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

ELEKTRONSKA TRGOVINA

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

SRB-CERT

Kao moderan vid trgovine, elektronska trgovina je dobila značajno mesto zahvaljujući pogodnostima koje pruža. Korisnici ove usluge mogu da naruče proizvode, bez izlaska iz kuće ili sa posla, u bilo koje doba dana, bez čekanja u redovima ili u saobraćajnoj gužvi a izabrani proizvodi će im biti dostavljeni na kućnu ili drugu željenu adresu. Popularnost ovog načina obavljanja trgovine je još više porasla usled COVID-19 pandemije gde je fizička distanca bila prepoznata kao preduslov za očuvanje zdravlja.

Međutim, pogodnosti elektronske trgovine praćene su novim načinima za zloupotrebu tradicionalnog poverenja između prodavca i kupca koje se uspostavlja u kupoprodajnom odnosu. Prevara može biti orijentisana kako na kupce, tako i na prodavce, dok se sami napadi najčešće sprovode uz pomoć lažnih internet stranica i/ili zloupotrebom samog procesa obavljanja trgovine.

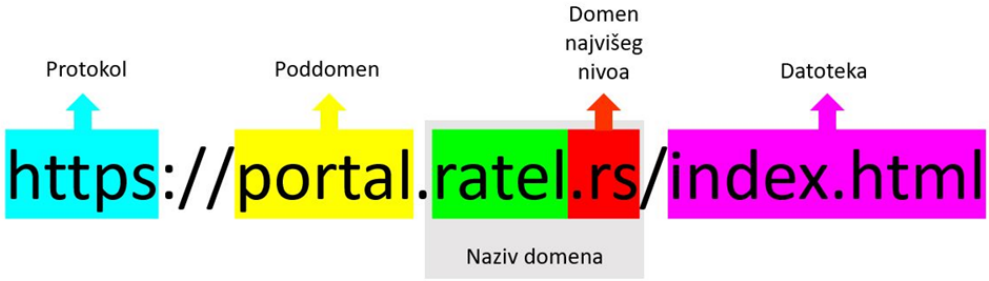
LAŽNA INTERNET STRANICA (PHISHING)

Jedna od taktika za prevaru korisnika od strane napadača jeste kreiranje lažne internet stranice, koja je kreirana tako da bude što verodostojnija kopija legitimne internet prodavnice, sa osnovnim ciljem da se klijenti prevare tako što bi ostavili svoje lične i finansijske podatke.

Do lažne internet prodavnice moguće je doći putem imejla, koji sadrži maliciozni link, SMS poruka, zlonamernih reklamnih oglasa, društvenih mreža i tome slično.

Preporuka je da korisnik uvek proveri adresu internet prodavnice koja se nalazi u adresnoj liniji internet pregledača, odnosno *browser-a*. Napadačima je osnovni cilj kreiranje internet stranica koje izgledaju kao legitimne stranice i s toga je nekada veoma teško uvideti razliku, zbog čega je neophodno prvenstveno proveriti *URL* adresu internet prodavnice.

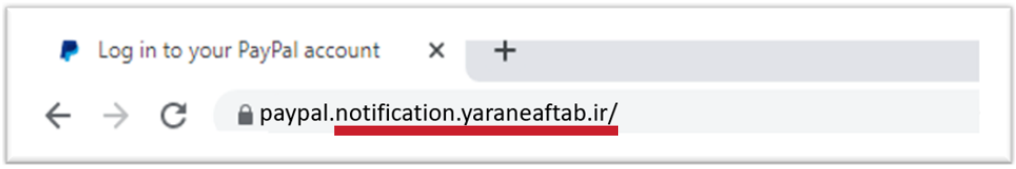
Kako bi postigli svoj cilj, napadači neretko kreiraju poddomene koji oponašaju prave domene, a posao im je olakšan načinom na koji browser-i skraćuju *URL*. U sledećem primeru[1] biće prikazan način na koji se kreira *URL* kao i načini kojima napadači mogu obmanuti korisnike.



