Bezbednost na društvenim mrežama

Imajući u vidu trend rasta sajber napada koji su usmereni na društvene mreže, korisnici bi trebalo da imaju svest o tome da su njihovi podaci, privatnost, novac ili čak njihov lični integritet potencijalno narušeni ili ugroženi, u svakom trenutku.

СРБ-ЦЕРТ

Београд, децембар 2023. године

Sve što drugi ljudi mogu saznati o nama, kao korisnicima društvenih mreža, zapravo je dostupno na našim profilima, sadržaju koji objavljujemo, kao i interakcijama koje imamo sa drugim korisnicima. Ako pogrešno konfigurišemo podešavanje privatnosti profila, postoji šansa da sajber napadač to iskoristi za kreiranje mamaca i učini nas žrtvom sajber napada.

Čak i veoma mali broj javno dostupnih informacija, napadačima omogućava:

- sprečavanje pristupa nalogu na društvenim mrežama
- krađu identiteta
- korišćenje naših naloga ili informacija za kreiranje fišing napada
- zloupotrebu naših finansija ili narušavanje reputacije

Upoznajmo tri tipa sajber napada na društvene mreže:

Malver napadi

Društvene mreže sve učestalije postaju instrumenti za distribuciju malvera. Pretnje poput Crva (eng.*Worm*), Trojanaca (eng.*Trojan virus*) ili Ransomvera (eng. *Ransomware*), se mogu distribuirati neverovatnom brzinom istog trenutka kada se neki nalog na društvenim mrežama inficira. Infekcija se širi na sve kontakte koje korisnik naloga ima u svojoj listi prijatelja. Dalja distribucija se nastavlja na kontakte iz liste svih povezanih kontakata. Ovaj maliciozni program preuzima ili otima informacije u zamenu za otkup, kontroliše sistem i snima lozinke ili aktivne sesije korisnika. Pored navedenog, malveri mogu da naruše performanse inficiranog uređaja.

Krađa podataka

Korisnici razmenjuju različite tipove ličnih podataka koji mogu biti veoma korisni napadačima. Dva najzastupljenija tipa krađe podataka su:

- ***Socijalni inženjering***

Napadači žele da ostvare direktan kontakt sa žrtvom i kroz razgovor prikupe željene informacije, pokušavajući da uspostave što prisniji odnos.

- ***Javno dostupne informacije***

Kao što smo ranije pomenuli, pogrešna podešavanja privatnosti profila, prilikom kreiranja naloga na društvenim mrežama, može napadačima učiniti naše lične podatke lako dostupnim.

Vršnjačko nasilje (eng. Cyberbullying)

Vršnjačko nasilje podrazumeva korišćenje digitalnih komunikacionih medija, sa ciljem uznemiravanja ili maltretiranja osobe ili grupe korisnika. Vršnjačko nasilje se širi svim kanalima društvenih mreža i veoma ga je teško zaustaviti.

Uzimajući u obzir navedene mogućnosti, od vitalnog je značaja učiniti društvene mreže bezbednijim okruženjem.

Kako se možemo zaštititi na društvenim mrežama?

Imajući u vidu pomenuta scenarija mogućih zloupotreba društvenih mreža u prethodnoj lekciji, njihovo korišćenje može zvučati veoma nebezbedno. Prvi korak koji je neophodno preduzeti jeste da se korisnici prethodno dobro upoznaju sa temom društvenih mreža, kao i da se upoznaju sa merama prevencije za bezbednije korišćenje interneta. Upravo zbog toga ćemo podeliti neke od preporuka i primera dobre prakse koje će vam, uz odgovarajuću primenu, pružiti odgovarajući nivo zaštite.

