Ne budi i ti hrvatski naivac

#SurfajSigurnije na društvenim mrežama

CERT.hr
surfaj sigurnije

Sufinancirano instrumentom Europske unije za povezivanje Europe

SIGURNOST DRUŠTVENIH MREŽA

Društvene mreže su neodvojivi dio današnjeg interneta i putem njih se odvijaju novi oblici privatne i poslovne komunikacije. S jedne strane pojednostavljuju i ubrzavaju komunikaciju, no s druge strane omogućavaju lakši pristup zlonamjernim korisnicima do potencijalnih žrtava raznih prijevara, krađa identiteta i ucjena.

Globalno gledajući, društvene mreže u 2018. godini koristi 98% internetskih korisnika. Dnevno se u prosjeku provede više od 2 sata na društvenim mrežama kroz dopisivanje i razmjenu informacija. Društvene mreže koriste se i za praćenje novih proizvoda i trendova te ih gotovo polovica svih korisnika koristi upravo u tu svrhu.

Međutim, ne koriste svi samo jednu društvenu mrežu već imaju više korisničkih računa na više društvenih mreža. Podaci pokazuju kako korisnici interneta u prosjeku imaju 8,5 različitih korisničkih računa za više različitih društvenih mreža, ali trendovi pokazuju smanjenje tog broja kod mlađih generacija.

Mlađe generacije, a pogotovo korisnici između od 16 do 24 godine, koriste društvene mreže za ispunjavanje slobodnog vremena ili za pronalazak smiješnog sadržaja za razonodu. Stariji, s druge strane, društvene mreže koriste za informiranje o novostima ili komunikaciju s prijateljima jer društvene mreže više nisu samo platforme za komunikaciju već i za razmjenu znanja, mišljenja, novosti, glazbe, slika i ostalog sadržaja.

Prema broju i strukturi korisnika društvenih mreža u 2018. godini izrađen je popis 10 najpopularnijih društvenih mreža s postotcima registriranih članova i posjetitelja koji su barem jednom mjesečno pristupali navedenim društvenim mrežama. Istraživanje je rađeno na globalnom uzorku od 98 011 internetskih korisnika u dobi od 16 do 64 godine (bez Kine):

DRUŠTVENE MREŽE	BROJ REGISTRIRANIH KORISNIKA	BROJ KORISNIKA POSJETITELJA
Facebook	85%	79%
YouTube	79%	86%
FB Messenger	72%	55%
WhatsApp	66%	60%
Instagram	63%	58%
Twitter	56%	43%
Google+	51%	40%
LinkedIn	40%	28%
Skype	35%	28%
Snapchat	35%	24%

Za uvodni dio publikacije korišteni su podaci iz izvještaja Social – GlobalWebIndex's flagship report on the latest trends in social media. Dostupno na: https://www.globalwebindex.com/reports/social

POPULARNE DRUŠTVENE MREŽE

1. Instagram | Minimalna dob za registraciju: 13 godina

Korisnici mogu snimati, uređivati i dijeliti fotografije i kratak video sadržaj. Postavke privatnosti mogu biti podešene tako da sadržaj učine javno dostupnim ili privatnim. Sama platforma dopušta dijeljenje i komentiranje sadržaja. Sve dok je korisnički račun privatan, nitko ne može pogledati ili komentirati objavu. Rizici uključuju dijeljenje neprimjerenog sadržaja među prijateljima te javno dijeljenje lokacije na temelju oznaka lokacije.

2. WhatsApp | Minimalna dob za registraciju: 16 godina

Popularna aplikacija za razmjenu poruka jer korisnicima omogućava slanje tekstualnih poruka, zvučnih zapisa, video sadržaja i fotografija jednoj ili više osoba bez naknade. WhatsApp korisniku ograničava pristup na samo one korisnike koje ima u imeniku. Međutim, korisnici koji se nalaze u istim grupama kao vi, mogu komunicirati s vama čak i ako ih nemate u imeniku.

3. Snapchat | Minimalna dob za registraciju: 13 godina

Popularna aplikacija za dijeljenje fotografija. Snapchat korisnicima dopušta dijeljenje fotografija i video sadržaja unutar određenog vremenskog perioda, odnosno protekom vremena sadržaj se automatski briše. Međutim, valja imati na umu kako zlonamjerni korisnici mogu preslikom ekrana sačuvati sadržaj te ga na taj način pohraniti. Snapchat kod korisnika budi lažnu sigurnost jer smatraju da će se sadržaj uvijek obrisati, ali postoje načini kako se ovo može zaobići. Također, opcija Discover (hrv. Otkrij) može omogućiti korisnicima pristup do zlonamjernog ili neprimjerenog sadržaja.

