Безбедност на друштвеним мрежама

Имајући у виду тренд раста сајбер напада који су усмерени на друштвене мреже, корисници би требало да имају свест о томе да су њихови подаци, приватност, новац или чак њихов лични интегритет потенцијално нарушени или угрожени, у сваком тренутку.

СРБ-ЦЕРТ

Београд, децембар 2022.

Све што други људи могу сазнати о нама, као корисницима друштвених мрежа, заправо је доступно на нашим профилима, садржају који објављујемо, као и интеракцијама које имамо са другим корисницима. Ако погрешно конфигуришемо подешавање приватности профила, постоји шанса да сајбер нападач то искористи за креирање мамаца и учини нас жртвом сајбер напада.

Чак и веома мали број јавно доступних информација, нападачима омогућава:

- спречавање приступа налогу на друштвеним мрежама
- крађу идентитета
- коришћење наших налога или информација за креирање фишинг напада
- злоупотребу наших финансија или нарушавање репутације

Упознајмо три типа сајбер напада на друштвене мреже:

Малвер напади

Друштвене мреже све учесталије постају инструменти за дистрибуцију малвера. Претње попут Црва (енг.Worm), Тројанаца (енг.Trojan virus) или Рансомвера (енг. Ransomware), се могу дистрибуирати невероватном брзином истог тренутка када се неки налог на друштвеним мрежама инфицира. Инфекција се шири на све контакте које корисник налога има у својој листи пријатеља. Даља дистрибуција се наставља на контакте из листе свих повезаних контаката. Овај малициозни програм преузима или отима информације у замену за откуп, контролише систем и снима лозинке или активне сесије корисника. Поред наведеног, малвери могу да наруше перформансе инфицираног уређаја.

Крађа података

Корисници размењују различите типове личних података који могу бити веома корисни нападачима. Два најзаступљенија типа крађе података су:

- ***Социјални инжењеринг***

Нападачи желе да остваре директан контакт са жртвом и кроз разговор прикупе жељене информације, покушавајући да успоставе што присније однос.

- ***Јавно доступне информације***

Као што смо раније поменули, погрешна подешавања приватности профила, приликом креирања налога на друштвеним мрежама, може нападачима учинити наше личне податке лако доступним.

Вршњачко насиље (енг. *Cyberbullying*)

Вршњачко насиље подразумева коришћење дигиталних комуникационих медија, са циљем узнемиравања или малтретирања особе или групе корисника. Вршњачко насиље се шири свим каналима друштвених мрежа и веома га је тешко зауставити.

Узимајући у обзир наведене могућности, од виталног је значаја учинити друштвене мреже безбеднијим окружењем.

Како се можемо заштитити на друштвеним мрежама?

Имајући у виду поменута сценарија могућих злоупотреба друштвених мрежа у претходној лекцији, њихово коришћење може звучати веома небезбедно. Први корак који је неопходно предузети јесте да се корисници претходно добро упознају са темом друштвених мрежа, као и да се упознају са мерама превенције за безбедније коришћење интернета. Управо због тога ћемо поделити неке од препорука и примера добре праксе које ће вам, уз одговарајућу примену, пружити одговарајући ниво заштите.

Основне препоруке за заштиту су:

- **Исправно креирање корисничког профила:**

Почетна, подразумевана, подешавања профила на друштвеним мрежама нису обавезно усаглашена и са основним безбедносним препорукама. Управо из тог разлога је препорука свим корисницима да одвоје довољно времена и пажљиво се упознају са свим детаљима у вези са могућим изазовима уколико дође до неовлашћеног преузимања личних података са неког налога на друштвеним мрежама на којем је корисник само прихватио понуђена подразумевана подешавања.

- **Користите безбедносна решења:**

Требало би користити антивирусни софтвер који има могућност идентификације, као и ажурирану базу потписа. Решења попут Антиспам и Заштитног зида (енг. *Firewall*) такође могу додатно оптимизовати безбедносна подешавања за одбрану система од могућих ризика.

