https://doi.org/10.37528/FTTE/9788673954165/POSTEL.2022.012

MODELI FIŠING KAMPANJA KOJIMA JE ZLOUPOTREBLJEN LOGO I IME POŠTE SRBIJE

Goran Paunović
Regulatorna agencija za elektronske komunikacije i poštanske usluge, Nacionalni CERT RS, goran.paunovic@ratel.rs

Rezime: *Fišing (na engleskom phishing) je vrsta 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. U poslednje vreme intenzivirana je fišing kampanja kojom napadači zloupotrebljavaju logotip i ime Pošte Srbije. Osnovni razlog zašto je Pošta Srbije meta napada je činjenica da je Pošta u direktnom kontaktu sa korisnicima u delu novčanih transakcija, prenosa pismonosnih, paketskih i ekspres pošiljaka. Svaki od ova tri segmenta poslovanja Pošte Srbije može biti zanimljiv korisnicima, stoga napadači imaju pogodno tle za aktivnosti socijalnog inženjeringa, konkretno fišinga. U dosadašnjoj praksi bilo je više pokušaja napada u kojima je zloupotrebljen logo i ime Pošte Srbije.*

Ključne reči: *: socijalni inženjering, fišing, sajber napad, domen, domen najvišeg nivoa*

1. Uvod

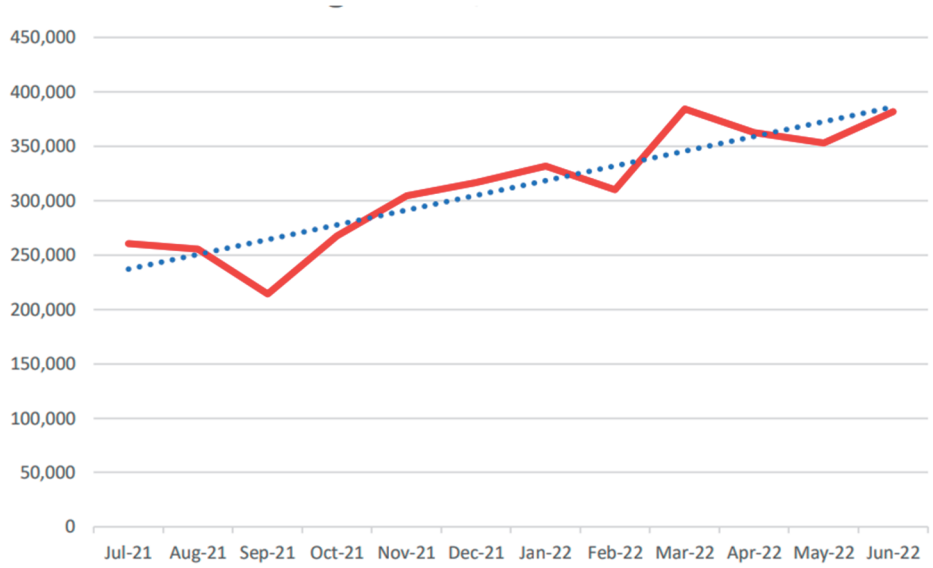
Fišing (na engleskom phishing) je tip prevare koja ima za cilj prikupljanje izloupotrebu poverljivih podataka korisnika, poput brojeva bankovnihračuna, lozinki naloga na društvenim mrežama ili pristupa elektronskojpošti. Žrtva ovog tipa sajber napada dobija poruku putem elektronske pošte, društvenih 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 prispele putem elektronske pošte. Međutim, primetan je izvestan broj napada putem upotrebe društvenih mreža i aplikacija za slanje poruka poput *WhatsApp-a, Viber-a* i ostalih. Promena koja se očekuje u izvođenju ovih napada jeste da će metode koje se koriste za slanje poruka biti sve sofisticiranije. 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 ponuđeni link;
- Ažuriranje lozinke;
- Otvaranje dokumenta 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 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, lozinke, podaci sa bankovnih kartica i drugi.

