https://pixabay.com/photos/e-commerce-online-commerce-3692440/

ЕЛЕКТРОНСКА ТРГОВИНА

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

СРБ-ЦЕРТ

Као модеран вид трговине, електронска трговина је добила значајно место захваљујући погодностима које пружа. Корисници ове услуге могу да наруче производе, без изласка из куће или са посла, у било које доба дана, без чекања у редовима или у саобраћајној гужви а изабрани производи ће им бити достављени на кућну или другу жељену адресу. Популарност овог начина обављања трговине је још више порасла услед COVID-19 пандемије где је физичка дистанца била препозната као предуслов за очување здравља.

Међутим, погодности електронске трговине праћене су новим начинима за злоупотребу традиционалног поверења између продавца и купца које се успоставља у купопродајном односу. Превара може бити оријентисана како на купце, тако и на продавце, док се сами напади најчешће спроводе уз помоћ лажних интернет страница и/или злоупотребом самог процеса обављања трговине.

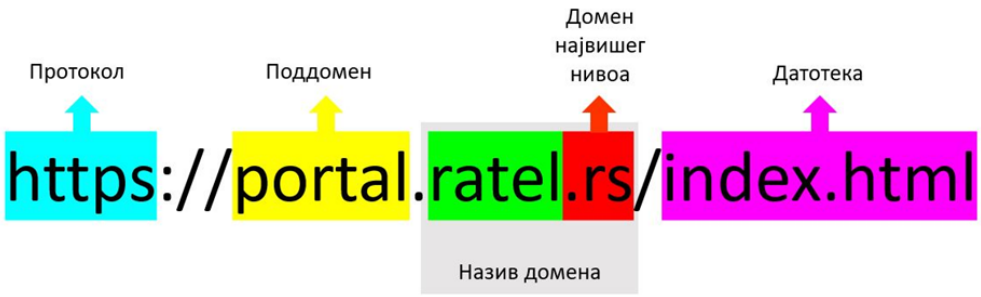
ЛАЖНА ИНТЕРНЕТ СТРАНИЦА (PHISHING)

Једна од тактика за превару корисника од стране нападача јесте креирање лажне интернет странице, која је креирана тако да буде што веродостојнија копија легитимне интернет продавнице, са основним циљем да се клијенти преваре тако што би оставили своје личне и финансијске податке.

До лажне интернет продавнице могуће је доћи путем имејла, који садржи малициозни линк, СМС порука, злонамерних рекламних огласа, друштвених мрежа и томе слично.

Препорука је да корисник увек провери адресу интернет продавнице која се налази у адресној линији интернет прегледача, односно *browser-a*. Нападачима је основни циљ креирање интернет страница које изгледају као легитимне странице и с тога је некада веома тешко увидети разлику, због чега је неопходно првенствено проверити *URL* адресу интернет продавнице.

Како би постигли свој циљ, нападачи неретко креирају поддомене који опонашају праве домене, а посао им је олакшан начином на који browser-i скраћују *URL*. У следећем примеру[1] биће приказан начин на који се креира *URL* као и начини којима нападачи могу обманути кориснике.



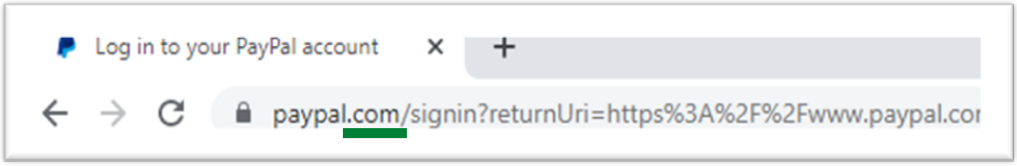
Слика 1 – Начин конструкције URL адресе

[1] https://www.it-klinika.rs/blog/kako-da-prepoznate-phishing-sajt

Креирањем лажних поддомена нападачи могу довести кориснике у заблуду. Следећи пример илуструје ситуацију где поддомени првог и другог нивоа, који су лажни, опонашају домен и домен највишег нивоа који су легитимни. Корисници се лако могу заварати да је у питању легитимна адреса, јер се конкретно у овом примеру користи ***paypal*** као поддомен, а оно на шта заиста треба обратити пажњу јесте назив домена и домена највишег нивоа. У овом примеру име домена је ***yaraneaftab***, и у питању је **фишинг сајт**, а не сајт легитимног сервиса ***PayPal***.

