SVEUČILIŠTE/UNIVERZITET „VITEZ“

FAKULTET INFORMACIONIH TEHNOLOGIJA

STUDIJ CIKLUSA; GODINA STUDIJA: I CIKLUS; III GODINA

SMJER: INFORMACIJSKE TEHNOLOGIJE

Zulka Musić

PHISHING NAPADI

SEMINARSKI RAD

Travnik, 29.06.2025. godine

SVEUČILIŠTE/UNIVERZITET „VITEZ“

FAKULTET INFORMACIONIH TEHNOLOGIJA

STUDIJ CIKLUSA; GODINA STUDIJA: I CIKLUS; III GODINA

SMJER: INFORMACIJSKE TEHNOLOGIJE

PHISHING NAPADI

SEMINARSKI RAD

IZJAVA: Ja **Zulka Musić**, student Sveučilišta/Univerziteta „VITEZ“, Indeks broj: **390-24/RIIT** odgovorno i uz moralnu i akademsku odgovornost izjavljujem da sam ovaj rad izradio potpuno samostalno uz korištenje citirane literature i pomoć predmetnog profesora.

STUDENT: Zulka Musić

PREDMET: Računarska pismenost

MENTOR: prof.dr.sc. Jasmin Azemović

ASISTENT: Nedim Sadović

SADRŽAJ

1. UVOD

1.1. PROBLEM, PREDMET I OBJEKT ISTRAŽIVANJA

U eri digitalne transformacije, gdje su elektronska komunikacija i internet postali neizostavni dio svakodnevnog života, sigurnost korisnika i informacija postaje kritično pitanje. Phishing napadi predstavljaju jedan od najrasprostranjenijih oblika sajber kriminala. Riječ je o vrsti prevare kojom napadači, lažno se predstavljajući kao pouzdani subjekti (npr. banke, servisi, poslodavci), nastoje prevariti korisnike da otkriju osjetljive podatke poput lozinki, brojeva kreditnih kartica ili pristupnih podataka za korisničke račune. Problem phishinga leži u njegovoj jednostavnosti, masovnosti i visokom stepenu efikasnosti, zbog čega se predstavlja kao ozbiljna prijetnja pojedincima, organizacijama i cjelokupnom informacionom sistemu.

Predmet istraživanja u ovom radu su phishing napadi – njihova struktura, metode, ciljevi i načini zaštite.

Objekt istraživanja obuhvata korisnike interneta, posebno one koji koriste elektronsku poštu, online bankarstvo, društvene mreže i ostale digitalne servise, kao i informacioni sistemi koji su često meta ovakvih napada.

1.2. SVRHA I CILJEVI ISTRAŽIVANJA

Svrha ovog rada jeste doprinijeti boljem razumijevanju phishing napada – njihovog porijekla, oblika i načina funkcionisanja – te naglasiti značaj prevencije i edukacije.

Ciljevi istraživanja su:

- Analizirati pojavu phishing napada i klasifikovati njihove oblike.
- Identifikovati najčešće metode napada i kanale putem kojih se realizuju.

- Prikazati stvarne slučajeve phishinga i njihove posljedice.
- Ponuditi pregled najefikasnijih mjera zaštite, kako tehničkih tako i edukativnih.
- Podići svijest korisnika o prepoznavanju i prijavljivanju phishing pokušaja.

1.3. RADNA HIPOTEZA I POMOĆNE HIPOTEZE

Na osnovu predmeta i problema istraživanja ovog seminarskog rada može se postaviti glavna hipoteza:

Phishing napadi se šire i uspijevaju prvenstveno zbog nedovoljne informatičke pismenosti korisnika i nedostatka efikasnih mjera zaštite.

Kroz svrhu i cilj istraživanja možemo izvući tri pomoćne hipoteze:

- Većina korisnika ne zna prepoznati lažnu elektronsku poruku.
- Organizacije ne ulažu dovoljno u edukaciju zaposlenika o sajber prijetnjama.
- Tehnološke barijere i alati nisu dovoljni bez svijesti i pažnje krajnjeg korisnika.