- **Брига о лозинкама:**

Лозинке су кључ дигиталних идентитета. Ево неких препорука за њихову заштиту:

- Не делити своје лозинке са другим лицима
- Не користити исту лозинку за приступ налогу на друштвеним мрежама за приступ некој другој интернет страници
- Креирајте комплексне лозинке које се не могу лако открити. На пример, не треба креирати лозинку која садржи име корисника или неке свакодневне речи
- Омогућите мултифакторску аутентификацију кад год је могуће. Креирајте додатни корак провере идентитета корисника. Применом комбинације нечега што корисник зна (лозинку), нечега што корисник има (безбедносни код који стиже путем СМС-а или токен), као и нечега што корисник јесте (биометријски податак попут отиска приста или мрежњаче ока), значајно се умањује могућност да се кориснику преотме налог.
- Да ли периодично обнављате своје лозинке? Неки експерти сматрају да није неопходно периодично мењати лозинку све док:
  - не утврдите да је она откривена од стране других лица,
  - је довољно комплексна и
  - је омогућена мултифакторска аутентификација.

Други су мишљења да, што је више потребно да заштитите своју лозинку, постоји већа потреба и да је периодично мењате. Сматрају да лозинке треба мењати свака три месеца, јер на тај начин можете бити сигурни да, уколико је ваша лозинка можда откривена, умањујете период злоупотребе одређеног налога који је хакован. Имајући у виду поменута два мишљења, предлог је пратити све претходно наведене препоруке што подразумева пажљиво креирање корисничког профила, заштита од могућег ''цурења'' личних података, као и измена лозинки кад год се то учини неопходним.

Такође је неопходно имати на уму и следеће препоруке:

- Избегавање коришћења туђих рачунара за пријављивање на налоге друштвених мрежа.
- Увек се одјавити са свог налога када се не користи, јер се на тај начин онемогућава да неко други преузме сесију.
- Пажљиво са кликом на понуђене рекламе или садржај који нуди обавезно преузимање (енг. *download*), или линк који преусмерава на неку другу интернет страницу. Важно је знати да овакви видови превара могу бити мамац за социјални инжењеринг.
- Не користити корисничке налоге којима је дозвољено управљање другим апликацијама и сервисима, док сте на мрежи.
- Уколико претражујете интернет, покушајте то да радите користећи *HTTPS* протокол.

Уколико се редовно примењују наведене препоруке, минимизоваће се било какве последице могућег хакерског напада.

Како могу проверити да ли ми је налог хакован?

Постоји неколико начина уз помоћ којих се може утврдити да ли је хакован налог корисника. Нажалост, у случају хаковања већег броја налога на друштвеним мрежама, сервис не обавештава сваког корисника појединачно да је дошло до неовлашћеног преузимања налога.

Уколико се примете неуобичајене активности на профилу, или посумња да је дошло до неовлашћеног приступа налогу корисника, прво што се може урадити је провера историје сесија налога. Ову опција је најчешће доступна у секцији ''Општа подешавања и приватност'' (енг. *Settings and Privacy*), а након тога се одабере опција ''Безбедност и пријава'' (енг. *Security and Login*). Ту се може пронаћи све о листи уређаја и информације које су у вези са пријавом, а где је коришћено конкретно корисничко име и лозинка. Уколико се закључи да се на листи налази нешто што није у реду, препорука је да се одмах промени лозинка за тај налог. Додатна препорука је да се обавести и кориснички центар одређене друштвене мреже да је дошло до сумњивих активности на налогу, или да је налог неовлашћено преузет.

Са друге стране, добра вест је да постоје и други сервиси који прикупљају информације о могућим злоупотребама корисничких налога и лозинки, који омогућавају корисницима да провере да ли је њихов налог компромитован. Најпопуларнији сервис је *''Have I been Pwnd?''*. Већ дуго година ова интернет страница прикупља информације о свим компромитацијама корисничких налога и омогућава нам да проверимо да ли има забележених података о нашем корисничком налогу. Веома је једноставна за коришћење. Довољно је унети вашу имејл адресу и уколико се ваша адреса појави на листи угрожених налога видећете поруку упозорења да је ваша имејл адреса компромитована.

Шта треба да урадим уколико ми је налог компромитован?

Једном када утврдимо да је наш налог компромитован, што брже реагујемо, бићемо изложени мањем броју ризика и негативних последица. Од виталног је значаја брзина реаговања. Постоји неколико препорука које треба одмах применити, како бисмо спречили да наши лични подаци падну у погрешне руке.

1. Покушајте да опозовете измене имејл адресе

Када измените имејл који је повезан са вашим профилом, платформа на друштвеним мрежама ће вам послати имејл обавештења, на оригиналну имејл адресу, са информацијом да је дошло до измене. Тај имејл садржи линк који вам омогућава да опозовете унете измене.