Слика 2 - Пример лажне URL адресе

Легитимна адреса сервиса ***Paypal*** би требало да буде приказана у адресној линији интернет прегледача као на примеру испод:

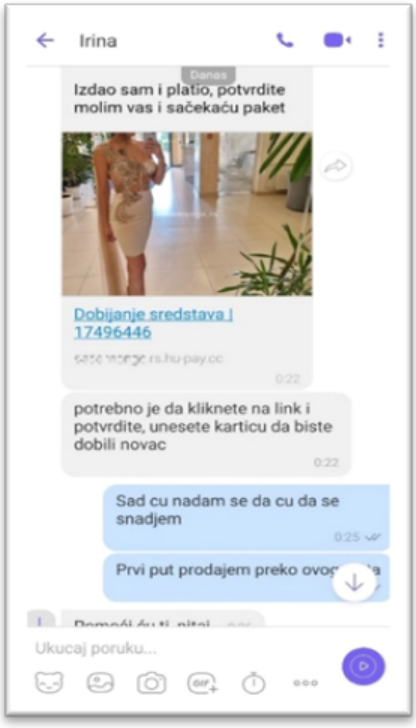


Слика 3 - Пример легитимне URL адресе

ЗЛОУПОТРЕБА ПЛАТФОРМИ ЗА ОГЛАШАВАЊЕ

Ситуација у којој корисници такође могу бити преварени приликом куповине на интернету јесте приликом коришћења платформи за оглашавање које омогућавају пружање услуга објављивања огласа и њихове промоције у циљу реализације продаје или куповине из огласа.

Наиме, све су учесталије преваре усмерене на оглашиваче производа, којима се путем неке од апликација за комуникацију (нпр. *WhatsApp*, *Viber*) јављају лажни купци који су наводно заинтересовани за производе које су видели на некој од интернет платформи за оглашавање.



Слика 4 – Пример преписке на апликацији Viber

У највећем броју случајева, лажни купац пошаље продавцу слику као доказ да је унапред „уплатио“ средства.

Након тога доставља продавцу линк путем неке од апликација за комуникацију (нпр. *WhatsApp, Viber*) са инструкцијом да продавац кликне на линк, како би преузео средства која је лажни купац уплатио.

Линк у поруци води на лажну интернет страницу за доставу пошиљки, која би након пријема уплате требало да омогући доставу робе. На тој интернет страници, од продавца се захтева да унесе податке са платне картице (број картице и *CVV* број) како би продавац наводно примио уплату.

Оног момента када се тражени подаци унесу на лажну интернет страницу, лице које врши превару подиже средства са банковног рачуна продавца, након чега прекида сваку врсту комуникације.

Због свега наведеног потребно је бити обазрив у случају захтева за унос података о платној картици, јер се подаци о платној картици уносе искључиво када се врши плаћање, док за пријем уплате ови подаци нису неопходни.

Препорука Националног ЦЕРТ-а је да корисници обрате пажњу код понуда које могу добити путем електронске поште или апликација за инстант слање порука (*WhatsApp, Viber* и сл.), а које у себи садрже линкове.

Такође, неретко се дешавају ситуације да продавац на интернет платформи делује поуздано (нпр. због великог броја позитивних оцена), што може навести купца да изврши уплату унапред, због чега је потребно додатно обратити пажњу на услове плаћања ових интернет платформи, јер већина подржава плаћање поузећем као једини вид плаћања. На тај начин купац се може заштити јер производ плаћа у моменту преузимања пошиљке.

ШТА ПРОВЕРИТИ ПРЕ ИНТЕРНЕТ КУПОВИНЕ?

Проверити SSL сертификат

SSL сертификат (енг. *Secure Sockets Layer*) омогућава безбедну онлајн комуникацију и обављање финансијских трансакција, односно, омогућава енкриптовану (шифровану) комуникацију између сервера і *browser*-а. Корисник може проверити да ли сајт има *SSL* сертификат, тако што ће обратити пажњу да ли се у оквиру адресне линије налази иконица закључаног катанца и да ли *URL* линк почиње са *HTTPS*, уместо *HTTP* (слово „*S*“ означава „*secure*“).

Проверити политику приватности

Политика приватности је изјава којом је објашњен начин на који компанија прикупља, користи и чува осетљиве податке својих клијената. Уколико политика приватности није доступна кориснику на сајту на коме се обавља куповина, то може бити први показатељ да могу постојати безбедносни пропусти. Поред политике приватности неопходно је анализирати услове плаћања, гаранције, начин вршења замене, препоруке и жалбе корисника.