1.4. NAUČNE METODE

Za izradu rada primijenjene su sljedeće naučne metode:

- Deskriptivna metoda, korištena za opis pojava, definicija i klasifikacija phishinga.
- Analitička metoda, korištena za ispitivanje strukture napada i posljedica.
- Kompilacijska metoda, primijenjena kroz prikupljanje podataka iz različitih izvora (naučnih članaka, izvještaja, online izvora).
- Komparativna analiza, za poređenje pristupa zaštiti u različitim kontekstima.

Prikupljeni podaci su obrađeni tekstualno. Izvori su: naučni članci, internet portali i izvještaji organizacija koje se bave sajber sigurnošću.

1.5. STRUKTURA RADA

Struktura seminarskog rada je usklađena sa Uputstvom za pisanje seminarskog rada na prvom ciklusu studija kao i temi seminarskog rada. On sadrži devet poglavlja.

- Prvo poglavlje, Uvod, sadrži pet pod poglavlja:
  - Problem, predmet i objekt isprašivanja,
  - Svrha i ciljevi istraživanja,
  - Radna hipoteza i pomoćne hipoteze,
  - Naučne metode,
  - Struktura rada.
- Drugo poglavlje, Pojam i historija phishinga, sadrži tri pod poglavlja:
  - Pojam phishinga,
  - Historija phishinga,
  - Savremeni značaj phishinga.
- Treće poglavlje, Vrste phishing napada, sadrži osam pod poglavlja:
  - Klasični (masovni) e-mail phishing,
  - Spear phishing (ciljani phishing),
  - Whaling (phishing visokog profila),
  - Smishing (SMS phishing),
  - Vishing (voice phishing),
  - Pharming,
  - Angler phishing (putem društvenih mreža),
  - Ostale i savremene varijacije phishinga.
- Četvrto poglavlje, Mehanizam i tehnike phishinga, sadrži osam pod poglavlja:
  - Socijalni inženjering,
  - Lažne web stranice,
  - Zlonamjerni linkovi i prilozi,
  - Spooging – lažno predstavljanje,
  - Automatizacija phishing kampanja,
  - Upotreba legitimnih servisa za obmanu,

    - Mobilni phishing i napadi putem aplikacija,
    - Phishing putem QR koda.
- Peto poglavlje, Primjeri phishing napada iz prakse, sadrži pet pod poglavlja:
    - Napad na Google i Facebook (2013 – 2015),
    - Phishing kampanje protiv građana u BiH i regionu,
    - Napad na američku kompaniju UBIQUITI (2021),
    - COVID–19 i phishing pandemija,
    - Ransomware phishing (npr. WANNACRY).
- Šesto poglavlje, Posljedice phishing napada, sadrži šest pod poglavlja:
    - Financijski gubici,
    - Krađa identiteta,
    - Ugrožavanje poslovne i državne sigurnosti,
    - Gubitak ugleda i povjerenja korisnika,
    - Pravne i regulatorne posljedice,
    - Psihološke posljedice na žrtve.
- Sedmo poglavlje, Zaštita od phishing napada, sadrži pet pod poglavlja:
    - Tehničke mjere zaštite,
    - Edukacija korisnika i digitalna pismenost,
    - Organizacione sigurnosne politike,
    - Pravna i institucionalna zaštita,
    - Uloga korisnika u prevenciji.
- Osmo poglavlje, Trendovi i budućnost phishing napada.
- Deveto poglavlje, Zaključak, daje odgovore na postavljene hipoteze.

