Mali priručnik digitalne sigurnosti

Za krajnje korisnike/ice

2018. godina

UVOD

O čemu je riječ u publikaciji?

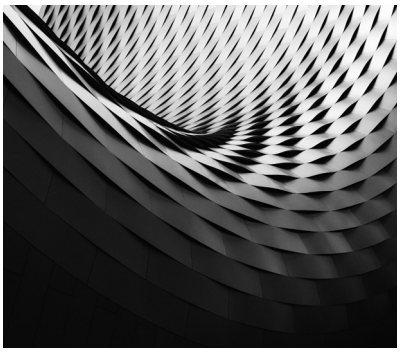
Nalazimo se u dobu transformacije društva. Digitalizacija je donijela nove izazove pred korisnike i potreba za osiguravanjem naših podataka je postala goruća tema društva. Publikacija ima namjenu da krajnjim korisnicima/cama pomogne u osiguravanju njihovih podataka, uređaja, te uvid u dobre prakse i aplikacije koje se svakodnevno koriste kroz primjere, savjete i mapiranje.

Publikaciju omogućili:

CRYPTO PARTY
-Bosna i Hercegovina-

CRYPTO PARTY SARAJEVO

Sadržaj

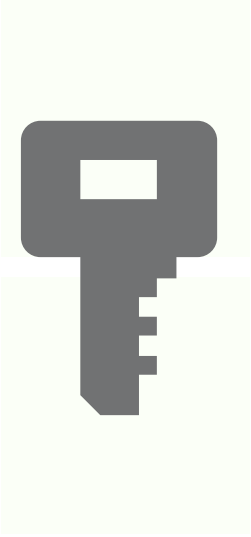


VI i 689 drugih korisnika
označavate objavu sa "Sviđa mi se"

Ostavite komentar...

SNAPSHOTS:

Sigurnost šifri



Šta je šifra?

Šifra je dio informacije koji se koristi za potvrdu autentifikacije kao osiguranje da drugi neće moći pristupiti našim podacima bez poznavanja iste.

Koraci za dobru šifru!

a) Napravite passphrase (prev. šifra fraza)

Što je šifra duža, teže je pogoditi. Napravite jednostavnu frazu koju poznajete samo Vi i osigurajte je brojevima ili simbolima.
Nešto poput "d1g1tAln4s1gUrn0sT%$&j3sup3r"

b) Koristite menadžere šifri

Menadžer šifri pamti i čuva vaše šifre. Umjesto šifri za e-mail ili socijalne mreže, pamtite samo jednu - Vašeg menadžera šifri.
Preporuka za instaliranje: KeePass

c) Dodajte dvostruku autentifikaciju

Dodatni sloj sigurnosti nije na odmet. Koristite dvostruku autentifikaciju koja najčešće dolazi u formi SMS-a na Vaš mobilni uređaj. Skoro sve socijalne mreže i servisi usluga poput elektronskog bankarstva ili platformi sa vulnerabilnim podacima imaju omogućavanje dvostruke autentifikacije u sigurnosnim postavkama.

Vi i 432 osobe označavaju objavu sa "Sviđa mi se!"

Savjet 1

Nema potrebe za čestim promjenama šifri. Stalno mijenjanje šifri može dovesti do smanjenja sigurnosti. Pronađite svoju sigurnu šifru i pustite da bude čuvar Vaših podataka.

Savjet 2

Jačinu Vaših šifri možete provjeriti na :

https://www.lastpass.com/

Savjet 3

Koristite različite šifre za različite platforme i web aplikacije. Uvijek imate menadžera šifri koji će ih sve upamtiti za Vas.

Savjet 4

Vodite dnevnik Vaših šifri. Zapišite ih na papir i spremite na sigurno mjesto.

Savjet 5

Ne vjerujte pretraživačima. Ukoliko Vam je potrebno pamćenje šifre, odlučite se za menadžera šifri.

Savjet 6

Ne unosite Vaše korisničke autentifikacijske podatke u javne računare ili uređaje za koje ne znate da li su dovoljno sigurni. Vaše korisničke podatke ne šaljite trećim, nepoznatim licima, osim ako imaju verificiranu potvrdu da su korisnička služba ili služba za podršku.

Sigurnost mobilnih uređaja

Preko 70 % mobilnih uređaja nije zaštičeno!

Mobilni uređaji su postali neizostavan dio naših dnevnih života u koje unosimo svoje podatke i koristimo ih za komunikaciju i poslovne svhre.

Kako osigurati svoj uređaj?

a) Enkriptujte uređaj

Enkripcija uzima samo 20 minuta vremena, a daje nam punu zaštitu naših podataka. Enkripcija za Android telefone je u Opcije -> Sigurnost -> Enkriptujte uređaj. Za vrijeme enkripcije, bitno je da punite svoj telefon.

b) Ne koristite javne mreže

Otvorene mreže često podrazumjevaju otvoreni izazov za našu sigurnost. Pokušajte izbjeći prijave na otvorene vajrles mreže, a ako morate da ih koristite, koristite ih sa uključenim VPN-om (detaljno u aplikacijama).

c) Vršite update aplikacija

Update aplikacija podrazumjeva ispravljenu sigurnosnu ranjivost aplikacije, te se krajnjim korisnicima sugeriše da održavaju svoje aplikacije na novim verzijama iste..