4. Twitter | Minimalna dob za registraciju: 13 godina

Aplikacija za dijeljenje kratkih objava koje mogu biti javno dostupne ili privatne. Najčešće ju koriste korisnici koji žele pratiti svoje prijatelje, bližnje i kolege te poznate osobe. Iako Twitter ima opciju za brisanje vaših objava, objavljeni sadržaj mogao je biti kopiran ili pohranjen.

5. Facebook | Minimalna dob za registraciju: 13 godina

Globalno popularna društvena mreža koja korisnicima dopušta da dijele fotografije, video i ostali sadržaj te ga komentiraju. Također, Facebook posjeduje svoju aplikaciju za razmjenu poruka zvanu Messenger. Putem Facebooka korisnici održavaju kontakt s bližnjima, prijateljima, kolegama, ali i prate događaje, razne stranice te mogu biti članovi raznih grupa.

6. YouTube | Minimalna dob za registraciju: 13 godina

Popularna usluga za razmjenu videozapisa na kojoj ih korisnici mogu postavljati, pregledavati i ocjenjivati. Za pregledavanje sadržaja nije potrebna registracija, ali je potrebna za komentiranje i postavljanje vlastitog sadržaja. YouTube korisnicima brani postavljanje pornografskog sadržaja, nasilja, sadržaja koji podržava kriminalne radnje, sadržaja s ciljem sramoćenja, klevete i reklama.

PRIJETNJE NA DRUŠTVENIM MREŽAMA

Broj korisnika društvenih mreža u stalnom je porastu, međutim, koncentracija velikog broja korisnika na jednom mjestu može privući i zlonamjerne pojedince koji putem društvenih mreža žele ostvariti neku novčanu dobit, dobiti pristup nekoj povjerljivoj ili osobnoj informaciji ili jednostavno izazvati strah i paniku kod nesmotrenih i neutemeljeno povjerljivih korisnika.

Na ovakve se prijetnje može uspješno odgovoriti bez složenog tehničkog znanja služeći se samo vlastitim zdravim razumom i dostupnim informacijama, ali valja imati na umu kako prijetnje postoje i kako postoje zlonamjerni korisnici. Imajući samo ovo na umu, prosječni korisnik značajno podiže razinu sigurnosti sebe, ali i svih ostalih pojedinaca s kojima je putem društvenih mreža vezan.

Za prepoznavanje i smanjenje rizika od potencijalno opasnih situacija korisnik treba osvijestiti postojanje nekih od ranjivosti i izazova na koje nailazimo kada razmatramo kibernetičku sigurnost na društvenim mrežama:

1. Pogrešno i/ili neodgovorno korištenje osobnih podataka
2. Prijetnje izazvane korištenjem vanjskih aplikacija
3. Prijetnje izazvane pretjeranim povjerenjem u društvenu mrežu
4. Zlonamjerni sadržaj i socijalni inženjering
5. Zakonski neregulirano korištenje društvenih mreža
6. Privatnost korisnika
7. Korištenje podataka korisnika

Na neke od izazova sam korisnik ne može odgovoriti, ali svojim opreznim i promišljenim djelovanjem može umanjiti rizik i povećati razinu sigurnosti sebe i bližnjih. Primjeri najčešćih oblika prijetnji navedeni su u nastavku s naglaskom kako napadač zna kako iskoristiti žrtvu na različite načine i svaki korisnik treba biti toga svjestan pri korištenju interneta i društvenih mreža.

1. Napadi u kojima se koristi socijalni inženjering

Socijalni inženjering podrazumijeva niz tehnika i metoda kojima se napadač služi kako bi nagnao žrtvu da učini nešto što nije u njenom interesu. Primjer ovakvog napada na društvenim mrežama je phishing napad u kojem napadač šalje poruku u kojoj se predstavlja kao neka druga osoba, tvrtka ili organizacija te od žrtve traži slanje osobnih podataka u povratnoj poruci, na neku nepoznatu adresu ili upisivanjem osobnih podataka na nekoj internetskoj stranici čija je adresa dostavljena u tekstu poruke.