Slika 1 – Način konstrukcije URL adrese

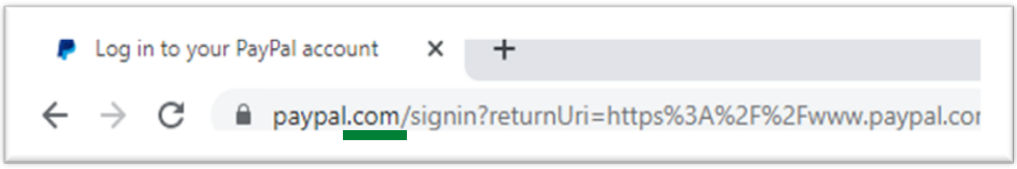
[1] https://www.it-klinika.rs/blog/kako-da-prepoznate-phishing-sajt

Kreiranjem lažnih poddomena napadači mogu dovesti korisnike u zabludu. Sledeći primer ilustruje situaciju gde poddomeni prvog i drugog nivoa, koji su lažni, oponašaju domen i domen najvišeg nivoa koji su legitimni. Korisnici se lako mogu zavarati da je u pitanju legitimna adresa, jer se konkretno u ovom primeru koristi **paypal** kao poddomen, a ono na šta zaista treba obratiti pažnju jeste naziv domena i domena najvišeg nivoa. U ovom primeru ime domena je **yaraneaftab**, i u pitanju je **fišing sajt**, a ne sajt legitimnog servisa **PayPal**.



Slika 2 - Primer lažne URL adrese

Legitimna adresa servisa **Paypal** bi trebalo da bude prikazana u adresnoj liniji internet pregledača kao na primeru ispod:

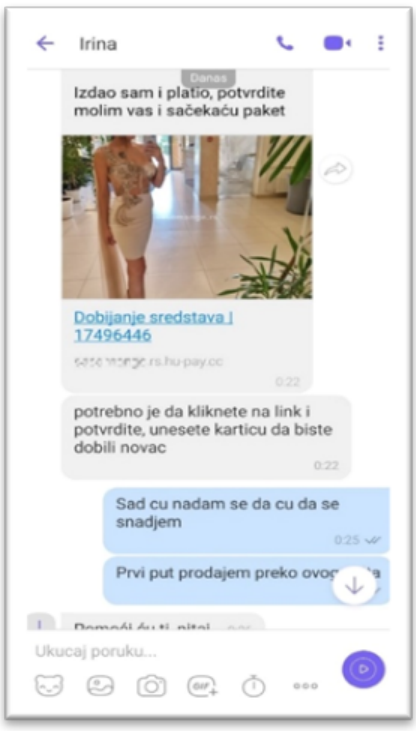


Slika 3 - Primer legitimne URL adrese

ZLOUPOTREBA PLATFORMI ZA OGLAŠAVANJE

Situacija u kojoj korisnici takođe mogu biti prevareni prilikom kupovine na internetu jeste prilikom korišćenja platformi za oglašavanje koje omogućavaju pružanje usluga objavljivanja oglasa i njihove promocije u cilju realizacije prodaje ili kupovine iz oglasa.

Naime, sve su učestalije prevare usmerene na oglašivače proizvoda, kojima se putem neke od aplikacija za komunikaciju (npr. *WhatsApp*, *Viber*) javljaju lažni kupci koji su navodno zainteresovani za proizvode koje su videli na nekoj od internet platformi za oglašavanje.



Slika 4 – Primer prepiske na aplikaciji VIber

U najvećem broju slučajeva, lažni kupac pošalje prodavcu sliku kao dokaz da je unapred „uplatio“ sredstva.

Nakon toga dostavlja prodavcu link putem neke od aplikacija za komunikaciju (npr. *WhatsApp, Viber*) sa instrukcijom da prodavac klikne na link, kako bi preuzeo sredstva koja je lažni kupac uplatio.