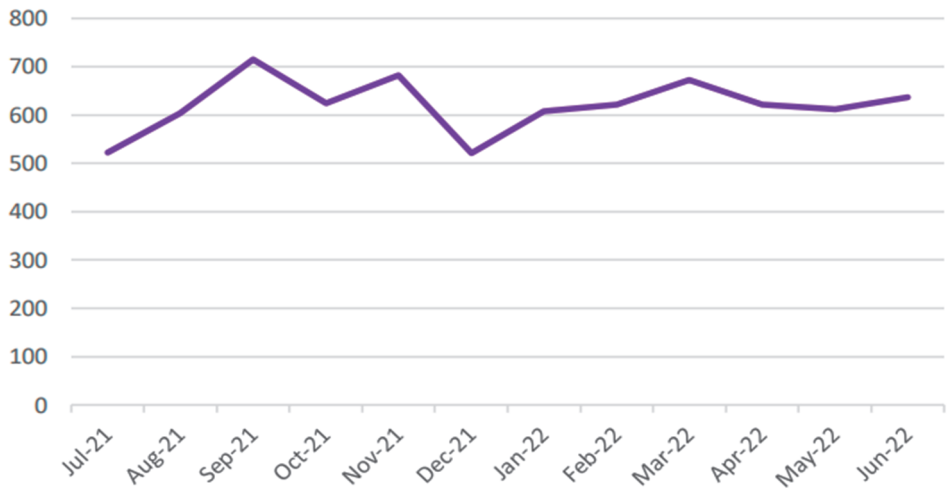
2. Stanje u svetu

U svetu je primetan rast obima fišing napada. Na slici 1. dat je prikaz trenda fizičkog obima fišing napada u svetu u periodu od početka trećeg kvartala 2021. godine do kraja drugog kvartala 2022. godine. Naime, period opservacije je poslednjih godinu dana, od jula 2021. godine do juna 2022. godine.



Slika 1. Trend obima fišing napada u periodu jul 2021. – jun 2022. godine
Izveštaj trendova phishing aktivnosti, 2. kvartal 2022. godine, [1]

U izveštaju su posebno obrađeni napadi koji su pogodili svetski priznate kompanije (svetske Brendove), prikaz je dat na slici 2.



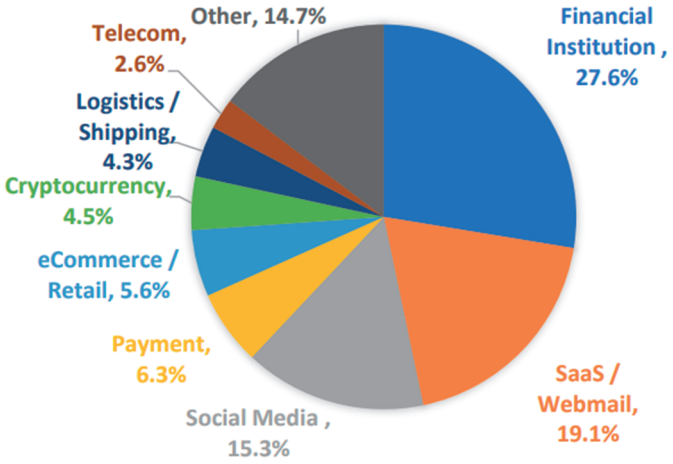
Slika 2. Broj napadnutih brendova u periodu jul 2021. – jun 2022. godine
Izveštaj trendova phishing aktivnosti, 2. kvartal 2022. godine, [1]

Tabela 1. Prikaz obima fišing napada u drugom kvartalu 2022. godine (Q2 2022)

	April 2022	Maj 2022	Jun 2022
Broj fišing web lokacija sa kojih su otkriveni napadi	362.852	353.242	381.717
Broj naslova fišing mejlova	21.540	20.339	23.550
Broj brendova ciljanih fišing napadom	621	612	637

U drugom kvartalu 2022. godine zabeleženo je ukupno 1.097.811 fišing napada, što je apsolutni kvartalni rekord ikada do sada zabeležen. U odnosu na početak 2020. godine kada je zabeleženo od 68. 000 do 94. 000 napada na mesečnom nivou, broj ovih napada je sada četiri puta veći i prešao je cifru od 380. 000 mesečno.

