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

FIŠING (PHISHING)

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

SRB-CERT

UVOD

Fišing (eng. *phishing*) je tip prevare koja ima za cilj prikupljanje i zloupotrebu poverljivih podataka korisnika, poput brojeva bankovnih računa, lozinki naloga na društvenim mrežama ili pristupa elektronskoj pošti.

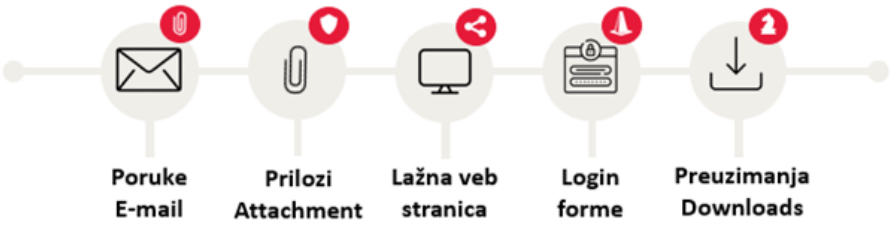
Žrtva ovog tipa sajber napada dobija poruku putem elektronske pošte, društvenih mreža, telefona ili SMS-a u kojoj se od nje zahteva da poseti link ili otvori dokument i upiše lične i poverljive podatke.

Trenutno su na prvom mestu u načinu izvođenja fišing prevara poruke putem elektronske pošte, uz očekivanje da će tako biti i u budućnosti. Međutim već je primetan porast upotrebe društvenih mreža i aplikacija za instant slanje poruka poput *WhatsApp*, *Viber* i ostalih, u izvođenju napada. Promena koja se očekuje u izvođenju ovih napada jeste da će metode koje se koriste za slanje poruka biti sve sofisticiranije[1]. Nedavna studija je pokazala da je 88% svetskih organizacija doživelo fišing napade, dok je 86% njih imalo susret sa kompromitovanjem poslovne elektronske pošte[2].

Jedan broj fišing napada ima za cilj krađu kredencijala, dok drugi imaju za cilj distribuciju zlonamernog softvera. Fišing napadi realizuju se kada žrtva preduzme radnje iz uputstva datog u tekstu poruke, koje su najčešće kreirane tako da upućuju na brzu reakciju. Neki od primera zahtevanih radnji u fišing napadima su sledeći:

- Klik na određeni link;
- Ažuriranje lozinke;
- Klik na „*Enable Content*“ ili „*Enable Editing*“ u dokumentu iz priloga;
- Prihvatanje zahteva za povezivanjem na društvenim mrežama;
- Korišćenje novih pristupnih tačaka za bežično spajanje na internet (*wi-fi hotspot*).

Fišing poruke su kreirane 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. Klik na „*Enable Content*“ ili „*Enable Editing*“ u dokumentu iz priloga, automatski pokreće zlonamerni softver koji ubrizgava određene procese u operativni sistem primaoca, kako bi onemogućio detekciju od strane antivirusa i drugih bezbednosnih softverskih rešenja.



Slika 1. Načini realizacije fišing napada

[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

VRSTE FIŠING NAPADA[3]

Najprepoznatljivije vrste fišing napada su: *Spear phishing, Microsoft 365 phishing, Business email compromise, Whaling, Social media phish, Vishing i Smishing*.

Spear phishing – Ciljana verzija napada, kojom napadač bira određene grupe pojedinaca, organizaciju ili preduzeće, umesto široke grupe korisnika. Cilj napada je najčešće krađa podataka, ali može biti i instalacija zlonamernog softvera na računar ciljanog korisnika. Za razliku od uobičajenog fišinga koji predstavlja napad usmeren ka većem broju korisnika, spear fišing kao metu ima tačno određenu žrtvu. Na taj način napadači komunikaciju mogu prilagoditi tako da izgleda autentično, jer istraživanjem mogu doći do određenih podataka o žrtvi kao što su adresa elektronske pošte, lista prijatelja, lokacije koje često posećuje i sl.

