КАКО ПОСТУПИТИ УКОЛИКО ДОЂЕ ДО КОМПРОМИТОВАЊА ЕЛЕКТРОНСКЕ ПОШТЕ И КАКО ЗАШТИТИТИ НАЛОГЕ

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ:
HTTPS://WWW.CERT.RS/PRIJAVA.HTML

СРБ-ЦЕРТ

Комуникација посредством електронске поште (*e-mail*) одвија се годинама уназад и представља ефикасан и једноставан начин размене порука како у циљу личне тако и професионалне комуникације.

Масовност употребе електронске поште, коришћење налога електронске поште за приступ друштвеним мрежама (*Facebook*, *Instagram*, *LinkedIn* itd.) или за пријем извода стања на банковном рачуну као и за приступ различитим апликацијама и сајтовима, за нападаче представља вредан ресурс, јер приступом налогу електронске поште (корисничком имену и лозинки) могу доћи у посед личних и поверљивих података о кориснику.

Када се одређени корисник интернета нађе у ситуацији да су нападачи неовлашћено приступили његовом налогу електронске поште, постоје кораци које је могуће предузети а који би кориснику омогућили поновни приступ налогу који је претходно био компромитован, као и смернице о начинима заштите налога како се корисник не би нашао у ситуацији да остане без приступа свом налогу електронске поште.

РАЗЛОЗИ ЗБОГ КОЈИХ ЈЕ ЕЛЕКТРОНСКА ПОШТА МЕТА НАПАДАЧА

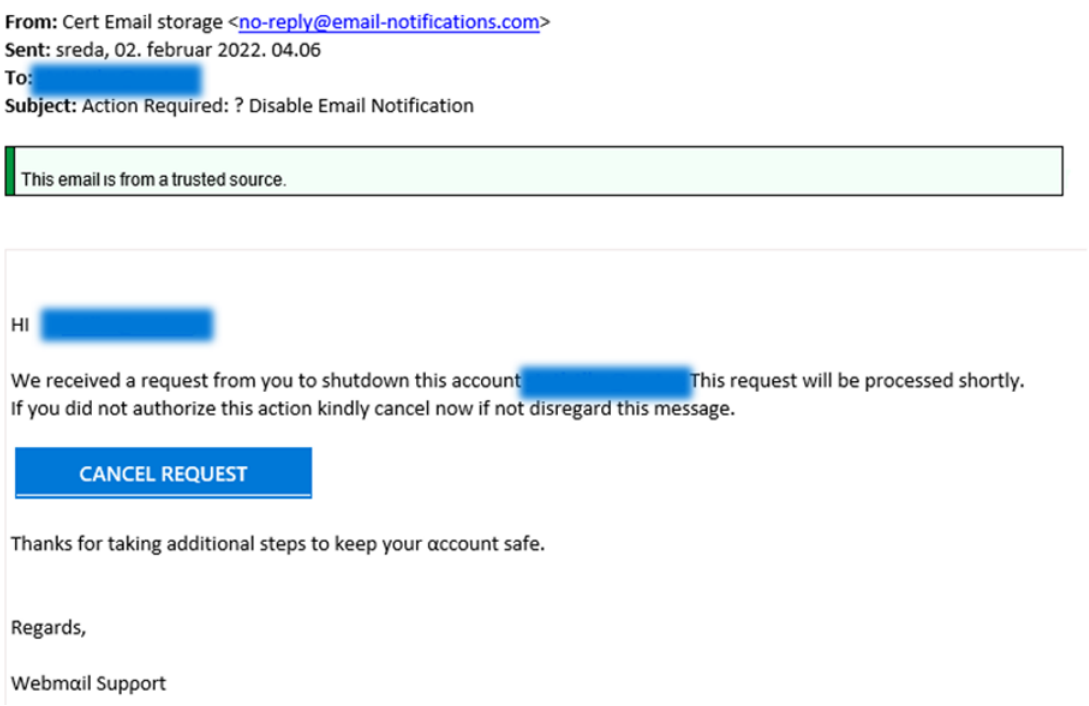
Најчешћи разлози због којих је електронска пошта мета нападача су:

- Уколико нападач преузме налог електронске поште корисника то му може омогућити приступ подацима на другим налозима, на пример може доћи до података корисника на друштвеним мрежама ако је налог креиран на основу те адресе или може приступити свим приватним фајловима корисника на *Dropbox-u*, *Google Drive-y* и другим сервисима за складиштење фајлова, и на тај начин нападач добија приступ личним информацијама корисника.
- Неовлашћеним приступањем налогу електронске поште корисника, нападачи имају могућност да ресетују лозинке и приступе свим другим налозима корисника, обзиром да већина интернет сајтова и апликација на адресу електронске поште шаље линк за ресетовање лозинке, чиме једним кликом нападачи могу променити лозинке свих других налога корисника.
- Када нападач приступи налогу електронске поште корисника, то му омогућава увид у преписке и листу контаката (чланови породице, пријатељи или пословни партнери) што нападачи даље могу искористити за слање нежељене електронске поште, најчешће кроз фишинг поруке, са циљем компромитовања што већег броја налога.