Na slici 3. vidi se da su finansijske institucije najviše napada pretrpele u drugom kvartalu 2022. godine. Odmah zatim su *SaaS* (*Software as a Service* aplikacije, ili *web based*) aplikacije kao deo *cloud* tehnologije u oblasti informacionih thenologija a posebno webmail aplikacije, koje se koriste za slanje mejlova preko *web-browsera* . Potom slede društvene mreže, elektronsko plaćanje roba i usluga, e-trgovinski lanci i maloprodaja, kriptovalute itd...



Slika 3. Najviše napadane grane industrije - na svetskom nivou, Izveštaj trendova phishing aktivnosti, 2. kvartal 2022. godine, [1]

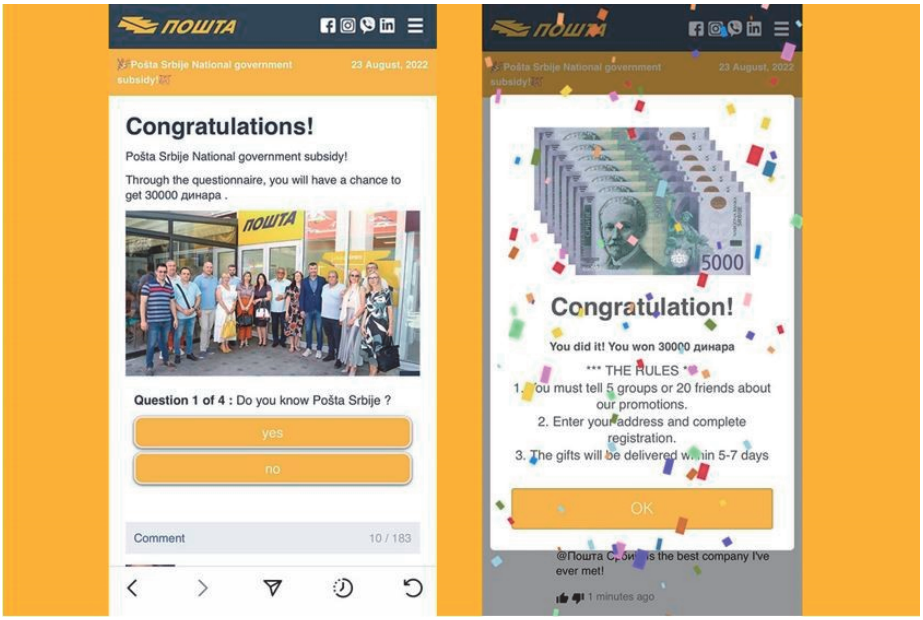
Začuđujuće deluje činjenica da je oblast telekomunikacija jedna od manje napadanih oblasti.

3. Fišing napadi na korisnike Pošte Srbije

U poslednje vreme intenzivirana je fišing kampanja kojom napadači zloupotrebljavaju logotip i ime Pošte Srbije. Osnovni razlog zašto je Pošta Srbije meta napada je činjenica da je Pošta kompanija kojoj korisnici veruju i koja je u direktnom kontaktu sa korisnicima u delu novčanih transakcija, prenosa pismonosnih, paketskih i ekspres pošiljaka. Svaki od ova tri segmenta poslovanja Pošte Srbije može biti zanimljiv korisnicima stoga napadači imaju pogodno tle za aktivnosti socijalnog inženjeringa, konkretno fišinga. U dosadašnjoj praksi bilo je više pokušaja napada u kojima je zloupotrebljen logo i ime Pošte Srbije.

3.1. Lažna nagradna igra

Korisnicima se putem društvenih mreža i raznih platformi za komunikaciju, upućuje informacija o nagradnoj igri koju navodno organizuje Pošta Srbije. Od korisnika se ljubazno zahteva da odgovore na nekoliko pitanja, nakon čega ulaze u uži izbor da osvoje novčanu nagradu. Ukoliko korisnik prihvati da odgovori na pitanja i da odgovore ubrzo zatim, biva obavešten da je „osvojio“ nagradu. Videti sliku 4.



Slika 4. Prikaz obaveštenja – Congratulations!