Препоручујемо вам да искористите ову опцију, уколико сте сигурни да сте имејл добили од легитимне платформе конкретне друштвене мреже. Да бисте били сигурни да је имејл легитиман, можете проверити на форуму или инструкцијама конкретне платформе за друштвене мреже, које информације су садржане у легитимним имејловима и са ког имејл налога би требало да добијете такво обавештење. Такође вам препоручујемо да не кликнете на понуђени линк у мејлу, већ да га прекопирате у неки документ попут *Word* документа, како бисте утврдили да ли је *URL* адреса легитимна, или вас преусмерава на неку лажну интернет страницу. Добар знак је уколико понуђена *URL* адреса почиње називом конкретне друштвене мреже.

2. Не тражите од других да пријаве ваш проблем са налогом.

Многи често замоле своје контакте да уместо њих пријаве проблем са профилом, као *''Spam''* или *''Inappropriate''*. Овакав начин пријаве проблема је бескористан за повраћај налога, а може и резултирати гашењем профила, јер пријаве стижу од већег броја корисника.

3. Захтевајте линк за опоравак профила.

На форми за унос корисничког имена и лозинке, обично можете пронаћи линк преко којег можете затражити подршку корисничког сервиса. Кликом на тај линк, биће вам послат безбедносни код за опоравак профила путем имејла или СМС поруке. Уколико сте закаснили за овакав вид опоравка, важно је знати да ће ваш захтев остати упамћен од стране платформе конкретне друштвене мреже и управо тај захтев вам може помоћи приликом решавања спора, уколико до тога дође.

4. Пријавите хаковање профила.

Потребно је да корисник пријави хаковање профила како би агент, који ради на платформи конкретне друштвене мреже, могао детаљније да истражи случај. Могуће је попунити доступну електронску форму, или контактирати кориснички сервис конкретне платформе путем имејла. У продужетку можете наћи неколико линкова који воде ка поменутим формама:

- Фејсбук
- Инстаграм
- Твитер
- Линкедин

Чест је случај у којем хакери промене име и назив профила како корисник више не би могао да прати или пријави злоупотребу налога. Уколико дође до преузимања профила, могуће је замолити неког од пратилаца да помогне у идентификовању новог назива отетог корисничког профила и замолити их да пошаљу снимак екрана на којем се види садашњи назив профила.

Важно је да се пре обраћања корисничком сервису прикупи што више информација попут:

- Корисничког имена (назива профила) пре његовог неовлашћеног преузимања
- Тренутни назив профила (ако је дошло до измене назива)
- Снимак екрана на којем се виде подаци корисника на профилу пре неовлашћеног преузимања профила
- Снимак екрана хакованог профила
- Број телефона и имејл адреса који су били део профила пре његовог неовлашћеног преузимања
- Опис догађаја који би требало да садржи: датум и време када је установљено да је профил хакован. Такве информације обично корисници добијају путем нотификационог имејла који их обавештава о пријавама на профил са другог уређаја, или о измени имејл адресе
- Снимак екрана на којем се види пријем имејл нотификације којом је корисник обавештени да је дошло до пријаве са другог уређаја, или измене имејл адресе, при чему је важно унети тачно време и датум имајући у виду информацију о временској (*UTC*) зони у којој се налази корисник
- Припремити листу свих уређаја са којих је корисник приступао свом профилу. Потребно је навести тип, модел, марку и верзију оперативног система уређаја.

Такође је неопходно приложити фотографију на којој се може видети лице корисника и идентификациони документ са фотографијом. У супротном, захтев може бити одбијен као непотпун.

Уколико корисник проследи имејл корисничкој подршци, важно је да се имејл пошаље на матерњем и енглеском језику, како би се убрзао процес. Наслов имејла би требало да буде на енглеском језику и да гласи као на примеру: **Account@nickname hacked on 2/nov/2022, details in message.**

Текст поруке треба да садржи све поменуте детаље, као и приложене фотографије идентификационог документа и слике екрана о профилу корисника.

Препорука је не одговарати на захтеве нападача, или плаћати износ за повраћај свог профила, јер је пракса показала да налог најчешће остаје трајно хакован.

Требало би да знамо да је велика вероватноћа да ће неки профил, идентитет или садржај на друштвеним мрежама бити хакован. Из тог разлога препоручујемо да се не уносе осетљиви подаци или садржај који вас може компромитовати, као ни информације које могу бити употребљене против вас. Важно је имати на уму да било који налог или уређај могу бити хаковани и да се људи често могу лажно представљати на интернету.