КОЈИ СУ НАЧИНИ НА КОЈЕ НАПАДАЧИ МОГУ НЕОВЛАШЋЕНО ПРИСТУПИТИ ЕЛЕКТРОНСКОЈ ПОШТИ?

Нападачи најчешће користе следеће начине како би неовлашћено приступили електронској пошти корисника:

- Слањем порука посредством електронске поште која је креирана тако да изгледа као да је послата из легитимног извора, нпр. од стране провајдера електронске поште (*Gmail*, *Yahoo*, *Microsoft Outlook* itd.), где се од корисника захтева да се опет пријави на налог. Најчешће је та порука креирана са елементима хитности, где се у кратком року захтева пријава на налог, на пример како би корисник избегао губитак података, гашење налога или како би променио лозинку јер је наводно друга особа покушала да приступи налогу корисника.



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

Слика 1 – Пример е-поште о наводном гашењу налога корисника

- *Brute Force* напади који подразумевају покушај приступа систему жртве непрекидним логовањем различитим комбинацијама слова, бројева и симбола са циљем идентификације корисничког имена и лозинке.
- Када корисник приступа електронској пошти коришћењем јавне бежичне мреже (*Wi-Fi*), нападачи могу да пресретну њихов приступ интернету чиме добијају увид у комплетан саобраћај и могу да преузму поверљиве податке или идентитет корисника.
- Преузимањем злонамерног софтвера (малвера) кроз поруке електронске поште из непроверених извора (најчешће су у питању фишинг поруке).

КАКО КОРИСНИК МОЖЕ ПРОВЕРИТИ ДА ЛИ ЈЕ НЕКО НЕОВЛАШЋЕНО ПРИСТУПИО ЊЕГОВОМ НАЛОГУ ЕЛЕКТРОНСКЕ ПОШТЕ?

Следећи примери илуструју ситуације у којима је највероватније дошло до неовлашћеног преузимања налога електронске поште од стране нападача:

- Очигледан показатељ да је налог компромитован јесте уколико корисник не може да приступи налогу уз обавештење да је лозинка промењена;
- Пријатељи и колеге примају нежељену пошту која долази са адресе електронске поште корисника који сумња да му је налог компромитован;
- Пријем више узастопних захтева за променом лозинке са других интернет страница и апликација;
- Провајдер електронске поште (*Gmail*, *Yahoo*, *Microsoft Outlook* itd.) обавештава корисника о вишеструким пријавама са непознатих *IP* адреса и локација.

КОРАЦИ КОЈЕ ЈЕ МОГУЋЕ ПРЕДУЗЕТИ УКОЛИКО ЈЕ ДОШЛО ДО НЕОВЛАШЋЕНОГ ПРЕУЗИМАЊА НАЛОГА ЕЛЕКТРОНСКЕ ПОШТЕ

Уколико корисник има и даље приступ налогу, потребно је у најкраћем року:

- Променити лозинку компромитоване електронске поште као и све лозинке на налозима где се ова адреса користила као и пратећа сигурноса питања која су везана за конкретан налог;
- Активирати антивирус, кликом на „*full scan*";
- У оквиру секције подешавања проверити да ли су промењени претходно дефинисани параметри.

Ако корисник нема приступ налогу, и лозинка је промењена од стране нападача, потребно је започети процедуру опоравка. У одређеним случајевима налог је могуће опоравити користећи методе враћања налога као што су коришћење секундарне адресе електронске поште, броја телефона или одговором на сигурносна питања. Провајдер електронске поште ће кориснику омогућити линк са лозинком за враћање налога на секундарну адресу електронске поште, или поруку на мобилни телефон са циљем враћања налога.

Процедуре за опоравак налога електронске поште, за различите провајдере, се налазе на следећим линковима:

- Gmail
- Microsoft Outlook
- Yahoo

Међутим, уколико су нападачи изменили податке за приступ налогу, потребно је контактирати подршку у циљу добијања информација о додатним корацима доказивања идентитета корисника што може бити дуготрајан процес, а не мора се увек завршити успешно – односно враћањем налога кориснику. Из тог разлога неопходно је предузети све кораке да се електронска пошта заштити од неовлашћеног приступа.

КАКО ЗАШТИТИТИ ЕЛЕКТРОНСКУ ПОШТУ ОД НЕОВЛАШЋЕНОГ ПРИСТУПА?

Слика 2 - Кораци заштите налога електронске поште

1. Креирање комплексних лозинки

Један од начина заштите налога, који смањује могућност неовлашћеног приступа личним и осетљивим подацима корисника јесте креирање комплексних лозинки.