Dalje se od korisnika traži da o dotičnoj nagradnoj igri obavesti 20 prijatelja ili nekoliko grupa, unese adresu i kompletira registraciju unosom ličnih podataka. Dakle korisnik se lagano dovodi do faze da napadaču dostavi svoje lične podatke koje napadač dalje zloupotrebljava. Takođe obaveštavanjem 20 prijatelja napadač uvećava svoju bazu podataka novih potencijalnih žrtava.

Preporuka korisnicima: Treba biti oprezan, ne unositi lične podatke nakon prijema sličnih poruka i ne postupati na način kako se u poruci traži.

3.2. Neuspeli pokušaj isporuke pošiljke

Pri ovom napadu napadač korisnicima šalje lažnu e-poštu sa obaveštenjem o neuspešnom pokušaju isporuke pošiljke. Poruka stiže sa naslovom „Ažurirajte adresu za isporuku“ sa zahtevom da se unesu podaci i da se klikne na jedan od 2 linka:

„**Dogovorite isporuku na ovu adresu“** i

„Ažurirajte adresu za dostavu“.

Primer originalne poruke koju su primali korisnici vidi se na slici 5.

Dragi cenjeni korisniče,

Ovim e-mailom vas obaveštavamo o poslednjem neuspešnom pokušaju isporuke za pošiljku broj RS263790013BB. Ovo je posledica toga što adresa koju ste naveli ne postoji ili se ne može pronaći u okviru našeg sistema.
Šta se dalje dešava?
Vaša pošiljka je vraćena u naš lokalni depo, gde će ostati narednih sedam radnih dana.
Sada nam možete dati ažuriranu adresu za ovu pošiljku klikom ovde.
Za ponovnu isporuku vaše pošiljke biće naplaćena naknada.

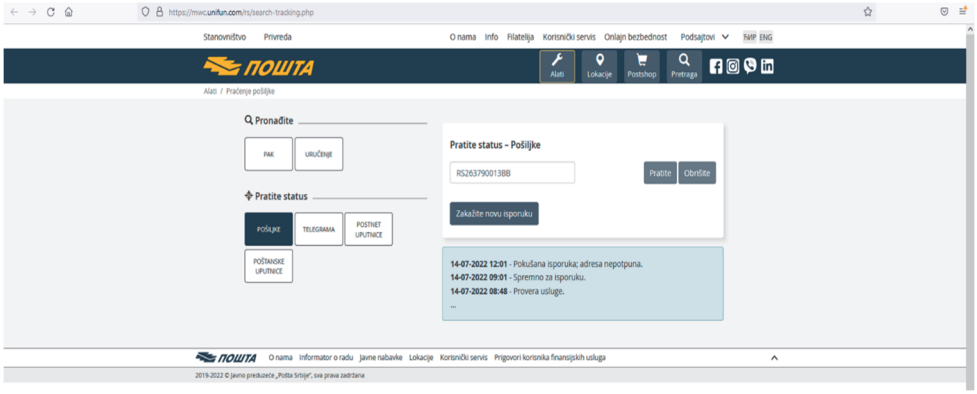
- >> Dogovorite isporuku na novu adresu
- >> Ažurirajte adresu za isporuku

Takođe možete izabrati da preuzmete svoju pošiljku iz našeg depoa na Takovska 2, 11120 Belgrade.
Ako su vam potrebne dodatne informacije o ovom pokušaju isporuke, molimo vas popunite našu kontakt formu.

Srdačan pozdrav
Pošta Srbije

Slika 5. Obaveštenje o neuspešnom pokušaju isporuke pošiljke

Oba data linka vode na fišing stranicu (slika 6.) koja lažira logo Pošte Srbije i na kojoj se od korisnika zahteva da unese lične podatke. Svi podaci koje korisnik unese na lažnu formu mogu biti zloupotrebljeni.