Microsoft 365 phishing – Napadači za pristup nalogu *Microsoft 365* elektronske pošte koriste metode koje su jednostavne i najčešće podrazumevaju oblik lažne poruke e-pošte od kompanije *Microsoft*. Poruka je kreirana tako da sadrži zahtev da se primaoci poruke uloguju i promene lozinku navodeći da je to neophodno, najčešće jer se određeno vreme nije pristupalo nalogu ili zato što postoji problem sa nalogom koji zahteva dodatnu pažnju.

Business email compromise (BEC) – Kompromitovanje poslovne elektronske pošte je vrsta napada, odnosno prevare, u kojoj napadač koristeći lažne naloge e-pošte ima kao krajnji cilj nanošenje štete kompaniji. Često će napadač koristiti nalog sa adresom e-pošte koja je skoro identična kao na korporativnoj mreži, oslanjajući se na pretpostavljeno poverenje između žrtve i pošiljaoca poruke sa tog naloga. Zlonamerni napadač se predstavlja kao neko kome primalac takve poruke treba da veruje – obično kao kolega, šef ili kompanija sa kojom, posredno ili neposredno, sarađuju. Zlonamerni napadač šalje poruku e-pošte za koju se čini da dolazi od poznatog izvora, i koji postavlja legitiman zahtev, kao npr. da izvrši transfer novca sa jednog na drugi račun, preusmeri platni spisak, promeni bankarske detalje za buduća plaćanja i sl.

Whaling – Napadi koji su usmereni ka višim rukovodiocima i najčešće se izvršavaju kroz e-poruke koje izgledaju legitimno. Iz tog razloga ovi napadi su od posebnog značaja jer viši rukovodioci imaju pristup velikom broju osetljivih informacija o kompaniji. Umesto slanja poruka široj grupi ljudi, napadači identifikuju jednu osobu od koje mogu dobiti sve željene podatke.

Social media phish - Napadači često istražuju svoje žrtve na društvenim mrežama i drugim veb lokacijama s ciljem prikupljanja detaljnih informacija, nakon čega u skladu sa tim planiraju napad.

Vishing (Glasovni fišing) - Vishing je zapravo forma fišinga, odnosno glasovni fišing i predstavlja svaku vrstu napada posredstvom telefonskih poziva i *Skype*-a , a kao ciljnu grupu ima korisnike *Voice Over Internet Protocol – VoIP* usluge. Za vreme telefonskog poziva, napadač koristi socijalni inženjering da bi žrtvu naterao da deli lične i finansijske podatke, kao što su brojevi računa i lozinke. Napadač se obično predstavlja kao predstavnik policije, osoba koja nudi pomoć u instaliranju softvera (upozorenje: To je verovatno zlonamerni softver), ili najčešće kao predstavnik banke govoreći žrtvi da joj je račun kompromitovan.

Smishing (SMS fišing) – Vrsta fišing napada koji se šalje putem SMS-a (*Short Message Service*) i koristi metode socijalnog inženjeringa kako bi se žrtva navela da podeli lične podatke. Smishing poruka sadrži pretnju ili primamljivu ponudu kako bi žrtva kliknula na link ili pozvala broj i podelila poverljive informacije u određenom roku. Ponekad napadači porukom mogu zahtevati instalaciju i nekog bezbednosnog softvera za koji će se kasnije ispostaviti da je zlonameran.