Link u poruci vodi na lažnu internet stranicu za dostavu pošiljki, koja bi nakon prijema uplate trebalo da omogući dostavu robe. Na toj internet stranici, od prodavca se zahteva da unese podatke sa platne kartice (broj kartice i *CVV* broj) kako bi prodavac navodno primio uplatu.

Onog momenta kada se traženi podaci unesu na lažnu internet stranicu, lice koje vrši prevaru podiže sredstva sa bankovnog računa prodavca, nakon čega prekida svaku vrstu komunikacije.

Zbog svega navedenog potrebno je biti obazriv u slučaju zahteva za unos podataka o platnoj kartici, jer se podaci o platnoj kartici unose isključivo kada se vrši plaćanje, dok za prijem uplate ovi podaci nisu neophodni.

Preporuka Nacionalnog CERT-a je da korisnici obrate pažnju kod ponuda koje mogu dobiti putem elektronske pošte ili aplikacija za instant slanje poruka (*WhatsApp*, *Viber* i *sl*.), a koje u sebi sadrže linkove.

Takođe, neretko se dešavaju situacije da prodavac na internet platformi deluje pouzdano (npr. zbog velikog broja pozitivnih ocena), što može navesti kupca da izvrši uplatu unapred, zbog čega je potrebno dodatno obratiti pažnju na uslove plaćanja ovih internet platformi, jer većina podržava plaćanje pouzećem kao jedini vid plaćanja. Na taj način kupac se može zaštiti jer proizvod plaća u momentu preuzimanja pošiljke.

ŠTA PROVERITI PRE INTERNET KUPOVINE?

Proveriti *SSL* sertifikat

SSL sertifikat (eng. *Secure Sockets Layer*) omogućava bezbednu onlajn komunikaciju i obavljanje finansijskih transakcija, odnosno, omogućava enkriptovanu (šifrovanu) komunikaciju između servera i browser-a. Korisnik može proveriti da li sajt ima *SSL* sertifikat, tako što će obratiti pažnju da li se u okviru adresne linije nalazi ikonica zaključanog katanca i da li *URL* link počinje sa *HTTPS*, umesto *HTTP* (slovo „*S*“ označava „*secure*“).

Proveriti politiku privatnosti

Politika privatnosti je izjava kojom je objašnjen način na koji kompanija prikuplja, koristi i čuva osetljive podatke svojih klijenata. Ukoliko politika privatnosti nije dostupna korisniku na sajtu na kome se obavlja kupovina, to može biti prvi pokazatelj da mogu postojati bezbednosni propusti. Pored politike privatnosti neophodno je analizirati uslove plaćanja, garancije, način vršenja zamene, preporuke i žalbe korisnika.

Pronaći poslovne podatke internet prodavnice

Proveriti da li internet prodavnica pruža osnovne informacije kao što su adresa, broj telefona i poreski identifikacioni broj (PIB) pod kojim je prodavnica registrovana. U slučaju da korisnik ima nedoumica ili dodatnih pitanja, preporuka je da se uspostavi kontakt sa internet prodavnicom putem mejla, čet opcija ili direktno putem telefona.

Obratiti pažnju ukoliko je ponuda suviše dobra da bi bila istinita

Korisnici bi pre kupovine trebalo da istraže tržište i uporede cenu određenog željenog proizvoda sa cenama istog proizvoda u drugim internet prodavnicama, jer postoji razlog za sumnju ukoliko je ponuda suviše dobra da bi bila istinita.

Proveriti stanje proizvoda

Obratite pažnju na stanje proizvoda (novo, korišćeno, neispravno), na detaljan opis ili tehničke specifikacije, kao i vreme isporuke proizvoda.

