https://pixabay.com/vectors/hack-fraud-card-code-computer-6077545/

ФИШИНГ (PHISHING)

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

СРБ-ЦЕРТ

УВОД

Фишинг (енг. *phishing*) је тип преваре која има за циљ прикупљање и злоупотребу поверљивих података корисника, попут бројева банковних рачуна, лозинки налога на друштвеним мрежама или приступа електронској пошти.

Жртва овог типа сајбер напада добија поруку путем електронске поште, друштвених мрежа, телефона или СМС-а у којој се од ње захтева да посети линк или отвори документ и упише личне и поверљиве податке.

Тренутно су на првом месту у начину извођења фишинг превара поруке путем електронске поште, уз очекивање да ће тако бити и у будућности. Међутим већ је приметан пораст употребе друштвених мрежа и апликација за инстант слање порука попут *WhatsApp*, *Viber* и осталих, у извођењу напада. Промена која се очекује у извођењу ових напада јесте да ће методе које се користе за слање порука бити све софистицираније.[1] Недавна студија је показала да је 88% светских организација доживело фишинг нападе, док је 86% њих имало сусрет са компромитовањемпословне електронске поште.[2]

Један број фишинг напада има за циљ крађу креденцијала, док други имају за циљ дистрибуцију злонамерног софтвера. Фишинг напади реализују се када жртва предузме радње из упутства датог у тексту поруке, које су најчешће креиране тако да упућују на брзу реакцију. Неки од примера захтеваних радњи у фишинг нападима су следећи:

- Клик на одређени линк;
- Ажурирање лозинке;
- Клик на „*Enable Content*“ или „*Enable Editing*“ у документу из прилога;
- Прихватање захтева за повезивањем на друштвеним мрежама;
- Коришћење нових приступних тачака за бежично спајање на интернет (*wi-fi hotspot*).

Фишинг поруке су креиране 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. Клик на „*Enable Content*“ или „*Enable Editing*“ у документу из прилога, аутоматски покреће злонамерни софтвер који убризгава одређене процесе у оперативни систем примаоца, како би онемогућио детекцију од стране антивируса и других безбедносних софтверских решења.

Слика 1. Начини реализације фишинг напада

[1]ENISA Threat Landscape 2020 - Phishing — ENISA (europa.eu)
[2] 2020 ‘State of the Phish’: Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike”. January 23, 2020. Proof Point

ВРСТЕ ФИШИНГ НАПАДА[3]

Најпрепознатљивије врсте фишинг напада су: *Spear phishing, Microsoft 365 phishing, Business email compromise, Whaling, Social media phish, Vishing i Smishing*.

Spear phishing – Циљана верзија напада, којом нападач бира одређене групе појединаца, организацију или предузеће, уместо широке групе корисника. Циљ напада је најчешће крађа података, али може бити и инсталација злонамерног софтвера на рачунар циљаног корисника. За разлику од уобичајеног фишинга који представља напад усмерен ка већем броју корисника, spear фишинг као мету има тачно одређену жртву. На тај начин нападачи комуникацију могу прилагодити тако да изгледа аутентично, јер истраживањем могу доћи до одређених података о жртви као што су адреса електронске поште, листа пријатеља, локације које често посећује и сл.

Microsoft 365 phishing – Нападачи за приступ налогу *Microsoft 365* електронске поште користе методе које су једноставне и најчешће подразумевају облик лажне поруке е-поште од компаније *Microsoft*. Порука је креирана тако да садржи захтев да се примаоци поруке улогују и промене лозинку наводећи да је то неопходно, најчешће јер се одређено време није приступало налогу или зато што постоји проблем са налогом који захтева додатну пажњу.

Business email compromise (BEC) – Компромитовање пословне електронске поште је врста напада, односно преваре, у којој нападач користећи лажне налоге е-поште има као крајњи циљ наношење штете компанији. Често ће нападач користити налог са адресом е-поште која је скоро идентична као на корпоративној мрежи, ослањајући се на претпостављено поверење између жртве и пошиљаоца поруке са тог налога. Злонамерни нападач се представља као неко коме прималац такве поруке треба да верује – обично као колега, шеф или компанија са којом, посредно или непосредно, сарађују. Злонамерни нападач шаље поруку е-поште за коју се чини да долази од познатог извора, и који поставља легитиман захтев, као нпр. да изврши трансфер новца са једног на други рачун, преусмери платни списак, промени банкарске детаље за будућа плаћања и сл.