---

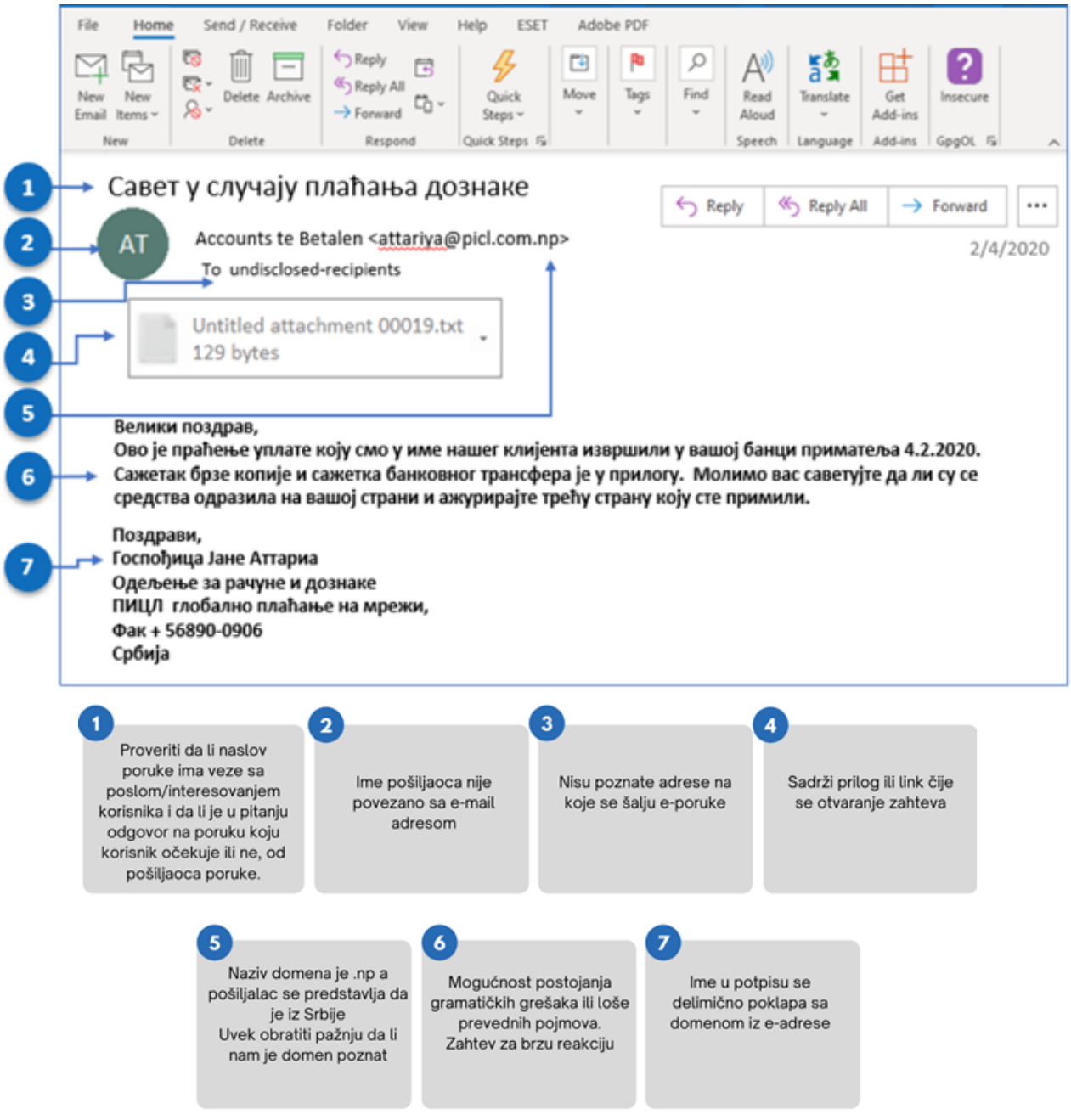
[3] What Is Phishing? Examples and Phishing Quiz - Cisco

KAKO PREPOZNATI FIŠING NAPAD?

U određenim situacijama može biti teško da se prepozna fišing napad, jer se poruke kreiraju tako da izgledaju autentično i zato je prvi korak odbrane postojanje svesti o mogućnosti prevare.

Da bi bili sigurni potrebno je ne žuriti sa otvaranjem priloga u poruci, klikom na linkove ili slanjem odgovora. Karakteristike koje mogu ukazati da je reč o fišing prevari su[4]:

- Prilozi i linkovi;
- Pravopisne greške;
- Nepotrebna hitnost u vezi sa verifikacijom adrese e-pošte ili drugih ličnih podataka;
- Opšti uvodni pozdravi poput „Poštovani klijentu“ umesto ličnog imena.