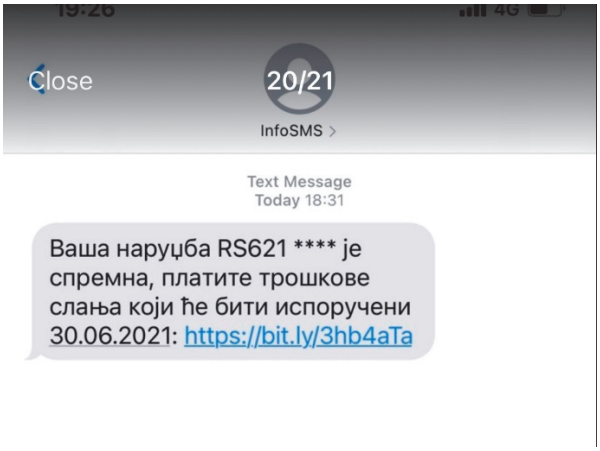


Slika 6. fišing stranica - Lažna forma koja podseća na jednu od web stranica Pošte Srbije

Preporuka korisnicima: Ne otvarati ovu poruku, ne unositi lične podatke, poruku treba obrisati.

3.3. Prispela porudžbina za koju treba platiti troškove

Informacija o prispeloj porudžbini/pošiljci za čije uručenje je potrebno platiti troškove je jedan od prvih napada u kojima je zloupotreblena pošta Srbije. Korisnicima se šalje *SMS* poruka da im je navodno stigla porudžbina i da je za isporuku potrebno platiti troškove (slika 7.)

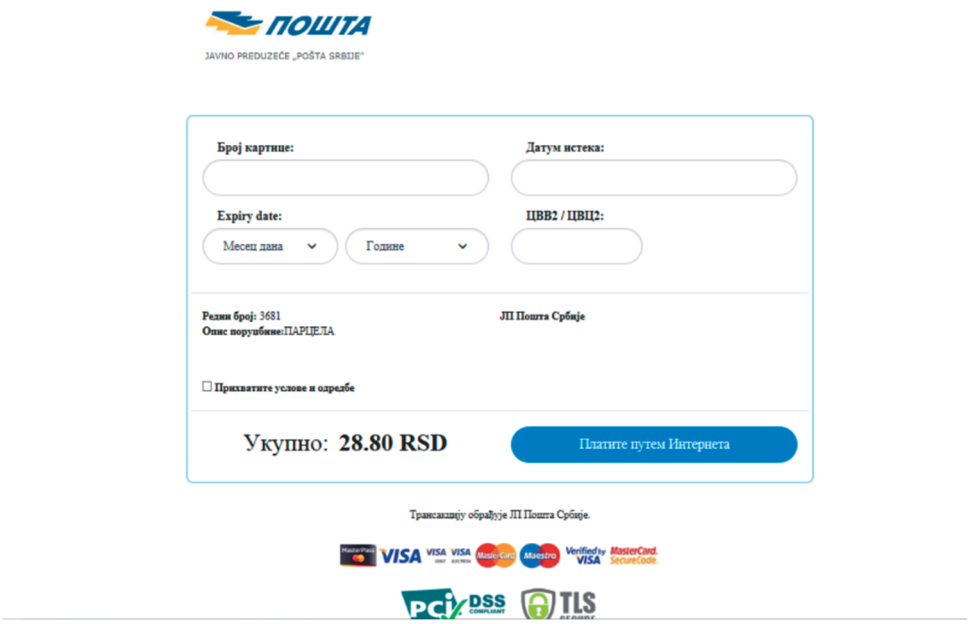


Slika 7. Inicijalna SMS poruka kojom se korisnik usmerava na maliciozni link

Link iz poruke vodi na lažnu stranicu (slika 8.) na kojoj se traži popunjavanje podataka o bankovnoj kartici koji omogućavaju napadačima da preuzmu sav novac sa računa korisnika. Lažna stranica zloupotrebljava vizuelni identitet Pošte Srbije, sadrži logo i naziv Pošte Srbije.

Javno preduzeće „Pošta Srbije“ je upozorilo javnost, korisnike i nadležne institucije uz obrazloženje da sa svojim korisnicima ne komunicira na ovaj način i da je potrebno da obrate dodatnu pažnju.

Preporuka korisnicima: Ne otvarati link iz poruke i ne popunjavati tražene podatke.