Whaling – Напади који су усмерени ка вишим руководиоцима и најчешће се извршавају кроз е-поруке које изгледају легитимно. Из тог разлога ови напади су од посебног значаја јер виши руководиоци имају приступ великом броју осетљивих информација о компанији. Уместо слања порука широј групи људи, нападачи идентификују једну особу од које могу добити све жељене податке.

Social media phish - Нападачи често истражују своје жртве на друштвеним мрежама и другим веб локацијама с циљем прикупљања детаљних информација, након чега у складу са тим планирају напад.

Vishing (Гласовни фишинг) - Vishing је заправо форма фишинга, односно гласовни фишинг и представља сваку врсту напада посредством телефонских позива и *Skype*-а , а као циљну групу има кориснике *Voice Over Internet Protocol – VoIP* услуге. За време телефонског позива, нападач користи социјални инжењеринг да би жртву натерао да дели личне и финансијске податке, као што су бројеви рачуна и лозинке. Нападач се обично представља као представник полиције, особа која нуди помоћ у инсталирању софтвера (упозорење: То је вероватно злонамерни софтвер), или најчешће као представник банке говорећи жртви да јој је рачун компромитован.

Smishing (СМС фишинг) – Врста фишинг напада који се шаље путем СМС-а (*Short Message Service*) и користи методе социјалног инжењеринга како би се жртва навела да подели личне податке. *Smishing* порука садржи претњу или примамљиву понуду како би жртва кликнула на линк или позвала број и поделила поверљиве информације у одређеном року. Понекад нападачи поруком могу захтевати инсталацију и неког безбедносног софтвера за који ће се касније испоставити да је злонамеран.

---

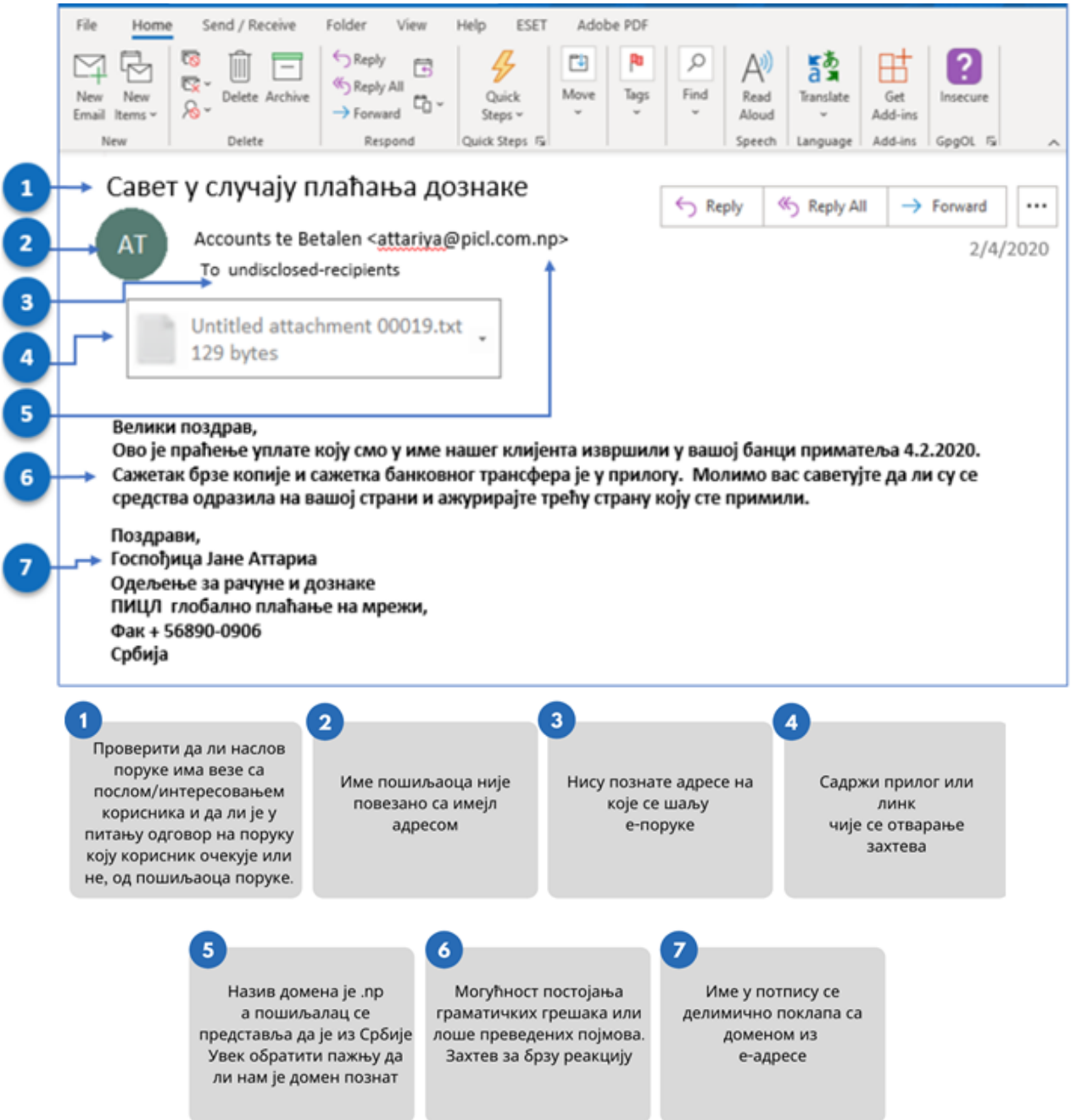
[3] What Is Phishing? Examples and Phishing Quiz - Cisco