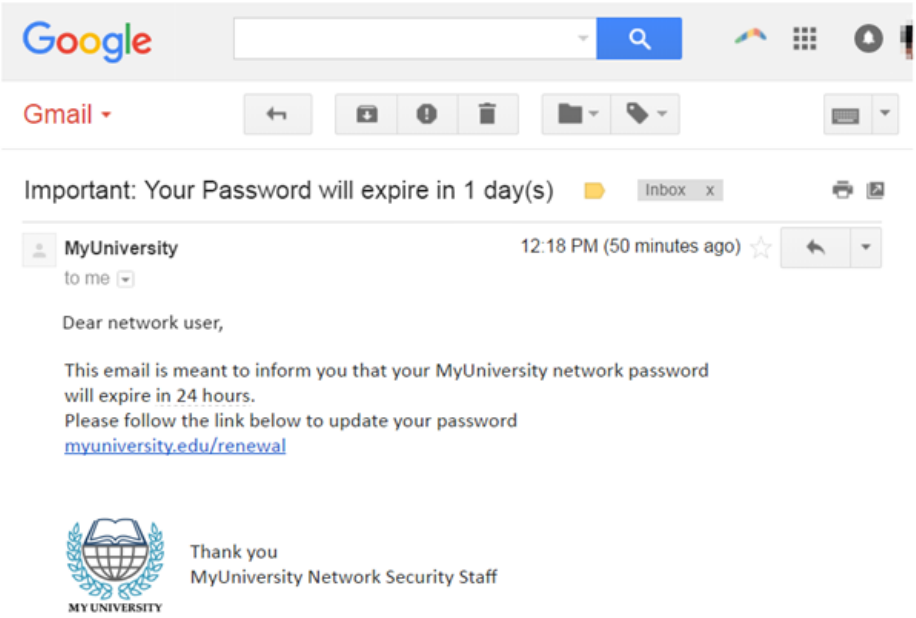
Slika 2. Saveti kako prepoznati fišing napad

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

Prilikom prijema e-poruke u kojoj se zahteva unos ličnih podataka, preporuka Nacionalnog CERT-a je detaljno analiziranje **imena i adrese pošiljaoca**, kao i sadržaj poruke. Najveći broj organizacija imaju sopstveni **domen e-pošte**, na primer za *Google* će biti *@google.com*. Ako se naziv domena (deo iza simbola @) podudara sa pošiljaocem, poruka je najverovatnije legitimna, a najbolji način da se proveri naziv domena organizacije je unošenje naziva kompanije u pretraživač. Kada napadači kreiraju svoje lažne e-adrese, odnosno email, oni imaju mogućnost da izaberu „ime za prikaz" (*From* polje) koje uopšte ne mora da se podudara sa adresom e-pošte. Napadači mogu koristiti nazive organizacija u lokalnom delu adrese e-pošte da bi se prilikom prijema iste kao ime pošiljaoca pojavilo ime organizacije koju napadači koriste da bi izvršili napad ili mogu da kreiraju lažne domene, npr. da koriste '*r*' i '*n*' jedno pored drugog '***rn***' umesto '***m***', ili korišćenje „-" umesto „." u nazivu domena, a sve u cilju da stvore osećaj kod žrtve da je u pitanju legitimna organizacija.

Sledeći primer ilustruje tok fišing napada kreiranjem lažne URL adrese[5]:

- Lažna adresa e-pošte, navodno sa *myuniversity.edu* distribuira se masovno što većem broju članova fakulteta;
- U e-poruci se navodi da korisnička lozinka ističe, uz uputstvo da se pristupi navedenom linku da bi kreirali novu lozinku u roku od 24 časa, a koja upućuje na fišing sajt.