Osnovne preporuke za zaštitu su:

- **Ispravno kreiranje korisničkog profila:**

Početna, podrazumevana, podešavanja profila na društvenim mrežama nisu obavezno usaglašena i sa osnovnim bezbednosnim preporukama. Upravo iz tog razloga je preporuka svim korisnicima da odvoje dovoljno vremena i pažljivo se upoznaju sa svim detaljima u vezi sa mogućim izazovima ukoliko dođe do neovlašćenog preuzimanja ličnih podataka sa nekog naloga na društvenim mrežama na kojem je korisnik samo prihvatio ponuđena podrazumevana podešavanja.

- **Koristite bezbednosna rešenja:**

Trebalo bi koristiti antivirusni softver koji ima mogućnost identifikacije, kao i ažuriranu bazu potpisa. Rešenja poput Antispam i Zaštitnog zida (eng. *Firewall*) takođe mogu dodatno optimizovati bezbednosna podešavanja za odbranu sistema od mogućih rizika.

- **Briga o lozinkama:**

Lozinke su ključ digitalnih identiteta. Evo nekih preporuka za njihovu zaštitu:

- Ne deliti svoje lozinke sa drugim licima

- Ne koristiti istu lozinku za pristup nalogu na društvenim mrežama za pristup nekoj drugoj internet stranici
-
- Kreirajte kompleksne lozinke koje se ne mogu lako otkriti. Na primer, ne treba kreirati lozinku koja sadrži ime korisnika ili neke svakodnevne reči

- Omogućite multifaktorsku autentifikaciju kad god je moguće. Kreirajte dodatni korak provere identiteta korisnika. Primenom kombinacije nečega što korisnik zna (lozinku), nečega što korisnik ima (bezbednosni kod koji stiže putem SMS-a ili token), kao i nečega što korisnik jeste (biometrijski podatak poput otiska prsta ili mrežnjače oka), značajno se umanjuje mogućnost da se korisniku preotme nalog.

- Da li periodično obnavljate svoje lozinke? Neki eksperti smatraju da nije neophodno periodično menjati lozinku sve dok:
  - ne utvrdite da je ona otkrivena od strane drugih lica,
  - je dovoljno kompleksna i
  - je omogućena multifaktorska autentifikacija.

  Drugi su mišljenja da, što je više potrebno da zaštitite svoju lozinku, postoji veća potreba i da je periodično menjate. Smatraju da lozinke treba menjati svaka tri meseca, jer na taj način možete biti sigurni da, ukoliko je vaša lozinka možda otkrivena, umanjujete period zloupotrebe određenog naloga koji je hakovan. Imajući u vidu pomenuta dva mišljenja, predlog je pratiti sve prethodno navedene preporuke što podrazumeva pažljivo kreiranje korisničkog profila, zaštita od mogućeg ''curenja'' ličnih podataka, kao i izmena lozinki kad god se to učini neophodnim.

Takođe je neophodno imati na umu i sledeće preporuke:

- Izbegavanje korišćenja tuđih računara za prijavljivanje na naloge društvenih mreža.

- Uvek se odjaviti sa svog naloga kada se ne koristi, jer se na taj način onemogućava da neko drugi preuzme sesiju.

- Pažljivo sa klikom na ponuđene reklame ili sadržaj koji nudi obavezno preuzimanje (eng. *download*), ili link koji preusmerava na neku drugu internet stranicu. Važno je znati da ovakvi vidovi prevara mogu biti mamac za socijalni inženjering.

- Ne koristiti korisničke naloge kojima je dozvoljeno upravljanje drugim aplikacijama i servisima, dok ste na mreži.

- Ukoliko pretražujete internet, pokušajte to da radite koristeći *HTTPS* protokol.

Ukoliko se redovno primenjuju navedene preporuke, minimizovaće se bilo kakve posledice mogućeg hakerskog napada.

Kako mogu proveriti da li mi je nalog hakovan?

Postoji nekoliko načina uz pomoć kojih se može utvrditi da li je hakovan nalog korisnika. Nažalost, u slučaju hakovanja većeg broja naloga na društvenim mrežama, servis ne obaveštava svakog korisnika pojedinačno da je došlo do neovlašćenog preuzimanja naloga.