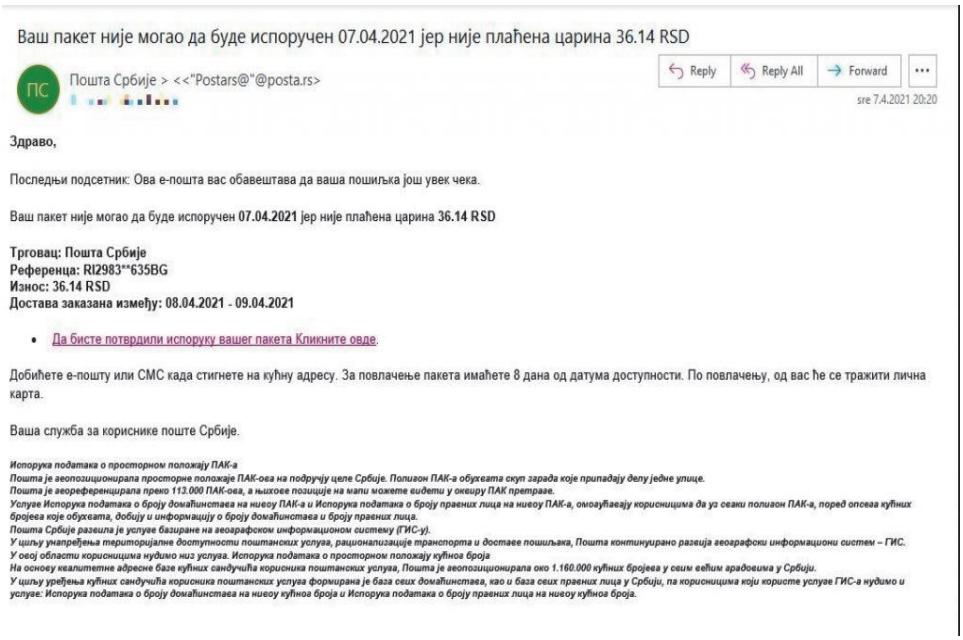


Slika 8. Lažna stranica na kojoj se traži popunjavanje podataka o bankovnoj kartici

3.4. Uplata carinskih dažbina za pošiljku prispelu iz inostranstva

Ova fišing kampanja koja je takođe usmerena na korisnike poštanskih usluga. Korisnici primaju e-poštu sa obaveštenjem da je za njih prispeo paket, ali da nije mogao biti isporučen jer nije uplaćen iznos od 36,14 dinara namenjen za carinske troškove (pogledati prikaz - slika 9). Poruka stiže sa lažne adrese: **Pošte Srbije *"Postas''@posta.rs,*** sa naslovom: **Vaš paket nije mogao da bude isporučen jer nije plaćena carina 36.14 RSD**. U poruci e-pošte se dalje od korisnika zahteva da klikne na link na kojem piše **"Da biste potvrdili isporuku vašeg paketa - kliknite ovde**", nakon čega korisnik navodno dobija e-poštu ili *SMS* poruku kojom se potvrđuje isporuka pošiljke. Klikom na ponuđeni link korisnik se preusmerava na lažnu stranicu za internet plaćanje (slika 10.) na kojoj se od korisnika zahteva da unese sledeće podatke: Broj platne kartice, Ime i Prezime, Rok trajanja kartice, kao i *CVV2/CVC2* broj kartice. Svi podaci koje korisnik unese u lažnu formu mogu biti zloupotrebljeni.

Preporuka korisnicima: Poruku ne otvarati i ne unositi lične podatke, istu treba trajno obrisati.



Ваш пакет није могао да буде испоручен 07.04.2021 јер није плаћена царина 36.14 RSD

ПС Пошта Србије > <<"Postars@"@posta.rs>

Reply | Reply All | Forward | ...

sre 7.4.2021 20:20

Здраво,

Последњи подсетник: Ова е-пошта вас обавештава да ваша пошиљка још увек чека.