Slika 3. Primer Phishing e-poruke u kojoj se zahteva promena šifre u kratkom roku

U ovom primeru URL adresa **myuniversity.edu/renewal** je promenjena u **myuniversity.edurenewal.com.**

Slika 4. Primer lažne URL adrese

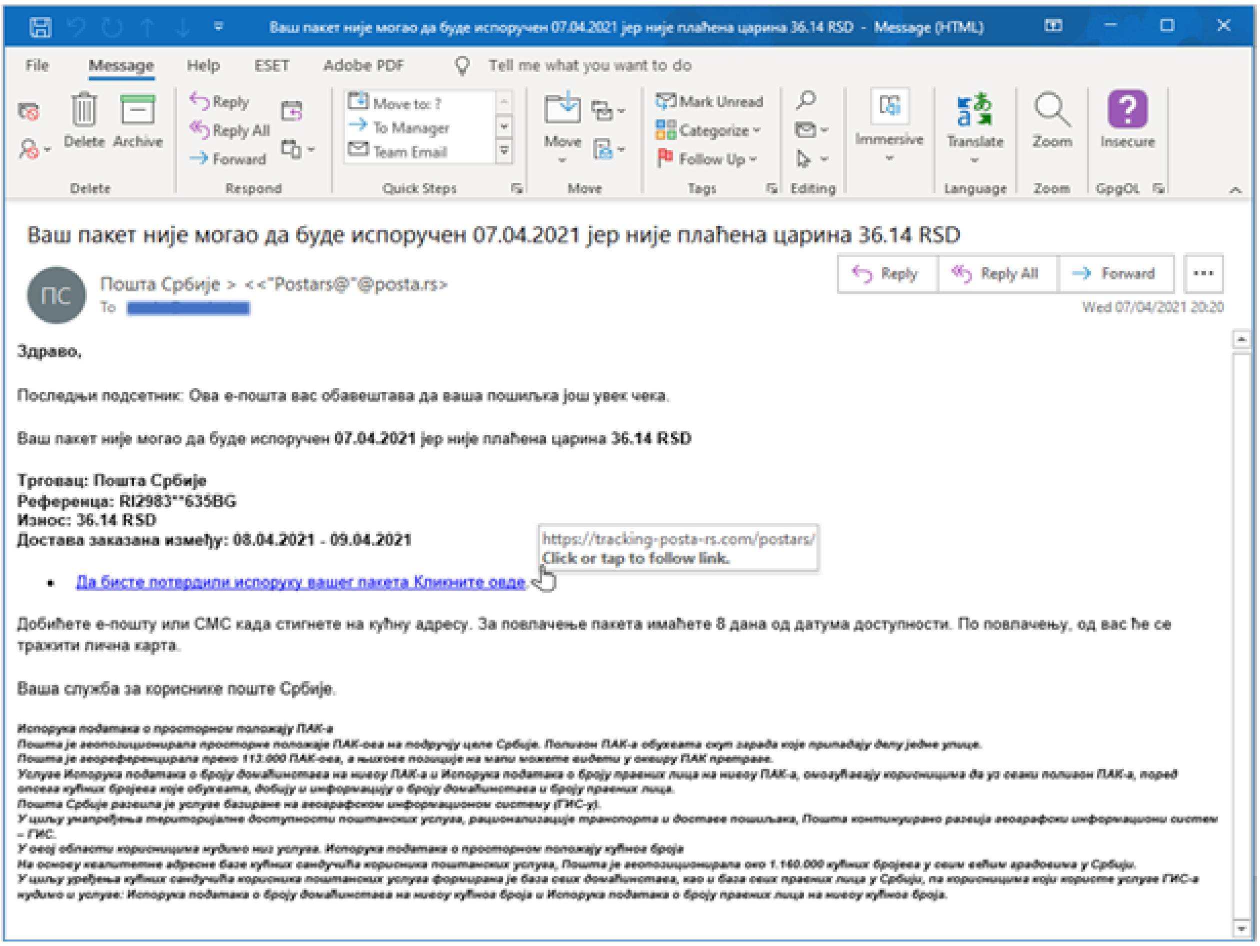
[5] https://www.imperva.com/learn/application-security/phishing-attack-scam/

Sličnost između ove dve adrese, korisnika može da navede na misao da je u pitanju bezbedna adresa internet stranice čineći ga manje svesnim da je u pitanju sajber napad.

