti tako da se odvija automatski.

Šta je to rezervna kopija podataka?

Rezervna kopija podataka je kopija svih važnih podataka sa naših uređaja, koja se čuva na zasebnoj, bezbjednoj lokaciji: obično na internetu sa skladištem u oblaku ili na prenosivim uređajima kao što su USB stick, SD kartica ili eksterni hard disk. Ako izgubimo pristup svojim originalnim podacima, i dalje možemo pristupiti kopijama iz rezervne kopije podataka. Rezervne kopije podataka ne služe samo za vraćanje izgubljenih, izbrisanih ili nedostupnih podataka. Rezervne kopije podataka takođe možemo da koristimo i za prenos postojećih datoteka, aplikacija i podešavanja na nove uređaje.

Postoje mnogi razlozi zbog kojih možda nećete moći da pristupite svojim podacima:

- imate novi uređaj i želite da kopirate postojeće fajlove na njega,
- vaš uređaj je izgubljen ili ukraden,
- vaš uređaj je pokvaren,
- podaci na vašem uređaju su slučajno obrisani (ili su postali nečitljivi),
- virus (ili neki drugi tip štetnog softvera kao što je ransomware, softver koji traži otkup za pristup podacima) može izbrisati vaše podatke ili vam onemogućiti pristup.

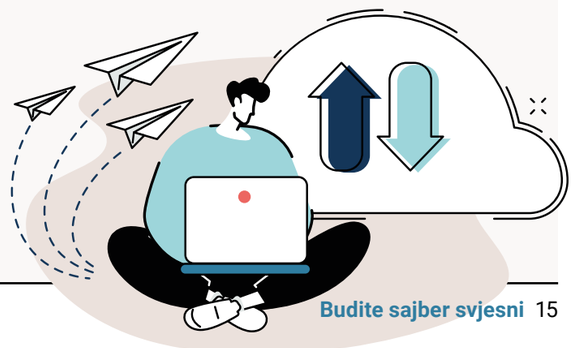
Većina rezervnih kopija podataka vam omogućava da izaberete za koje fajlove i informacije će biti napravljene rezervne kopije, bilo da su to samo dokumenti, fotografije i video-snimci ili cijeli sadržaj uređaja (uključujući aplikacije i programe koje koristimo). Opšte pravilo je da treba da pravimo rezervne kopije svega što smatramo važnim.

Pravljenje rezervne kopije podataka koristeći skladište u oblaku (*cloud storage*)

Rezervnu kopiju naših podataka možemo napraviti koristeći skladište u oblaku, što znači da se kopija naših podataka čuva na bezbjednom dijelu interneta. Korišćenje skladištenja u oblaku takođe znači da ćemo imati opciju da automatski kreiramo rezervne kopije, tako da je veća vjerovatnoća da ćemo imati nedavnu kopiju naših podataka i ne moramo da pamtimo da redovno pravimo rezervne kopije.

Rezervne kopije za Apple, Google i Microsoft uređaje mogu da se prave pomoću skladišta u oblaku, ali zapamtite da korištenje skladišta u oblaku zahtijeva pouzdanu internet vezu za pravljenje rezervne kopije (i vraćanje) podataka.

Svako ko može da pristupi nalogu za skladištenje u oblaku takođe će imati pristup podacima uskladištenim na njemu. Zbog toga je važno da zaštitimo svoj nalog za skladištenje u oblaku korišćenjem jakih lozinki tehnikom *Tri nasumične riječi* i uključivanjem verifikacije u dva koraka, kako bismo kontrolisali pristup svom nalogu.



Pravljenje rezervne kopije podataka pomoću prenosivog medija

Rezervnu kopiju svojih podataka takođe možete napraviti na prenosivim medijskim uređajima kao što su:

- eksterni hard disk (obično povezan USB kablom),
- USB stick ili fleš disk,
- SD kartica,
- DVD ili CD-R diskovi.

Pravljenje rezervnih kopija pomoću prenosivih medijskih uređaja omogućava vam da napravite rezervnu kopiju velike količine podataka, koja može biti izvan kapaciteta opcija za skladištenje u oblaku.

Važno je da isključite prenosive medije kada se ne koriste. Virusi (i drugi tipovi štetnog softvera) mogu automatski da inficiraju priključene medijske uređaje, što znači da bi bilo koja rezervna kopija sačuvana na medijskom uređaju takođe mogla da bude zaražena, što bi nas ostavilo bez rezervne kopije podataka za oporavak. Zato moramo da koristimo samo sopstvene prenosive medijske uređaje u koje imamo povjerenja i nikada ne treba da koristimo tuđi uređaj ili nepoznati uređaj.