Ваш пакет није могао да буде испоручен **07.04.2021** јер није плаћена царина **36.14 RSD**

Трговац: Пошта Србије
Референца: RI2983635BG**
Износ: 36.14 RSD
Достава заказана између: 08.04.2021 - 09.04.2021

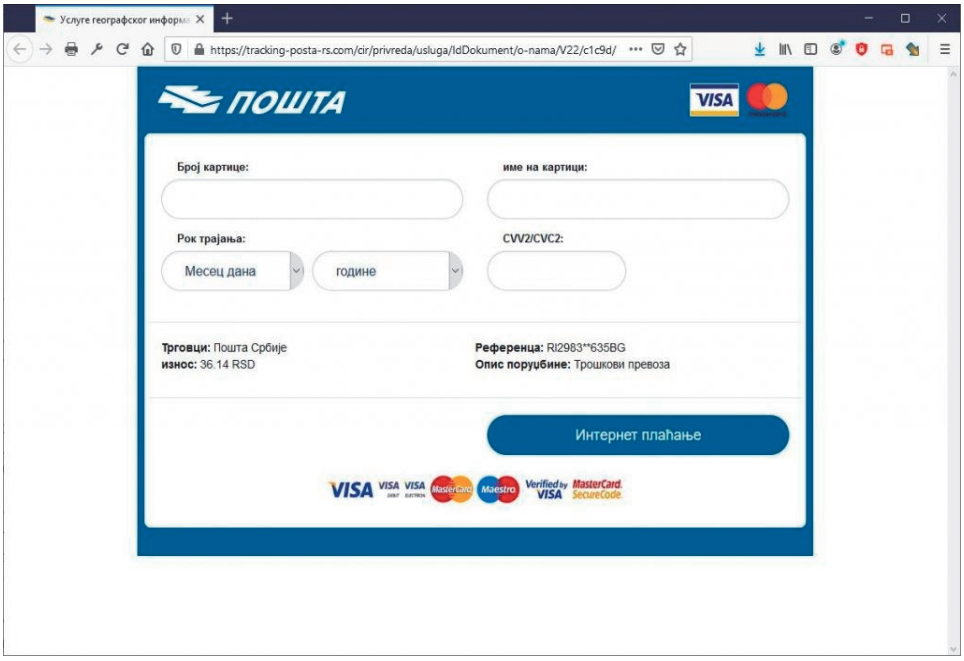
- Да бисте потврдили испоруку вашег пакета Кликните овде.

Добићете е-пошту или СМС када стигнете на кућну адресу. За повлачење пакета имаћете 8 дана од датума доступности. По повлачењу, од вас ће се тражити лична карта.

Ваша служба за кориснике поште Србије.

Испорука података о просторном положају ПАК-а
Пошта је геопозиционирала просторне положаје ПАК-ова на подручју целе Србије. Полигон ПАК-а обухвата скуп зграда које припадају делу једне улице.
Пошта је georeferencirala преко 113.000 ПАК-ова, а њихове позиције на мапи можете видети у оквиру ПАК претраге.
Услуге Испорука података о броју домаћинстава на нивоу ПАК-а и Испорука података о броју правних лица на нивоу ПАК-а, омогућавају корисницима да уз сваки полигон ПАК-а, поред описа кућних бројева које обухвата, добију и информацију о броју домаћинстава и броју правних лица.
Пошта Србије развила је услуге базиране на географском информационом систему (ГИС-у).
У циљу унапређења територијалне доступности поштанских услуга, рационализације транспорта и доставе пошиљака, Пошта континуирано развија географски информациони систем – ГИС.
У овој области корисницима нудимо низ услуга. Испорука података о просторном положају кућног броја
На основу квалитетне адресне базе кућних сандучића корисника поштанских услуга, Пошта је геопозиционирала око 1.160.000 кућних бројева у свим већим градовима у Србији.
У циљу уређења кућних сандучића корисника поштанских услуга формирана је база свих домаћинстава, као и база свих правних лица у Србији, па корисницима који користе услуге ГИС-а нудимо и услуге: Испорука података о броју домаћинстава на нивоу кућног броја и Испорука података о броју правних лица на нивоу кућног броја.

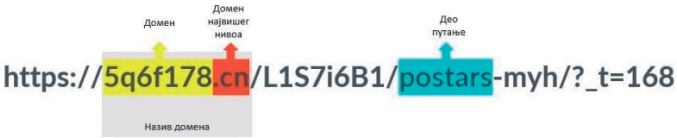
Slika 9. Lažni e-mail o nemogućnosti isporuke paketa



Slika 10. Lažna stranica na kojoj se traži popunjavanje podataka o bankovnoj kartici

4. Odbraniti se opreznošću i znanjem

Korisnici interneta se takođe savetuju da obrate pažnju na elemente linka koji mogu ukazivati na lažnu stranicu. Pažnju najviše treba usmeriti na naziv domena. U nastavku je primer lažne stranice, a naziv domena je: *5q6f178.cn*. Na ovom primeru se Pošta Srbije pominje u delu putanje ka datoteci, što je pokušaj navođenja korisnika interneta da pomisli da je to deo naziva domena (prikaz daje slika 11.).