Preporuka je da u slučaju prijema poruke koja sadrži zahtev poput promene lozinke, koju je potrebno sprovesti u nekom kratkom periodu, navodeći korisnika na brzu reakciju zbog isteka vremena i stvarajući osećaj hitnosti da se zahtev ispuni, uvek naknadno proveri URL adresa na kojoj se traži promena šifre. Preporuka je da se legitimna adresa pretraži putem internet pretraživača, a ne klikom na link iz e-poruke. Komparacijom adresa, često se mogu uočiti nedoslednosti, i na taj način se potencijalna prevara može izbeći.

Prilikom prijema poruka e-pošte u kojima se zahteva da se pristupi određenom linku, da se verifikuje lozinka i slično, iako poruka može izgledati kao da stiže iz pouzdanog izvora, male greške u kucanju ili nedoslednosti u domenu često mogu otkriti pravu prirodu date poruke, odnosno potencijalnog napada.

Sledeći primer ilustruje fišing kampanju koja je bila usmerena na korisnike poštanskih usluga. U ovom primeru, korisnici su dobijali e-poštu sa obaveštenjem da je pristigao paket korisnika, ali da nije mogao biti isporučen jer nije uplaćen iznos od 36,14 dinara za carinske troškove. Poruka je stizala sa lažne adrese: Pošte Srbije *"Postas@"@posta.rs*, sa naslovom: Vaš paket nije mogao da bude isporučen 07.04.2021 jer nije plaćena carina 36.14 RSD.