Ukoliko se primete neuobičajene aktivnosti na profilu, ili posumnja da je došlo do neovlašćenog pristupa nalogu korisnika, prvo što se može uraditi je provera istorije sesija naloga. Ovu opcija je najčešće dostupna u sekciji ''Opšta podešavanja i privatnost'' (eng. *Settings and Privacy*), a nakon toga se odabere opcija ''Bezbednost i prijava'' (eng. *Security and Login*). Tu se može pronaći sve o listi uređaja i informacije koje su u vezi sa prijavom, a gde je korišćeno konkretno korisničko ime i lozinka. Ukoliko se zaključi da se na listi nalazi nešto što nije u redu, preporuka je da se odmah promeni lozinka za taj nalog. Dodatna preporuka je da se obavesti i korisnički centar određene društvene mreže da je došlo do sumnjivih aktivnosti na nalogu, ili da je nalog neovlašćeno preuzet.

Sa druge strane, dobra vest je da postoje i drugi servisi koji prikupljaju informacije o mogućim zloupotrebama korisničkih naloga i lozinki, koji omogućavaju korisnicima da provere da li je njihov nalog kompromitovan. Najpopularniji servis je ''*Have I been Pwnd?*''. Već dugo godina ova internet stranica prikuplja informacije o svim kompromitacijama korisničkih naloga i omogućava nam da proverimo da li ima zabeleženih podataka o našem korisničkom nalogu. Veoma je jednostavna za korišćenje. Dovoljno je uneti vašu imejl adresu i ukoliko se vaša adresa pojavi na listi ugroženih naloga videćete poruku upozorenja da je vaša imejl adresa kompromitovana.

Šta treba da uradim ukoliko mi je nalog kompromitovan?

Jednom kada utvrdimo da je naš nalog kompromitovan, što brže reagujemo, bićemo izloženi manjem broju rizika i negativnih posledica. Od vitalnog je značaja brzina reagovanja. Postoji nekoliko preporuka koje treba odmah primeniti, kako bismo sprečili da naši lični podaci padnu u pogrešne ruke.

1. Pokušajte da opozovete izmene imejl adrese.

Kada izmenite imejl koji je povezan sa vašim profilom, platforma na društvenim mrežama će vam poslati imejl obaveštenja, na originalnu imejl adresu, sa informacijom da je došlo do izmene. Taj imejl sadrži link koji vam omogućava da opozovete unete izmene. Preporučujemo vam da iskoristite ovu opciju, ukoliko ste sigurni da ste imejl dobili od legitimne platforme konkretne društvene mreže. Da biste bili sigurni da je imejl legitiman, možete proveriti na forumu ili instrukcijama konkretne platforme za društvene mreže, koje informacije su sadržane u legitimnim imejlovima

i sa kog imejl naloga bi trebalo da dobijete takvo obaveštenje. Takođe vam preporučujemo da ne kliknete na ponuđeni link u mejlu, već da ga prekopirate u neki dokument poput *Word* dokumenta, kako biste utvrdili da li je *URL* adresa legitimna, ili vas preusmerava na neku lažnu internet stranicu. Dobar znak je ukoliko ponuđena *URL* adresa počinje nazivom konkretne društvene mreže.

2. Ne tražite od drugih da prijave vaš problem sa nalogom.

Mnogi često zamole svoje kontakte da umesto njih prijave problem sa profilom, kao ''*Spam*'' ili ''*Inappropriate*''. Ovakav način prijave problema je beskoristan za povraćaj naloga, a može i rezultirati gašenjem profila, jer prijave stižu od većeg broja korisnika.

