KAKO POSTUPITI UKOLIKO DOĐE DO KOMPROMITOVANJA ELEKTRONSKE POŠTE I KAKO ZAŠTITITI NALOGE

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU:
HTTPS://WWW.CERT.RS/RS/PRIJAVA.HTML

SRB-CERT

Komunikacija posredstvom elektronske pošte (*e-mail*) odvija se godinama unazad i predstavlja efikasan i jednostavan način razmene poruka kako u cilju lične tako i profesionalne komunikacije.

Masovnost upotrebe elektronske pošte, korišćenje naloga elektronske pošte za pristup društvenim mrežama (*Facebook*, *Instagram*, *LinkedIn* itd.) ili za prijem izvoda stanja na bankovnom računu kao i za pristup različitim aplikacijama i sajtovima, za napadače predstavlja vredan resurs, jer pristupom nalogu elektronske pošte (korisničkom imenu i lozinki) mogu doći u posed ličnih i poverljivih podataka o korisniku.

Kada se određeni korisnik interneta nađe u situaciji da su napadači neovlašćeno pristupili njegovom nalogu elektronske pošte, postoje koraci koje je moguće preduzeti a koji bi korisniku omogućili ponovni pristup nalogu koji je prethodno bio kompromitovan, kao i smernice o načinima zaštite naloga kako se korisnik ne bi našao u situaciji da ostane bez pristupa svom nalogu elektronske pošte.

RAZLOZI ZBOG KOJIH JE ELEKTRONSKA POŠTA META NAPADAČA

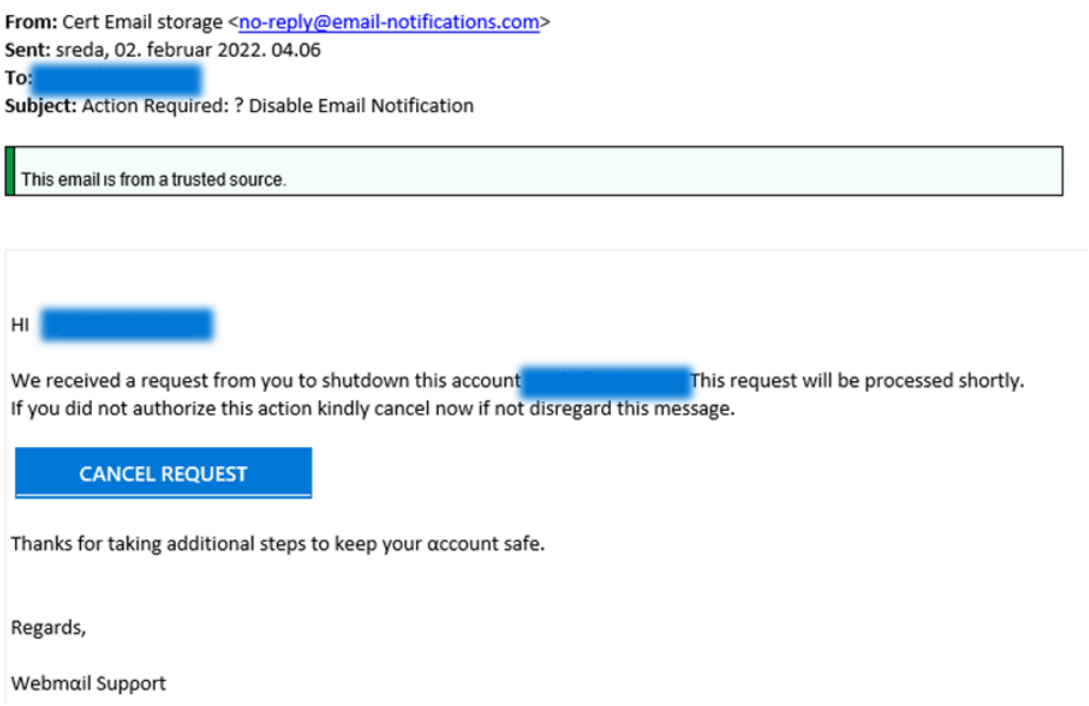
Najčešći razlozi zbog kojih je elektronska pošta meta napadača su:

- Ukoliko napadač preuzme nalog elektronske pošte korisnika to mu može omogućiti pristup podacima na drugim nalozima, na primer može doći do podataka korisnika na društvenim mrežama ako je nalog kreiran na osnovu te adrese ili može pristupiti svim privatnim fajlovima korisnika na *Dropbox-u*, *Google Drive-u* i drugim servisima za skladištenje fajlova, i na taj način napadač dobija pristup ličnim informacijama korisnika.
- Neovlašćenim pristupanjem nalogu elektronske pošte korisnika, napadači imaju mogućnost da resetuju lozinke i pristupe svim drugim nalozima korisnika, obzirom da većina internet sajtova i aplikacija na adresu elektronske pošte šalje link za resetovanje lozinke, čime jednim klikom napadači mogu promeniti lozinke svih drugih naloga korisnika.
- Kada napadač pristupi nalogu elektronske pošte korisnika, to mu omogućava uvid u prepiske i listu kontakata (članovi porodice, prijatelji ili poslovni partneri) što napadači dalje mogu iskoristiti za slanje neželjene elektronske pošte, najčešće kroz fišing poruke, sa ciljem kompromitovanja što većeg broja naloga.

KOJI SU NAČINI NA KOJE NAPADAČI MOGU NEOVLAŠĆENO PRISTUPITI ELEKTRONSKOJ POŠTI?

Napadači najčešće koriste sledeće načine kako bi neovlašćeno pristupili elektronskoj pošti korisnika:

- Slanjem poruka posredstvom elektronske pošte koja je kreirana tako da izgleda kao da je poslata iz legitimnog izvora, npr. od strane provajdera elektronske pošte (*Gmail*, *Yahoo*, *Microsoft Outlook* itd.), gde se od korisnika zahteva da se opet prijavi na nalog. Najčešće je ta poruka kreirana sa elementima hitnosti, gde se u kratkom roku zahteva prijava na nalog, na primer kako bi korisnik izbegao gubitak podataka, gašenje naloga ili kako bi promenio lozinku jer je navodno druga osoba pokušala da pristupi nalogu korisnika.



From: Cert Email storage <no-reply@email-notifications.com>
Sent: sreda, 02. februar 2022. 04.06
To: [redacted]
Subject: Action Required: ? Disable Email Notification

This email is from a trusted source.

HI [redacted]

We received a request from you to shutdown this account [redacted] This request will be processed shortly.
If you did not authorize this action kindly cancel now if not disregard this message.

CANCEL REQUEST

Thanks for taking additional steps to keep your account safe.

Regards,

Webmail Support

Slika 1 – Primer e-pošte o navodnom gašenju naloga korisnika

- *Brute Force* napadi koji podrazumevaju pokušaj pristupa sistemu žrtve neprekidnim logovanjem različitim kombinacijama slova, brojeva i simbola sa ciljem identifikacije korisničkog imena i lozinke.
- Kada korisnik pristupa elektronskoj pošti korišćenjem javne bežične mreže (*Wi-Fi*), napadači mogu da presretnu njihov pristup internetu čime dobijaju uvid u kompletan saobraćaj i mogu da preuzmu poverljive podatke ili identitet korisnika.
- Preuzimanjem zlonamernog softvera (malvera) kroz poruke elektronske pošte iz neproverenih izvora (najčešće su u pitanju fišing poruke).

KAKO KORISNIK MOŽE PROVERITI DA LI JE NEKO NEOVLAŠĆENO PRISTUPIO NJEGOVOM NALOGU ELEKTRONSKE POŠTE?

Sledeći primeri ilustruju situacije u kojima je najverovatnije došlo do neovlašćenog preuzimanja naloga elektronske pošte od strane napadača:

- Očigledan pokazatelj da je nalog kompromitovan jeste ukoliko korisnik ne može da pristupi nalogu uz obaveštenje da je lozinka promenjena;
- Prijatelji i kolege primaju neželjenu poštu koja dolazi sa adrese elektronske pošte korisnika koji sumnja da mu je nalog kompromitovan;
- Prijem više uzastopnih zahteva za promenom lozinke sa drugih internet stranica i aplikacija;
- Provajder elektronske pošte (*Gmail*, *Yahoo*, *Microsoft Outlook* itd.) obaveštava korisnika o višestrukim prijavama sa nepoznatih IP adresa i lokacija.