Ako koristite prenosive medijske uređaje, dobra ideja je da podesite termin u kalendaru ili podsjetnik kako biste to redovno radili.

Prenosivi medijski uređaji mogu biti izgubljeni ili ukradeni, pa je važno da ih zaštitimo najbolje što možemo. Ako imamo opciju da zaštitimo rezervnu kopiju podataka lozinkom, trebalo bi to i da uradimo. Bez lozinke, neko ko ima medijski uređaj ne može da pristupi podacima u našoj rezervnoj kopiji. Da bismo bili dodatno obezbijeđeni, trebalo bi da izbjegavamo čuvanje kopija povjerljivih ili osjetljivih informacija na prenosivim medijskim uređajima i da koristimo skladištenje u oblaku koje se može zaštititi.

Oporavak greškom izbrisanih fajlova

Ponekad se fajlovi mogu slučajno izbrisati ili premjestiti. Zato je dobro znati kako da povratimo svoje podatke kada se to dogodi.

Da vratite fajlove koji su možda izbrisani greškom, potražite funkcije *korpe za otpatke* (‘recycle bin’) i *istorija fajlova* (‘file history’) i uvjerite se da su date funkcije uključene. Ovo je brže od obnavljanja cijele rezervne kopije podataka ako treba da povratimo samo nekoliko fajlova. Postarajte se da su ove funkcije uključene unaprijed kako biste mogli da vratite izgubljene fajlove po potrebi. Fajlovi se mogu vratiti samo u slučaju kada je funkcija *istorija fajlova* (‘file history’) bila prethodno uključena.

Korpa za otpatke nam daje neko vrijeme da obnovimo izbrisane fajlove prije nego što budu trajno izbrisani sa naših uređaja. Alternativno, naša istorija fajlova nam daje opciju da povratimo fajl na prethodnu verziju, u slučaju da treba da poništimo slučajnu promjenu dokumenta.

Postanite svjesni svog digitalnog otiska

Kada koristimo internet, za sobom ostavljamo digitalni otisak koji se naziva i elektronski otisak.

Digitalni otisak se sastoji od informacija o internet sajtovima koje posjećujemo, e-mailova koje šaljemo i podataka koje unosimo onlajn. Onlajn ponašanje pojedinca i njegovi uređaji mogu se pratiti preko njegovog digitalnog otiska.

Sajber napadači i zlonamjerni akteri mogu potražiti naš onlajn identitet i digitalni otisak i iskoristiti ove informacije za ciljane sajber napade protiv nas.

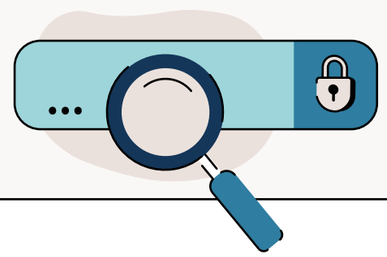
Postoji nekoliko stvari koje možemo uraditi kako bismo ostali svjesni svojih digitalnih otisaka:

- **Iskoristiti pretraživače kako bismo provjerili svoj digitalni otisak**
  Možemo pretražiti svoje ime u pretraživačima kao što je Google da bismo provjerili svoj digitalni otisak.

  Da bismo uradili ovo, tražićemo svoje puno ime, ime i prezime i bilo koji alternativni način pisanja, kao i naše staro i novo ime ukoliko smo ga mijenjali.

  Pregledajući rezultate pretraživača, možemo saznati kakve informacije o nama su javno dostupne. Takođe, možemo da stupimo u kontakt sa administratorom sajta da provjerimo da li on može da ukloni rezultate ukoliko bilo koji od njih sadrži osjetljive informacije koje ne želimo da podijelimo sa širom javnošću.

- **Provjeriti povrede podataka**
  Možemo da provjerimo da li je neki od naših naloga kompromitovan povredom podataka na internet sajtovima kao što je Have I Been Pwned.



- **Kreirati Google upozorenja**
  Možemo kreirati Google upozorenje koje će nas obavijestiti ukoliko se i kada naše ime ili e-mail adresa pomenu na Googleu. Za više informacija o tome kako to da uradite, za pomoć posjetite zvanične Google stranice.