Пронаћи пословне податке интернет продавнице

Проверити да ли интернет продавница пружа основне информације као што су адреса, број телефона и порески идентификациони број (ПИБ) под којим је продавница регистрована. У случају да корисник има недоумица или додатних питања, препорука је да се успостави контакт са интернет продавницом путем мејла, чет опција или директно путем телефона.

Обратити пажњу уколико је понуда сувише добра да би била истинита

Корисници би пре куповине требало да истраже тржиште и упореде цену одређеног жељеног производа са ценама истог производа у другим интернет продавницама, јер постоји разлог за сумњу уколико је понуда сувише добра да би била истинита.

Проверити стање производа

Обратите пажњу на стање производа (ново, коришћено, неисправно), на детаљан опис или техничке спецификације, као и време испоруке производа.

ПРЕПОРУКЕ ЗА БЕЗБЕДНУ ЕЛЕКТРОНСКУ ТРГОВИНУ

Пре куповине, корисник би требало да одвоји мало времена за истраживање интернет продавница како би своју куповину учинио што безбеднијом. Основне препорука за безбеднију онлајн куповину могу бити:

Унос легитимне URL адресе директно у адресну линију интернет прегледача

Препорука је да се сајтовима за електронску трговину не приступа кликом на линкове који стижу до корисника путем електронске поште, СМС порука, апликација за инстант слање порука (нпр. *WhatsApp*, *Viber*), друштвених мрежа и сл., већ уношењем адреса директно у адресно поље *browser*-а (нпр. *Google Chrome, Mozilla Firefox, Microsoft Edge, Microsoft Internet Explorer, Opera, Apple Safari* итд.).

Креирање комплексних лозинки

Потребно је посветити одговарајућу пажњу при избору лозинке за приступ сајтовима за електронску трговину.

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 попут имена, презимена, надимака, датума рођења, имена кућних љубимаца и сл.;
- Приликом креирања лозинки не би требало користити секвенце са тастатуре (део реда на тастатури као што су: qwerty, 123456 и сл.);
- За сваки налог корисник треба да креира засебну лозинку.

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

Препоруке током обављања куповине преко интернет продавнице

- Обратите пажњу на све појединачне кораке и пажљиво прочитати све захтеве који вам се упућују приликом електронске трговине;

- У циљу заштите података неопходно је бити пажљив у телефонским позивима у којима се захтевају лични подаци, лозинке и бројеви кредитних картица. Препорука корисницима јесте да смање количину информација које се могу добити о њима и на тај начин да ограниче могућност нападачима да направе налог на име корисника.
- Проверите да ли достављен производ одговара купљеном и да ли је паковање неоштећено, пре самог плаћања.
- Важно је сачувати све информације о куповини као што су ваучери, број налога или било коју другу интеракцију са сајтом. Ови подаци могу бити од великог значаја уколико се појави проблем.

Обазривост приликом коришћења отвореног бежичног интернета (*Wi-Fi*)

Препорука Националног ЦЕРТ-а је да отворене *Wi-Fi* тачке за приступ интернету, које су доступне на јавним местима попут ресторана, хотела, јавног и градског превоза и сл. корисници употребљавају само за сурфовање интернетом, док је за електронску трговину или друге финансијске трансакције пожељно користити интернет који нуде овлашћени оператори интернета и мобилних услуга. Такође није препоручено коришћење рачунара трећих лица за извршавање платних трансакција, јер њихови уређаји могу бити компромитовани или заражени.

Редовно ажурирање оперативног система и софтвера

Редовно ажурирање оперативних система, софтвера и апликација је значајно за заштиту уређаја, имајући у виду да је њихова главна сврха да унапреде безбедносне аспекте, поправе или побољшају софтвер који се користи на уређају.

За обављање електронске трговине, препоручљиво је користити рачунар који има:

- инсталиране најновије верзије апликација;
- примењена најновија ажурирања/закрпе (*patch*);
- и користи следеће сигурносне механизме:
  - *Antimalware*
  - *Antispam*
  - *Firewall personal*

Поред тога, у циљу унапређења нивоа безбедности за онлајн куповину, општа је препорука корисницима да обезбеде једну засебну платну картицу за потребе куповине преко интернета. На тај начин корисници ограничавају приступ средствима која су расположива само на тој платној картици и онемогућавају нападачима да преузму средства која корисници имају на својим динарским или валутним рачунима.

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.