KORACI KOJE JE MOGUĆE PREDUZETI UKOLIKO JE DOŠLO DO NEOVLAŠĆENOG PREUZIMANJA NALOGA ELEKTRONSKE POŠTE

Ukoliko korisnik ima i dalje pristup nalogu, potrebno je u najkraćem roku:

- Promeniti lozinku kompromitovane elektronske pošte kao i sve lozinke na nalozima gde se ova adresa koristila kao i prateća sigurnosa pitanja koja su vezana za konkretan nalog;
- Aktivirati antivirus, klikom na „*full scan*";
- U okviru sekcije podešavanja proveriti da li su promenjeni prethodno definisani parametri.

Ako korisnik nema pristup nalogu, i lozinka je promenjena od strane napadača, potrebno je započeti proceduru oporavka. U određenim slučajevima nalog je moguće oporaviti koristeći metode vraćanja naloga kao što su korišćenje sekundarne adrese elektronske pošte, broja telefona ili odgovorom na sigurnosna pitanja. Provajder elektronske pošte će korisniku omogućiti link sa lozinkom za vraćanje naloga na sekundarnu adresu elektronske pošte, ili poruku na mobilni telefon sa ciljem vraćanja naloga.

Procedure za oporavak naloga elektronske pošte, za različite provajdere, se nalaze na sledećim linkovima:

- Gmail
- Microsoft Outlook
- Yahoo

Međutim, ukoliko su napadači izmenili podatke za pristup nalogu, potrebno je kontaktirati podršku u cilju dobijanja informacija o dodatnim koracima dokazivanja identiteta korisnika što može biti dugotrajan proces, a ne mora se uvek završiti uspešno – odnosno vraćanjem naloga korisniku. Iz tog razloga neophodno je preduzeti sve korake da se elektronska pošta zaštiti od neovlašćenog pristupa.

KAKO ZAŠTITITI ELEKTRONSKU POŠTU OD NEOVLAŠĆENOG PRISTUPA?

Slika 2 - Koraci zaštite naloga elektronske pošte

1. Kreiranje kompleksnih lozinki

Jedan od načina zaštite naloga, koji smanjuje mogućnost neovlašćenog pristupa ličnim i osetljivim podacima korisnika jeste kreiranje kompleksnih lozinki.

Osnovne smernice za kreiranje sigurnih lozinki su:

- Korišćenje najmanje 9 alfanumeričkih karaktera i to:

  - malih slova (a-z)

  - velikih slova (A-Z)

  - brojeva (0-9)

  - znakova (!@#$%^&*)

- Lozinka ne bi trebalo da sadrži lične podatke (ime, prezime, nadimak, datum rođenja, ime kućnog ljubimca itd.)
- Prilikom kreiranja lozinki ne koristiti sekvence sa tastature (deo reda na tastaturi kao što su qwerty, 123456 itd.)
- Ne koristiti istu lozinku za više naloga.

Lozinka treba da sadrži svaki od preporučenih slovnih ili znakovnih karaktera, kako bi složenost lozinke bila što veća čime bi se otežao neovlašćeni pristup.

2. Korišćenje dvofaktorske autentifikacije

Korišćenjem dvofaktorske autentifikacije obezbeđuje se dodatan nivo bezbednosti što se naloga tiče, obzirom da podrazumeva postojanje više koraka provere kako bi korisnik dokazao identitet, odnosno da je zapravo korisnik taj koji pristupa nalogu. Na primer, za prijavu na nalog elektronske pošte pored lozinke, korisnik će dobiti sigurnosni kod putem SMS poruke čijim unošenjem dokazuje identitet i pristupa nalogu. Dvofaktorska autentifikacija podrazumeva kombinovanje dva načina od sledeća četiri:

- Ono što znam (lozinka, PIN)
- Ono što imam (token, kartice, mobilni telefon)
- Ono što jesam (otisak prsta, prepoznavanje lica, oka...)
- Ono što radim (govor)

3. Prilikom korišćenja otvorenog bežičnog interneta (*Wi-Fi*), odnosno javno dostupnih tačaka za pristup internetu treba biti dodatno obazriv