2. Krađa identiteta

Pojedini korisnici koriste isto korisničko ime i lozinku za više različitih servisa i društvenih mreža, ali i koriste sustav za autentifikaciju pojedinih društvenih mreža za prijavu na neke vanjske servise. Na primjer, korisnik se može prijaviti na neku uslugu koristeći opciju prijave putem društvene mreže. Na ovaj se način korisniku olakšava prijava jer koristi samo jedno korisničko ime i lozinku, ali valja imati na umu kako kompromitacija jednog korisničkog računa sa sobom povlači i kompromitaciju svih povezanih servisa i usluga. Također, ukradeni korisnički podaci napadaču mogu poslužiti u daljnjem izvođenju napada, a takvo što može imati značajne posljedice po žrtvu.

3. Zlonamjerni sadržaj

Putem društvenih mreža svakodnevno se razmjenjuje mnogo podataka i komunicira s velikim brojem korisnika. Međutim, društvenim se mrežama služe i zlonamjerni korisnici koji ih mogu koristiti za slanje zlonamjernog sadržaja žrtvama. Ovakav sadržaj se ne mora doimati zlonamjerno na prvi pogled, ali preuzimanje istoga na vlastiti uređaj ili slanje na adrese ostalih kontakata na društvenim mrežama može prouzročiti značajnu štetu za sve koji su bili u kontaktu s takvim sadržajem. Stoga je važno preuzimati sadržaj koji vam šalju osobe koje poznajete, ne preuzimati nešto što vam se čini sumnjivim na vaše računalo i nikako ne slati takav sadržaj dalje.

4. Curenje podataka

Danas je prosječni korisnik interneta član velikog broja servisa i usluga od kojih svaka zahtijeva izradu korisničkog računa ili vezivanje postojećeg korisničkog računa na nekoj društvenoj mreži kako bi ispravno radila. Mnogi se korisnici za prijavu na različite servise služe istim korisničkim podacima što značajno povećava rizik jer kompromitacija jednog korisničkog računa često za sobom donosi i kompromitaciju svih računa koji se služe istim korisničkim podacima. Štoviše, u mnogim situacijama korisnici nisu mogli ni utjecati na činjenicu kako su njihovi podaci završili u rukama zlonamjernih korisnika. Sve češća curenja velikog broja korisničkih podataka iz popularnih usluga i servisa dodatno osvještavaju važnost kreiranja zasebnih korisničkih podataka za svaku uslugu, servis i društvenu mrežu.

5. Dijeljenje neprikladnih informacija

Jedna od primarnih svrha društvenih mreža jest i dijeljenje slika, glazbe, ali i osobnih informacija s prijateljima i poznanicima. Međutim, za razliku od fizičkog svijeta u kojem vrijeme briše tragove, virtualni svijet bilježi sve informacije ikad objavljene. Takvim informacijama se može pristupiti veoma brzo, a skup svih objavljenih informacija, kao i onih koje se vezuju uz pojedinog korisnika (poput aktivnosti na društvenim mrežama, navika na internetu ili lokacije) čine digitalni trag koji predstavlja neodvojivi dio identiteta korisnika. Prije dijeljenja informacija treba osvijestiti činjenicu kako se društvene, kulturne norme, ali i vlastita razmišljanja i stavovi korisnika s godinama mijenjaju te je važno uvijek si postaviti pitanje: „Hoću li i za deset godina biti ponosan na ovu sliku ili objavu?“.

ZAŠTITA NA DRUŠTVENIM MREŽAMA

Kako bi se zaštitili od zlonamjernih korisnika, važno je imati na ispravan način podešene postavke sigurnosti. U nastavku možete pronaći neke općenite savjete koji su primjenjivi na gotovo sve društvene mreže:

Snažna lozinka

Snažna lozinka predstavlja temelj sigurnosti korisničkog računa i prvu liniju obrane od zlonamjernih korisnika. Iako smo nekada govorili o tome kako sigurna lozinka može imati i 4 znaka, danas dobrom lozinkom smatramo onu koja ima najmanje 12 znakova te je kombinacija velikih i malih slova, brojki te specijalnih znakova.