PREPORUKE ZA BEZBEDNU ELEKTRONSKU TRGOVINU

Pre kupovine, korisnik bi trebalo da odvoji malo vremena za istraživanje internet prodavnica kako bi svoju kupovinu učinio što bezbednijom. Osnovne preporuka za bezbedniju onlajn kupovinu mogu biti:

Unos legitimne *URL* adrese direktno u adresnu liniju internet pregledača

Preporuka je da se sajtovima za elektronsku trgovinu ne pristupa klikom na linkove koji stižu do korisnika putem elektronske pošte, SMS poruka, aplikacija za instant slanje poruka (npr. *WhatsApp, Viber*), društvenih mreža i sl., već unošenjem adresa direktno u adresno polje browser-a (npr. *Google Chrome*, *Mozilla Firefox*, *Microsoft Edge*, *Microsoft Internet Explorer*, *Opera*, *Apple Safari* itd.).

Kreiranje kompleksnih lozinki

Potrebno je posvetiti odgovarajuću pažnju pri izboru lozinke za pristup sajtovima za elektronsku trgovinu.

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 poput imena, prezimena, nadimaka, datuma rođenja, imena kućnih ljubimaca i sl.;
- Prilikom kreiranja lozinki ne bi trebalo koristiti sekvence sa tastature (deo reda na tastaturi kao što su: *qwerty*, 123456 i sl.);
- Za svaki nalog korisnik treba da kreira zasebnu lozinku.

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

Preporuke tokom obavljanja kupovine preko internet prodavnice

- Obratite pažnju na sve pojedinačne korake i pažljivo pročitati sve zahteve koji vam se upućuju prilikom elektronske trgovine;
- U cilju zaštite podataka neophodno je biti pažljiv u telefonskim pozivima u kojima se zahtevaju lični podaci, lozinke i brojevi kreditnih kartica. Preporuka korisnicima jeste da smanje količinu informacija koje se mogu dobiti o njima i na taj način da ograniče mogućnost napadačima da naprave nalog na ime korisnika.
- Proverite da li dostavljen proizvod odgovara kupljenom i da li je pakovanje neoštećeno, pre samog plaćanja.

- Važno je sačuvati sve informacije o kupovini kao što su vaučeri, broj naloga ili bilo koju drugu interakciju sa sajtom. Ovi podaci mogu biti od velikog značaja ukoliko se pojavi problem.

Obazrivost prilikom korišćenja otvorenog bežičnog interneta (*Wi-Fi*)

Preporuka Nacionalnog CERT-a je da otvorene *Wi-Fi* tačke za pristup internetu, koje su dostupne na javnim mestima poput restorana, hotela, gradskog prevoza i sl. korisnici upotrebljavaju samo za surfovanje internetom, dok je za elektronsku trgovinu ili druge finansijske transakcije poželjno koristiti internet koji nude ovlašćeni operatori interneta i mobilnih usluga. Takođe nije preporučeno korišćenje računara trećih lica za izvršavanje platnih transakcija, jer njihovi uređaji mogu biti kompromitovani ili zaraženi.

Redovno ažuriranje operativnog sistema i softvera

Redovno ažuriranje operativnih sistema, softvera i aplikacija je značajno za zaštitu uređaja, imajući u vidu da je njihova glavna svrha da unaprede bezbednosne aspekte, poprave ili poboljšaju softver koji se koristi na uređaju.

Za obavljanje elektronske trgovine,preporučljivo je koristiti računar koji ima:

- instalirane najnovije verzije aplikacija;
- primenjena najnovija ažuriranja/zakrpe (*patch*);
- i koristi sledeće sigurnosne mehanizme:
  - *Antimalware*
  - *Antispam*
  - *Firewall personal*

Pored toga, u cilju unapređenja nivoa bezbednosti za onlajn kupovinu, opšta je preporuka korisnicima da obezbede jednu zasebnu platnu karticu za potrebe kupovine preko interneta. Na taj način korisnici ograničavaju pristup sredstvima koja su raspoloživa samo na toj platnoj kartici i onemogućavaju napadačima da preuzmu sredstva koja korisnici imaju na svojim dinarskim ili valutnim računima.