Основне смернице за креирање сигурних лозинки су:

- Коришћење најмање 9 алфанумеричких карактера и то:

  - малих слова (a-z)

  - великих слова (A-Z)

  - бројева (0-9)

  - знакова (!@#$%^&*)

- Лозинка не би требало да садржи личне податке (име, презиме, надимак, датум рођења, име кућног љубимца итд.)
- Приликом креирања лозинки не користити секвенце са тастатуре (део реда на тастатури као што су qwerty, 123456 итд.)
- Не користити исту лозинку за више налога.

Лозинка треба да садржи сваки од препоручених словних или знаковних карактера, како би сложеност лозинке била што већа чиме би се отежао неовлашћени приступ.

2. Коришћење двофакторске аутентификације

Коришћењем двофакторске аутентификације обезбеђује се додатан ниво безбедности што се налога тиче, обзиром да подразумева постојање више корака провере како би корисник доказао идентитет, односно да је заправо корисник тај који приступа налогу. На пример, за пријаву на налог електронске поште поред лозинке, корисник ће добити сигурносни код путем СМС поруке чијим уношењем доказује идентитет и приступа налогу. Двофакторска аутентификација подразумева комбиновање два начина од следећа четири:

- Оно што знам (лозинка, ПИН)
- Оно што имам (токен, картице, мобилни телефон)
- Оно што јесам (отисак прста, препознавање лица, ока...)
- Оно што радим (говор)

3. Приликом коришћења отвореног бежичног интернета (*Wi-Fi*), односно јавно доступних тачака за приступ интернету треба бити додатно обазрив

Бесплатан приступ бежичном интернету представља све распрострањенију услугу која се нуди корисницима угоститељских објеката, хотела, тржних центара, аеродрома, чак и возила јавног превоза. Велики број корисника свакодневно користи бесплатан приступ бежичном интернету за различите потребе - за приступ друштвеним мрежама, електронској пошти или на пример за „рад на даљину“ у омиљеном кафе бару. Већина корисника није свесна да су на тај начин изложени ризику од губитака података, као што су фотографије, поруке, лични подаци, лозинке и информације о банковним рачунима. Веома распрострањен тип сајбер напада приликом коришћења јавних бежичних мрежа јесте тзв. „човек у средини“ (енг. ***Man-in-the-middle - MITM***), где је нападачима циљ да буду у истој мрежи са другим корисницима и пресретну њихов приступ интернету чиме добијају увид у комплетан саобраћај и могу да преузму поверљиве податке или идентитет корисника.

Нападачи такође могу лако креирати лажно приступно место (*hotspot*) за бежичну јавну мрежу, која имитира мрежу неког угоститељског или другог објекта - где је најчешће слободан приступ или су шифре лако доступне и ретко се мењају. То омогућава нападачу да постави замку са називом мреже која личи на назив угоститељског објекта, или називом као што је “Бесплатан *Wi-Fi*“. Када се корисник повеже на приступну тачку, креирану на овакав начин, за бесплатан бежични интернет, тада нападач добија приступ осетљивим подацима корисника.

Најбољи начин да се заштите поверљиви подаци приликом коришћења јавних бежичних мрежа је да се избегава приступање налозима електронске поште, друштвених мрежа или обављање финансијских трансакција.

4. Водити рачуна приликом пријема порука које у себи садрже прилоге или линкове

Фишинг је тип преваре која за циљ има прикупљање и злоупотребу поверљивих података корисника, попут бројева банковних рачуна, лозинки налога на друштвеним мрежама или приступа електронској пошти. Један број фишинг напада има за циљ крађу креденцијала, док други имају за циљ дистрибуцију злонамерног софтвера. Фишинг поруке најчешће се дистрибуирају путем порука електронске поште и креиране су са намером да изгледају као да су послате из поузданих извора, док је текст поруке такав да ствара осећај знатижеље, страха или хитности с циљем навођења примаоца поруке да брзо реагује – кликом на одређени линк или преузимањем докумената из прилога. Клик на линк води на лажну страницу, која личи на легитимну, и креирана је у циљу прикупљања података као што су адресе електронске поште и лозинке. Додатно је важно водити рачуна о пошиљаоцу поруке, о самом тексту поруке - да ли постоје граматичке или правописне грешке и бити посебно обазрив код порука које садрже прилоге или линкове. Више о фишинг преварама можете прочитати овде.

5. Редовно ажурирање оперативног система и софтвера

Редовно ажурирање оперативних система, софтвера и апликација поможе у превенцији да до безбедносних ризика уопште дође, обзиром да је главна сврха ажурирања да додају новине, поправе или побољшају софтвер који се користи. Препорука је да се укључи аутоматско ажурирање за оперативни систем као и за све апликације које имају ту опцију јер нападачи могу користити уочене и познате рањивости система или апликација у току спровођења напада. Редовним ажурирањем обезбеђују се закрпе за уочене рањивости, што за нападача отежава посао у извођењу напада.

Национални ЦЕРТ препоручује свим корисницима електронске поште да пријаве инцидент уколико дође до неовлашћеног преузимања налога, док применом свих наведених превентивних мера корисници имају могућност да се сами заштите од оваквих видова малициозних активности нападача.