КАКО ПРЕПОЗНАТИ ФИШИНГ НАПАД?

У одређеним ситуацијама може бити тешко да се препозна фишинг напад, јер се поруке креирају тако да изгледају аутентично и зато је први корак одбране постојање свести о могућности преваре.

Да би били сигурни потребно је не журити са отварањем прилога у поруци, кликом на линкове или слањем одговора. Карактеристике које могу указати да је реч о фишинг превари су:[4]

- Прилози и линкови;
- Правописне грешке;
- Непотребна хитност у вези са верификацијом адресе е-поште или других личних података;
- Општи уводни поздрави попут „Поштовани клијенту“ уместо личног имена.



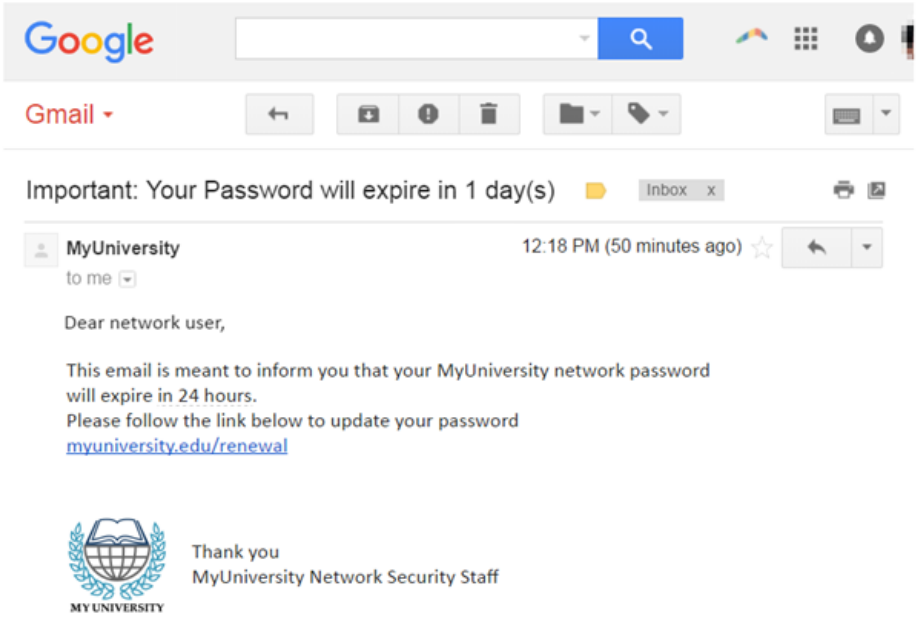
Слика 2. Савети како препознати фишинг напад