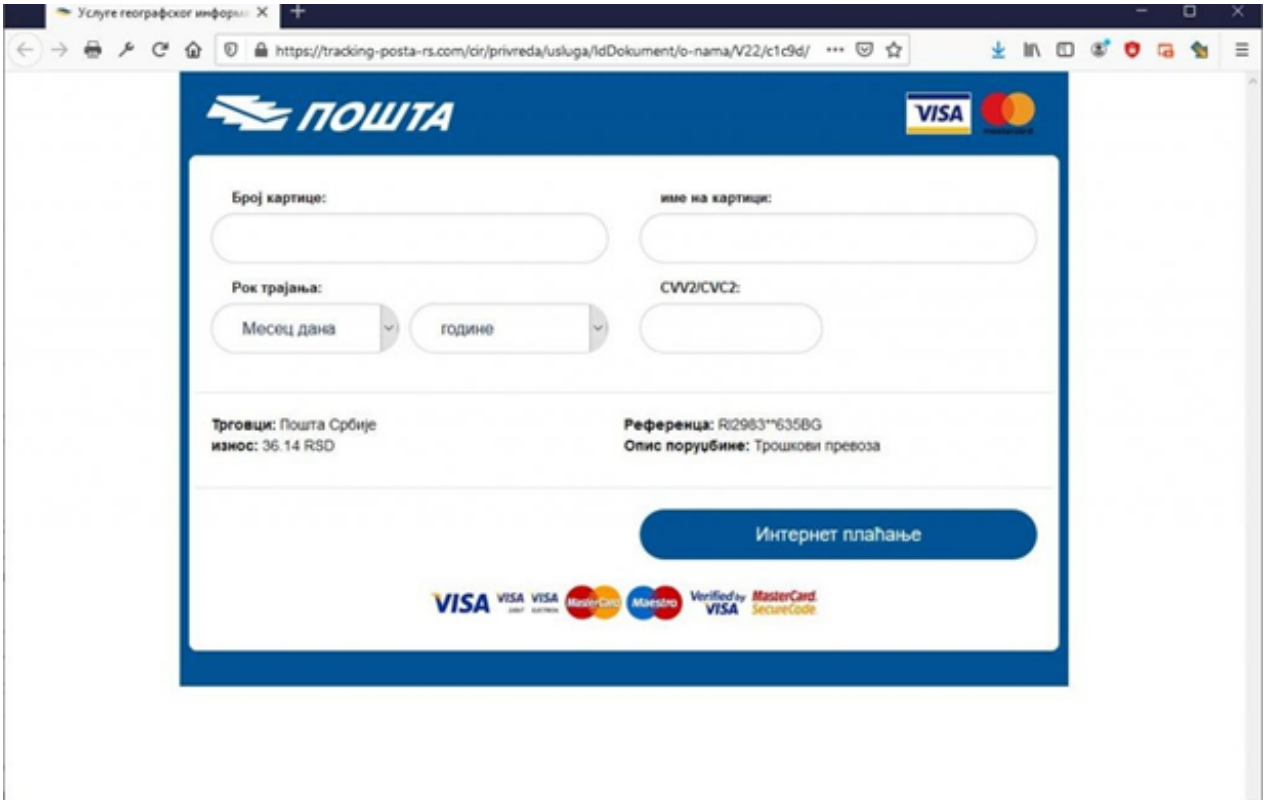


Slika 5. Primer Phishing e-poruke za Poštu Srbije uz link na kom se zahteva plaćanje

Preporuka Nacionalnog CERTa je da se pre pristupa linku, prvo proveri adresa pošiljaoca, obzirom da se adresa može lažirati, što se može videti u ovom primeru *''Postas@"@posta.rs*, iako je kao ime za prikaz naznačena „Pošta Srbije". Takođe, savet je obratiti pažnju na gramatičke greške, koje su takođe jedan od pokazatelja da je u pitanju fišing prevara.

Dalje u tekstu, prelaskom kursora preko linkovanog teksta (linka), vidi se link koji može izgledati legitimno, i otvaranjem istog, prikazuje se fišing stranica koja sadrži logo Pošte Srbije i ima sadržaj hitnosti kako bi pošiljka bila dostavljena. Iako internet stranica može izgledati kao legitimna stranica sajta Pošte Srbije, ona to zapravo nije. Na vrhu ekrana se može videti potpuno netačna URL adresa, što se može proveriti pretragom zvanične stranice Pošte Srbije putem pretraživača.

Otvaranjem linka, korisnik se preusmeravao na lažnu stranicu za internet plaćanje Pošte Srbije, u kojoj se zahtevao unos podataka: Broj platne kartice, Ime i Prezime, Rok trajanja, kao i *CVV2/CVC2* broj kartice. Unosom traženih podataka, napadač bi došao u posed informacija na osnovu kojih bi mogao da preuzme novac sa računa lica koje je ostavilo podatke.



Slika 6. Primer Phishing sajta sa formom za unos podataka za platne kartice

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

Preporuke Nacionalnog CERTa za prevenciju od fišing napada jesu:

- Obratiti pažnju na polje „*From*“ i da li je pošiljalac poznat;
- Proveriti da li postoje pravopisne greške u tekstu poruke;
- Ukoliko postoji nepotrebna hitnost za reakciju, ne žuriti sa otvaranjem linkova i priloga iz poruke;
- Proveriti legitimnost *URL* adrese, proverom adrese u internet pretraživaču;
- Uporediti da li je ime pošiljaoca povezano sa adresom e-pošte;
- Obratite dodatno pažnju kada se traži unos podataka o bankovnoj kartici, posebno kada je reč o *CVV2/CVC2* broj kartice;
- Ako primite sumnjivu poruku elektronske pošte označite je kao *Spam/Junk* ili je odmah izbrišite.

Ako ste kliknuli na link ili dokument preduzmite sledeće korake:

- Ako koristite službeni telefon ili laptop odmah kontaktirajte IT službu;
- Ako ste dali svoje podatke o bankovnom računu odmah obavestite banku;
- Aktivirajte antivirus i kliknite na „*full scan*“;
- Ako ste ostavili svoju lozinku, odmah promenite lozinke na svim nalozima;
- Ako ste izgubili novac odmah kontaktirajte svoju banku i prijavite policiji na vtk@mup.gov.rs;

Nacionalni CERT Republike Srbije ne promoviše ili favorizuje bilo koji od korišćenih javnih izvora, među kojima su i komercijalni proizvodi i usluge. Sve preporuke, analize i predlozi dati su u cilju prevencije i zaštite od bezbednosnih rizika.

REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

#odbraniseznanjem

SRB-CERT