3. Zahtevajte link za oporavak profila.

Na formi za unos korisničkog imena i lozinke, obično možete pronaći link preko kojeg možete zatražiti podršku korisničkog servisa. Klikom na taj link, biće vam poslat bezbednosni kod za oporavak profila putem imejla ili SMS poruke. Ukoliko ste zakasnili za ovakav vid oporavka, važno je znati da će vaš zahtev ostati upamćen od strane platforme konkretne društvene mreže i upravo taj zahtev vam može pomoći prilikom rešavanja spora, ukoliko do toga dođe.

4. Prijavite hakovanje profila.

Potrebno je da korisnik prijavi hakovanje profila kako bi agent, koji radi na platformi konkretne društvene mreže, mogao detaljnije da istraži slučaj. Moguće je popuniti dostupnu elektronsku formu, ili kontaktirati korisnički servis konkretne platforme putem imejla. U produžetku možete naći nekoliko linkova koji vode ka pomenutim formama:

- Fejsbuk
- Instagram
- Tviter
- Linkedin

Čest je slučaj u kojem hakeri promene ime i naziv profila kako korisnik više ne bi mogao da prati ili prijavi zloupotrebu naloga. Ukoliko dođe do preuzimanja profila, moguće je zamoliti nekog od pratilaca da pomogne u identifikovanju novog naziva otetog korisničkog profila i zamoliti ih da pošalju snimak ekrana na kojem se vidi sadašnji naziv profila. Važno je da se pre obraćanja korisničkom servisu prikupi što više informacija poput:

- Korisničkog imena (naziva profila) pre njegovog neovlašćenog preuzimanja

- Trenutni naziv profila (ako je došlo do izmene naziva)

- Snimak ekrana na kojem se vide podaci korisnika na profilu pre neovlašćenog preuzimanja profilaнеовлашћеног преузимања профила

- Snimak ekrana hakovanog profila

- Broj telefona i imejl adresa koji su bili deo profila pre njegovog neovlašćenog preuzimanja

- Opis događaja koji bi trebalo da sadrži: datum i vreme kada je ustanovljeno da je profil hakovan. Takve informacije obično korisnici dobijaju putem notifikacionog imejla koji ih obaveštava o prijavama na profil sa drugog uređaja, ili o izmeni imejl adrese

- Snimak ekrana na kojem se vidi prijem imejl notifikacije kojom je korisnik obavešteni da je došlo do prijave sa drugog uređaja, ili izmene imejl adrese, pri čemu je važno uneti tačno vreme i datum imajući u vidu informaciju o vremenskoj (UTC) zoni u kojoj se nalazi korisnik

- Pripremiti listu svih uređaja sa kojih je korisnik pristupao svom profilu. Potrebno je navesti tip, model, marku i verziju operativnog sistema uređaja.

Takođe je neophodno priložiti fotografiju na kojoj se može videti lice korisnika i identifikacioni dokument sa fotografijom. U suprotnom, zahtev može biti odbijen kao nepotpun.

Ukoliko korisnik prosledi imejl korisničkoj podršci, važno je da se imejl pošalje na maternjem i engleskom jeziku, kako bi se ubrzao proces. Naslov imejla bi trebalo da bude na engleskom jeziku i da glasi kao na primeru:
Account@nickname hacked on 2/nov/2022, details in message.

Tekst poruke treba da sadrži sve pomenute detalje, kao i priložene fotografije identifikacionog dokumenta i slike ekrana o profilu korisnika.

Preporuka je ne odgovarati na zahteve napadača, ili plaćati iznos za povraćaj svog profila, jer je praksa pokazala da nalog najčešće ostaje trajno hakovan.

Trebalo bi da znamo da je velika verovatnoća da će neki profil, identitet ili sadržaj na društvenim mrežama biti hakovan. Iz tog razloga preporučujemo da se ne unose osetljivi podaci ili sadržaj koji vas može kompromitovati, kao ni informacije koje mogu biti upotrebljene protiv vas. Važno je imati na umu da bilo koji nalog ili uređaj mogu biti hakovani i da se ljudi često mogu lažno predstavljati na internetu.