[4] https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Приликом пријема е-поруке у којој се захтева унос личних података, препорука Националног ЦЕРТ-а је детаљно анализирање **имена и адресе пошиљаоца**, као и садржај поруке. Највећи број организација имају сопствени **домен е-поште**, на пример за *Google* ће бити *@google.com.* Ако се назив домена (део иза симбола @) подудара са пошиљаоцем, порука је највероватније легитимна, а најбољи начин да се провери назив домена организације је уношење назива компаније у претраживач. Када нападачи креирају своје лажне е-адресе, односно email, они имају могућност да изаберу „име за приказ" (*From* поље) које уопште не мора да се подудара са адресом е-поште. Нападачи могу користити називе организација у локалном делу адресе е-поште да би се приликом пријема исте као име пошиљаоца појавило име организације коју нападачи користе да би извршили напад или могу да креирају лажне домене, нпр. да користе '*r*' и '*n*' једно поред другог '***rn***' уместо '***m***', или коришћење „-" уместо „." у називу домена, а све у циљу да створе осећај код жртве да је у питању легитимна организација.

Следећи пример илуструје ток фишинг напада креирањем лажне URL адресе[5]:

- Лажна адреса е-поште, наводно са *myuniversity.edu* дистрибуира се масовно што већем броју чланова факултета;
- У е-поруци се наводи да корисничка лозинка истиче, уз упутство да се приступи наведеном линку да би креирали нову лозинку у року од 24 часа, а која упућује на фишинг сајт.



Слика 3. Пример Phishing е-поруке у којој се захтева промена шифре у кратком року

У овом примеру URL адреса **myuniversity.edu/renewal** је промењена у **myuniversity.edurenewal.com.**

Слика 4. Пример лажне URL адресе

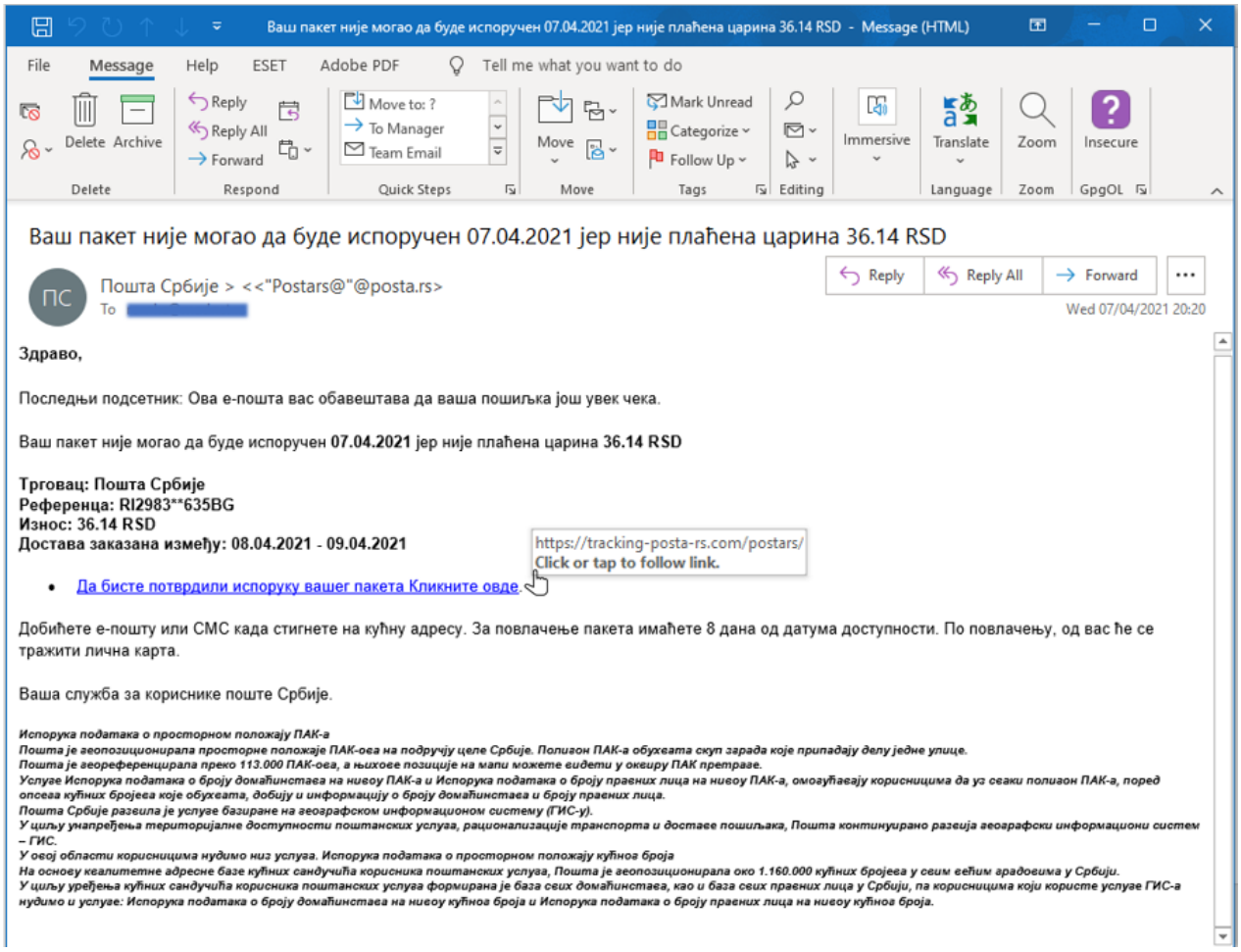
[5]https://www.imperva.com/learn/application-security/phishing-attack-scam/