Dvostruka autentifikacija

Dvostruka autentifikacija je sigurnosni mehanizam koji prilikom prijave na neku uslugu, servis ili društvenu mrežu od korisnika traži unošenje dodatnog podatka. Uobičajeno je riječ o dodatnom kodu koji se šalje na adresu elektroničke pošte ili na pametni mobitel što dodatno osigurava pristup jer je za kompromitaciju ovako zaštićenog računa potrebno doći i do lozinke i do dodatnog koda.

Ključna pitanja pri korištenju društvenih mreža

- Tko ima pristup informacijama i podacima koje objavljujem na internetu?
- Tko nadzire i u čijem su vlasništvu informacije koje stavljam na stranice društvenih mreža?
- Koje informacije o meni se prosljeđuju putem mojih kontakata drugim osobama?
- Hoće li se moji kontakti protiviti mojem dijeljenju informacija o njima s drugim osobama?
- Vjerujem li svima s kojima sam povezan?

POSTAVKE PRIVATNOSTI I SIGURNOSTI NA DRUŠTVENIM MREŽAMA

Snapchat

Koraci za ispravan način podešavanja postavki privatnosti i sigurnosti:

1. Na glavnom zaslonu aplikacije Snapchat odabir sličice profila u gornjem lijevom kutu;
2. Odabir sličice zupčanika u gornjem desnom kutu;
3. Spuštanjem ovog izbornika dolazi se do opcija pod kategorijom WHO CAN... koje omogućavaju prikaz objava i ostalih informacija samo za prijatelje;
    a) Ograničite vaše Story objave i vašu lokaciju samo na prijatelje;
    b) Onemogućite nepoznatim korisnicima da vas dodaju;
    c) Onemogućite aplikaciji da vas nudi kao prijatelja potencijalnim poznanicima.

Instagram

Koraci za ispravan način podešavanja postavki privatnosti i sigurnosti:

1. Na glavnom zaslonu aplikacije Instagram, u donjem desnom kutu odabir sličice profila;
2. Odabir sličice ☰ koja se nalazi u gornjem desnom kutu te potom opcije Postavke (engl. Settings) u donjem desnom kutu;
3. U ovom prozoru odabir opcije Privatnost i sigurnost (engl. Privacy and security) te zatim Privatnost računa (engl. Account privacy);
4. U ovom prozoru možete onemogućiti ljudima koji nisu vaši prijatelji pregledavanje vaših slika i objava;
5. U prozoru Privatnost i sigurnost se nalaze i ostale sigurnosne opcije koje mogu dodatno doprinijeti sigurnosti vašeg računa poput popisa blokiranih računa i postavki Story objava.

Facebook

Koraci za ispravan način podešavanja postavki privatnosti i sigurnosti:

1. Na naslovnoj stranici odabir strelice za otvaranje padajućeg izbornika u gornjem desnom kutu;
2. Odabir opcije Postavke (engl. Settings) u padajućem izborniku;
3. U traci s desne strane odabir opcije Privatnost (engl. Privacy);
4 U ovom izborniku možete ograničiti vidljivost vaših aktivnosti na vaše prijatelje te ostale postavke privatnosti.

Youtube

Koraci za ispravan način podešavanja postavki privatnosti i sigurnosti:

1. Na naslovnoj stranici odabir sličice profila u gornjem lijevom kutu;
2. Odabir opcije Postavke (engl. Settings);
3. U novom prozoru odabir opcije Privatnost (engl. Privacy) koja se nalazi u traci s desne strane;
4. U ovom izborniku možete ograničiti vidljivost vaših pozitivno ocjenjenih videozapisa, pretplata te popisa za reprodukciju.

POPIS ZA ODRŽAVANJE HIGIJENE NA DRUŠTVENIM STRANICAMA

- Postavke sigurnosti i privatnosti postoje s razlogom.
- Održavajte popis prijatelja čistim.
- Budite iskreni u neugodnim situacijama.
- Znajte kako si pomoći.
- Jednom objavljeno, uvijek objavljeno.
- Vaš virtualni ugled vam može pomoći.
- Držite osobne podatke osobnima.
- Pretpostavka da ste sigurni na društvenim mrežama je kriva.

CERT.hr

Hrvatska akademska i istraživačka mreža

CARNET

Projekt je sufinanciran sredstvima CEF - Connecting Europe Facility programa Europske komisije, broj ugovora: INEA/CEF/ICT/A2016/1334308 (Action No: 2016-HR-IA-0085)

Sufinancirano instrumentom Europske unije za povezivanje Europe