- **Ograničiti dijeljenje podataka što je više moguće i provjeriti podešavanja privatnosti**
  Koristeći podešavanja privatnosti na društvenim mrežama, možemo da upravljamo time ko može da vidi šta objavljujemo onlajn. Iako društvene mreže olakšavaju povezivanje sa ljudima, takođe mogu da učine lakšim prekomjerno dijeljenje. Na društvenim mrežama ne bi trebalo nikada da dijelimo svoje lične podatke kao što su broj telefona ili e-mail adresa. Moramo biti obazrivi kada dijelimo podatke kao što su lokacija, plan putovanja ili druge privatne stvari. Sajber napadači mogu da iskoriste ove informacije da kreiraju ciljane napade.

  Možemo da provjerimo svoja podešavanja privatnosti na svojim nalozima na društvenim mrežama kako bismo bili sigurni da su na nivou koji nam odgovara. Na primjer, Facebook nam omogućava da kreiramo personalizovane liste onih koji mogu vidjeti naš profil i podesimo ažuriranja profila da budu vidljiva samo našim prijateljima. Na ovaj način onemogućavamo dijeljenje svoje lokacije i ličnih informacija sa ljudima koje ne poznajemo ili im ne vjerujemo.

- **Biti pažljivi šta *lajkujemo* onlajn**
  Trebalo bi da izbjegnemo *lajkovanje* usluga koje koristimo, na primjer, svoje banke, pružaoca zdravstvenih usluga ili apoteke jer bi ovo moglo da usmjeri sajber napadače ka našim važnim nalozima. Kada su upoznati sa uslugama i organizacijama koje koristimo, lakše im je da se lažno predstavljaju i otimaju naš identitet.

Preskočiti opasne internet sajtove
Bezbjedan internet sajt treba da ima URL koji počinje sa “https://” umjesto “http://”. *S* stoji za *bezbjedan* i označava prisustvo sigurnosnog certifikata.

Dodatno, lijevo od adresne trake, trebalo bi da se nalazi simbol katanca. Ovo nas obavještava da su internet sajtovi koje posjećujemo bezbjedniji od potencijalnih napada.

Ukoliko nijesmo sigurni u vezi sa nekim internet sajtom, uvijek možemo da ga provjerimo na www.virustotal.com – taj sajt predstavlja besplatnu Google uslugu za otkrivanje zlonamjernih internet sajtova.

Ne dijeliti privatne informacije na javnoj wi-fi mreži
Nikada ne možemo biti sigurni ko je postavio javnu wi-fi mrežu ili ko motri na korisnike mreže. Javne wi-fi mreže su u osnovi manje bezbjedne od wi-fi mreže kojoj imamo pristup kod kuće ili na poslu. Kada koristimo javne wi-fi mreže, ne bi trebalo da dijelimo privatne ili osjetljive informacije kao što su kontakt podaci ili informacije koje bi mogle da pomognu sajber napadačima da se predstavljaju kao mi. Takođe, trebalo bi da se uzdržimo od pristupa osjetljivim informacijama, kao što su zvanična dokumenta za posao i kada koristimo javne ili nezaštićene wi-fi mreže.

Ukloniti prethodne naloge
Uklanjanje zastarjelih naloga kao što su sajtovi društvenih mreža koje više ne koristimo ili pretplata za biltene koje više ne čitamo jedan je od pristupa za smanjenje digitalnog otiska. Uklanjanje neaktivnih naloga smanjuje našu ranjivost kada je riječ o povredi podataka.

Budite sajber svjesni

- Da li smo postavili snažnu lozinku koristeći tehniku *Tri nasumične riječi*?
- Da li koristimo menadžer lozinki 'Password Manager' za upravljanje našim različitim lozinkama?
- Da li smo kreirali snažnu *glavnu lozinku* za svoj menadžer lozinki koristeći tehniku *Tri nasumične riječi*?
- Da li smo uključili verifikaciju u dva koraka na našim nalozima i uređajima?
- Da li smo podesili otisak prsta ili prepoznavanje lica na svojim mobilnim uređajima (pored svojih lozinki) da bismo ih zaštitili?
- Da li smo uključili automatsko zaključavanje na svojim mobilnim uređajima?
- Da li smo uključili praćenje lokacije na svojim mobilnim uređajima?
- Da li znamo kako da koristimo zvaničnu uslugu praćenja lokatora na mreži za praćenje izgubljenih ili ukradenih uređaja?
- Da li su aplikacije i softver na našem uređaju ažurirani?
- Da li smo uključili automatsko ažuriranje softvera?
- Ako je naš uređaj stariji, znamo li da li proizvođač još uvijek pruža podršku za njega?
- Da li smo napravili rezervne kopije svojih podataka?
- Da li smo zakazali redovnu izradu rezervnih kopija podataka? Ili da li smo uključili automatsko pravljenje rezervnih kopija u skladištu na oblaku?
- Jesmo li provjerili svoj digitalni otisak?