Сличност између ове две адресе, корисника може да наведе на мисао да је у питању безбедна адреса интернет странице чинећи га мање свесним да је у питању сајбер напад.

Препорука је да у случају пријема поруке која садржи захтев попут промене лозинке, коју је потребно спровести у неком кратком периоду, наводећи корисника на брзу реакцију због истека времена и стварајући осећај хитности да се захтев испуни, увек накнадно провери URL адреса на којој се тражи промена шифре. Препорука је да се легитимна адреса претражи путем интернет претраживача, а не кликом на линк из е-поруке. Компарацијом адреса, често се могу уочити недоследности, и на тај начин се потенцијална превара може избећи.

Приликом пријема порука е-поште у којима се захтева да се приступи одређеном линку, да се верификује лозинка и слично, иако порука може изгледати као да стиже из поузданог извора, мале грешке у куцању или недоследности у домену често могу открити праву природу дате поруке, односно потенцијалног напада.

Следећи пример илуструје фишинг кампању која је била усмерена на кориснике поштанских услуга. У овом примеру, корисници су добијали е-пошту са обавештењем да је пристигао пакет корисника, али да није могао бити испоручен јер није уплаћен износ од 36,14 динара за царинске трошкове. Порука је стизала са лажне адресе: Поште Србије ''*Postas@"@posta.rs*, са насловом: Ваш пакет није могао да буде испоручен 07.04.2021 јер није плаћена царина 36.14 РСД.