Slika 11. Link ka lažnoj stranici Pošte Srbije

Primer za legitimnu veb adresu internet stranice Pošte Srbije pokazuje registrovan naziv domena Pošte Srbije (slika 12). Kao što se može videti domen najvišeg nivoa u ovom slučaju odgovara domenu Republike Srbije (. rs).

Slika 12. Link ka legitimnoj stranici Pošte Srbije

5. Informisanje nadležnih institucija

Napadi na Poštu Srbije ali i svi drugi napadi na institucije, pravna i fizička lica mogu se prijaviti Nacionalnim CERT-u na e-mail: info@cert.rs ili na sajtu Nacionalnopg CERT-a: https://www.cert.rs/ kroz formu koja se nalazi na sledećem linku: https://www.cert.rs/prijava.html .

6. Zaključak

Način na koji je došlo do kompromitovanja imena i logoa Pošte Srbije može biti primenjen i na druge kompanije, privatne poštanske opšreatore, telekomunikacione opreatore, banke, osiguravajuće kuće, prevoznike, trgovinske lance, turističke agencije i sve kompanije koje se bave pružanjem usluga korisnicima. U konkretnim napadima Pošta ni jednim svojim postupkom nije načinila grešku niti pokazala ranjivost svog informacionog sistema, jedina njena krivica je što postoji na internetu, ima svoj domen, i pruža usluge korisnicima koje mogu biti primamljive kako korisnicima tako i napadačima (koji ih zloupotrebljavaju). Podizanje nivoa svesti u čitavom društvu je jedan od preduslova za uspešnu odbranu od navedene vrste napada.

Literatura

[1] APWG.ORG, „Phishing Activity Trends report-a, 2nd Quarter 2022, Unifying the Global Response to Cybercrime", 20.09.2022. http://www.apwg.org/

[2] B. Rodić, D Živković, S. Milojević, i V. Rodić, "Da li smo sigurni da smo bezbedni", Osnove informacione bezbednosti, Jul 2019

[3] ENISA, European Union Agency for Cybersecurity, IX edition of the ENISA Threat Landscape (ETL) report, Annual report on the status of the cybersecurity threat landscape 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[4] ENISA, European Cybersecurity Skills Framework Role Profiles, document lists, Cybersecurity professional role profiles https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles, 19 sept. 2022

[5] ENISA, European Cybersecurity Skills Framework Role Profiles, document lists, Cybersecurity professional role profiles https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles, 19 sept. 2022

[6] D Schlette and Marco Caselli, „Beyond Incident Reporting - An Analysis of Structured Representations for Incident Response", 2022 First Conference, Dublin, IE, June 29 2022

Abstract: *Phishing is a type of fraud that aims to collect and abuse confidential user data, such as bank account numbers, passwords, accounts on social networks or access to e-mail. The victim of this type of cyber attack receives a message via e-mail, social networks, telephone or SMS in which it is required to visit a link or open a document and enter personal and confidential information. Recently, a phishing campaign has been intensified in which the attackers abuse the logo and name of the Post of Serbia. The main reason why the Post of Serbia is the target of attacks is the fact that the Post is in direct contact with users in the area of financial transactions, the traffic of letters,*

parcels and express items. Each of these four business segments of the Post of Serbia can be interesting to users, therefore attackers have a suitable ground for social engineering activities, specifically phishing. There have been several attempted attacks in which the logo and name of the Post of Serbia were misused, so far.

Keywords: *social engineering, phishing, cyber attack, domain, top level domain*

MODELS OF PHISHING CAMPAIGNS WHICH HAVE ABUSED THE LOGO AND NAME OF THE POST OF SERBIA

Goran Paunović