Vi i 432 osobe označavaju objavu sa "Sviđa mi se!"

Savjet 1

Koristite jaki PIN.

Savjet 2

Izbjegavajte aplikacije koje nemaju verificirani i povjerljivi izvor ili nisu otvorenog koda. Aplikacije na trgovinama mobilnih uređaja su često provjerene, ali potreban je dodatni oprez.

Savjet 3

Razmislite o dozvolama koje Vam aplikacije traže.

Savjet 4

Održavajte svoje socijalne mreže, elektronsku poštu i pretraživače sigurnim sa jakim šiframa i dodatnom enkripcijom.

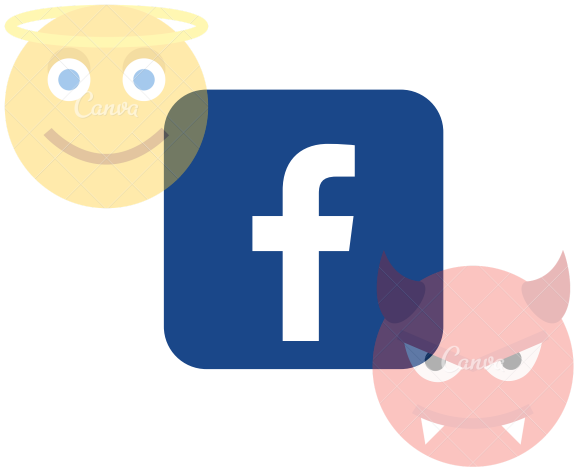
Savjet 5

Koristite samo mreže za koje ste sigurni da su zaštičene od potencijalnih nesigurnosti.

Savjet 6

Ne dijelite podatke sa drugim aplikacijama i platformama, osim ako je to nužno.

Sigurnost socijalnih mreža



Socijalne mreže su super... ako su zaštićene!

Socijalne mreže su mjesto upoznavanja, druženja i korisnih informacija. Ali, socijalne mreže su i mjesto krađe korisničkih podataka.

Vaš profil na socijalnoj mreži treba:

a) Biti zaštićen od znatiželjnika

Neka Vaše objave budu dostupne samo prijateljima, a prijatelji osobe koje poznajete.

b) Ne šaljite Vaše podatke nepoznatim korisnicima

Socijalne mreže vrve od mnoštva nagradnih igri koje zahtjevaju Vaše podatke, pa čak i uslikane identifikacijske dokumente. Takav vid manipulacije korisnicima se naziva "phishing" i napadaču služe da bi stekao uvid u podatke koje kasnije koristi na različite načine. Zaštita od phishinga ne postoji, osim da budete dovoljno informisani i čuvate svoje podatke.

c) Prijave na druge platforme

Nekako nam je uvijek najlakša opcija da jednostavno kliknemo prijavu putem Facebooka i uđemo na neku od platformi. Takav vid dijeljenja podataka je vrlo vulnerabilan iz prostog razloga što druga platforma ima skoro kompletan uvid u naše podatke.

Ako želite isključiti platforme, idite na Apps ---> Apps, Websites, Plugins ---> Lista platformi --> isključite one koje Vam više nisu potrebne

Vi i 432 osobe označavaju objavu sa "Sviđa mi se!"

Savjet 1

Koristite jaku šifru..

Savjet 2

Pročitajte uvjete o korištenju platforme ili socijalne mreže.

Savjet 3

Dijelite što manje povjerljivih informacija o sebi poput trenutne lokacije ili broja telefona sa drugim korisnicima/korisnicama.

Savjet 4

Ne idite na "clickbait" članke koji mogu biti izvor potencijalnih nesigurnosti.

Savjet 5

Provjerite identitet osobe sa kojom ste u kontaktu, ako je ne znate uživo. Često ljudi nisu oni kojim se predstavljaju na Internetu.

Savjet 6

Vašu arhivu podataka na Facebooku možete skinuti sa Settings --> General Account Settings ---> Download a copy of your Facebook data ---> Start my archive.

Korisne aplikacije

Haven je aplikacija za monitoring fizičkog prostora i nadzor vašeg uređaja od neželjenog korištenja.

Crypto Cat je aplikacija koja dopušta enkriptovani chat.

KeePass je menadžer šifri otvorenog koda.

SeaphimDroid je aplikacija koja osigurava bezbjednost od virusa, phishing napada, te prepušta kontrolu korisniku koje aplikacije koristi.

EtherApe je korisna aplikacija koja nam pomaže da vidimo koliko aplikacije troše podataka.

LastPass je jedan od najboljih menadžera šifri na tržištu. On čuva Vaše šifre i druge podatke sigurno.

K-9 elektronska pošta omogućava slanje i primanje enkriptovanih mejlova.

Signal je aplikacija za komunikaciju koja šifrira Vaše poruke i razgovore.

BRAVE je pretraživač koji štiti vašu privatnost, te omogućava sigurno pretraživanje Interneta.

Orbot je besplatna proxy aplikacija koja enkriptuje Internet saobraćaj.

Keybase je menadžer digitalnih identiteta dostupan u vidu javnog profila.

OpenVPN je rješenje za sigurnu komunikaciju preko Interneta, koja štiti Vašu mrežu.