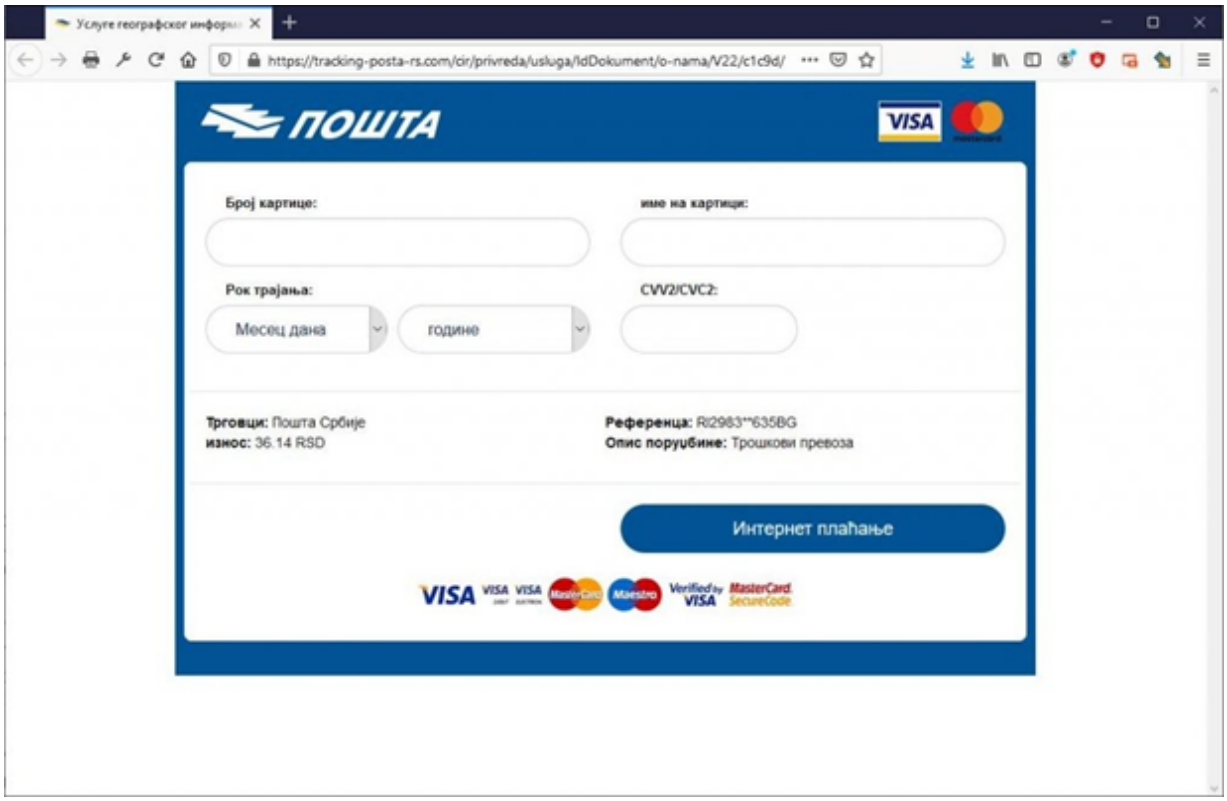


Слика 5. Пример Phishing е-поруке за Пошту Србије уз линк на ком се захтева плаћање

Препорука Националног ЦЕРТ-а је да се пре приступа линку, прво провери адреса пошиљаоца, обзиром да се адреса може лажирати, што се може видети у овом примеру ''*Postas@"@posta.rs*, иако је као име за приказ назначена „Пошта Србије". Такође, савет је обратити пажњу на граматичке грешке, које су такође један од показатеља да је у питању фишинг превара.

Даље у тексту, преласком курсора преко линкованог текста (линка), види се линк који може изгледати легитимно, и отварањем истог, приказује се фишинг страница која садржи лого Поште Србије и има садржај хитности како би пошиљка била достављена. Иако интернет страница може изгледати као легитимна страница сајта Поште Србије, она то заправо није. На врху екрана се може видети потпуно нетачна URL адреса, што се може проверити претрагом званичне странице Поште Србије путем претраживача.

Отварањем линка, корисник се преусмеравао на лажну страницу за интернет плаћање Поште Србије, у којој се захтевао унос података: Број платне картице, Име и Презиме, Рок трајања, као и *CVV2/CVC2* број картице. Уносом тражених података, нападач би дошао у посед информација на основу којих би могао да преузме новац са рачуна лица које је оставило податке.



Слика 6. Пример Phishing сајта са формом за унос података за платне картице

Препоруке Националног ЦЕРТа за превенцију од фишинг напада јесу:

- Обратити пажњу на поље „*From*“ и да ли је пошиљалац познат;
- Проверити да ли постоје правописне грешке у тексту поруке;
- Уколико постоји непотребна хитност за реакцију, не журити са отварањем линкова и прилога из поруке;
- Проверити легитимност *URL* адресе, провером адресе у интернет претраживачу;
- Упоредити да ли је име пошиљаоца повезано са адресом е-поште;
- Обратите додатно пажњу када се тражи унос података о банковној картици, посебно када је реч о *CVV2/CVC2* број картице;
- Ако примите сумњиву поруку електронске поште означите је као *Spam/Junk* или је одмах избришите.

Ако сте кликнули на линк или документ предузмите следеће кораке:

- Ако користите службени телефон или лаптоп одмах контактирајте ИТ службу;
- Ако сте дали своје податке о банковном рачуну одмах обавестите банку;
- Активирајте антивирус и кликните на „*full scan*“;
- Ако сте оставили своју лозинку, одмах промените лозинке на свим налозима;
- Ако сте изгубили новац одмах контактирајте своју банку и пријавите полицији на vtk@mup.gov.rs;

Национални ЦЕРТ Републике Србије не промовише или фаворизује било који од коришћених јавних извора, међу којима су и комерцијални производи и услуге. Све препоруке, анализе и предлози дати су у циљу превенције и заштите од безбедносних ризика.

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

#odbraniseznanjem

СРБ-ЦЕРТ