Besplatan pristup bežičnom internetu predstavlja sve rasprostranjeniju uslugu koja se nudi korisnicima ugostiteljskih objekata, hotela, tržnih centara, aerodroma, čak i vozila javnog prevoza. Veliki broj korisnika svakodnevno koristi besplatan pristup bežičnom internetu za različite potrebe - za pristup društvenim mrežama, elektronskoj pošti ili na primer za „rad na daljinu“ u omiljenom kafe baru. Većina korisnika nije svesna da su na taj način izloženi riziku od gubitaka podataka, kao što su fotografije, poruke, lični podaci, lozinke i informacije o bankovnim računima. Veoma rasprostranjen tip sajber napada prilikom korišćenja javnih bežičnih mreža jeste tzv. „čovek u sredini“ (eng. ***Man-in-the-middle - MITM***), gde je napadačima cilj da budu u istoj mreži sa drugim korisnicima i presretnu njihov pristup internetu čime dobijaju uvid u kompletan saobraćaj i mogu da preuzmu poverljive podatke ili identitet korisnika.

Napadači takođe mogu lako kreirati lažno pristupno mesto (hotspot) za bežičnu javnu mrežu, koja imitira mrežu nekog ugostiteljskog ili drugog objekta - gde je najčešće slobodan pristup ili su šifre lako dostupne i retko se menjaju. To omogućava napadaču da postavi zamku sa nazivom mreže koja liči na naziv ugostiteljskog objekta, ili nazivom kao što je “Besplatan *Wi-Fi*“. Kada se korisnik poveže na pristupnu tačku, kreiranu na ovakav način, za besplatan bežični internet, tada napadač dobija pristup osetljivim podacima korisnika.

Najbolji način da se zaštite poverljivi podaci prilikom korišćenja javnih bežičnih mreža je da se izbegava pristupanje nalozima elektronske pošte, društvenih mreža ili obavljanje finansijskih transakcija.

4. Voditi računa prilikom prijema poruka koje u sebi sadrže priloge ili linkove

Fišing je tip prevare koja za cilj ima prikupljanje i zloupotrebu poverljivih podataka korisnika, poput brojeva bankovnih računa, lozinki naloga na društvenim mrežama ili pristupa elektronskoj pošti. Jedan broj fišing napada ima za cilj krađu kredencijala, dok drugi imaju za cilj distribuciju zlonamernog softvera. Fišing poruke najčešće se distribuiraju putem poruka elektronske pošte i kreirane su sa namerom da izgledaju kao da su poslate iz pouzdanih izvora, dok je tekst poruke takav da stvara osećaj znatiželje, straha ili hitnosti s ciljem navođenja primaoca poruke da brzo reaguje – klikom na određeni link ili preuzimanjem dokumenata iz priloga. Klik na link vodi na lažnu stranicu, koja liči na legitimnu, i kreirana je u cilju prikupljanja podataka kao što su adrese elektronske pošte i lozinke. Dodatno je važno voditi računa o pošiljaocu poruke, o samom tekstu poruke - da li postoje gramatičke ili pravopisne greške i biti posebno obazriv kod poruka koje sadrže priloge ili linkove. Više o fišing prevarama možete pročitati ovde.

5. Redovno ažuriranje operativnog sistema i softvera

Redovno ažuriranje operativnih sistema, softvera i aplikacija pomože u prevenciji da do bezbednosnih rizika uopšte dođe, obzirom da je glavna svrha ažuriranja da dodaju novine, poprave ili poboljšaju softver koji se koristi. Preporuka je da se uključi automatsko ažuriranje za operativni sistem kao i za sve aplikacije koje imaju tu opciju jer napadači mogu koristiti uočene i poznate ranjivosti sistema ili aplikacija u toku sprovođenja napada. Redovnim ažuriranjem obezbeđuju se zakrpe za uočene ranjivosti, što za napadača otežava posao u izvođenju napada.

Nacionalni CERT preporučuje svim korisnicima elektronske pošte da prijave incident ukoliko dođe do neovlašćenog preuzimanja naloga, dok primenom svih navedenih preventivnih mera korisnici imaju mogućnost da se sami zaštite od ovakvih vidova malicioznih aktivnosti napadača.