2. POJAM I HISTORIJA PHISHINGA

2.1. POJAM PHISHINGA

Phishing je oblik sajber napada koji koristi tehnike socijalnog inženjeringa kako bi prevario korisnika i naveo ga da otkrije osjetljive informacije, kao što su korisnička imena, lozinke, brojevi kreditnih kartica ili drugi lični podaci. Termin „phishing“ je izveden iz engleske riječi fishing (pecanje), pri čemu se „peca“ korisnik pomoću lažne poruke koja izgleda kao da dolazi iz pouzdanog izvora. U tom smislu, napadač „baca mamac“ u obliku e-maila, poruke, telefonskog poziva ili lažne web stranice, a korisnik koji „zagrize“ taj mamac nesvjesno odaje svoje povjerljive informacije.[1]

Phishing poruke se najčešće šire putem e-maila, ali sve češće koriste i druge komunikacione kanale: SMS poruke (smishing), telefonske pozive (vishing), pa čak i društvene mreže i aplikacije za razmjenu poruka. Ono što phishing napade čini opasnima jeste njihova sposobnost da imitiraju stvarne komunikacije – koriste identične logotipe, dizajn i čak e-mail adrese koje izgledaju legitimno.

Ovi napadi se oslanjaju više na psihološku manipulaciju nego na tehničke ranjivosti. Napadači koriste taktike zastrašivanja, hitnosti („vaš račun je suspendovan!“), lažnog autoriteta („kontaktira vas banka“) i privida legitimnosti kako bi natjerali korisnika da brzo i nepromišljeno reaguje.

2.2. HISTORIJA PHISHINGA

Historija phishinga seže u rane dane komercijalnog interneta, sredinom 1990-ih. Prvi poznati oblik phishing napada pojavljuje se na America Online (AOL), gdje su se korisnici

[1] https://encyclopedia.kaspersky.com/glossary/phishing/ Pristupljeno 23.06.2025.

primoravali da unesu svoje podatke putem lažnih „sigurnosnih poruka“. Oni su postali žrtve kada su ti podaci korišteni za kreiranje novih lažnih naloga i širenje prevara.

Termin „phishing“ se prvi put pojavljuje 2. januara 1996. godine na Usenet grupi AOHell. S obzirom na povezanost sa tehničkom „phreaking“ scenom (telefon hacking), slova f su zamijenjena sa ph – naziv odaje počast toj frakciji hakera.[2]

Početkom 2000-ih, phishing napadi su se proširili globalno – lažne poruke slala su se u ime PayPala, eBaya i banaka, uz kreiranje lažnih web-stranica identičnih originalima i sofisticirane tehnike zamjene URL adresa radi prevare korisnika.

U posljednjih 10–15 godina, phishing je postao značajan alat kibernetičkog ratovanja i špijunaže – ciljana su meta korporacije, vladine institucije i kritična infrastruktura. Sa razvojem AI i deepfake tehnologija, napadi su postali personalizirani audio/video sadržaji te još vjerodostojniji.

2.3. SAVREMENI ZNAČAJ PHISHINGA

Danas phishing predstavlja pokretačku snagu većine sajber prijetnji. Prema analizama, preko 90 % sigurnosnih incidenata započinje phishingom. Iako su tehnički filtri i alati znatno unaprijeđeni, ključnu ulogu i dalje ima korisnik – koji ne prepozna lažne poruke i klikne na zaražene linkove.

Historijsko razumijevanje phishinga neophodno je jer pokazuje da, iako tehnologija napreduje, suštinska manipulacija ostaje ista – jer je i dalje u osnovi socijalni inženjering, a ne tehnička ranjivost.[3]

[2] https://www.phishing.org/history-of-phishing Pristupljeno 23.06.2025.
[3] https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full Pristupljeno 23.06.2025.

3. VRSTE PHISHING NAPADA

Phishing napadi su postali sveprisutni i raznovrsni, prilagođeni različitim ciljevima, okruženjima i komunikacionim kanalima. Iako svi imaju istu osnovnu svrhu – prevariti korisnika da otkrije povjerljive informacije – oblici phishinga se razlikuju prema tehnici, cilju i načinu distribucije. U nastavku su opisani najčešći oblici phishing napada.

3.1. KLASIČNI (MASOVNI) E-MAIL PHISHING

Ovo je najpoznatiji i najrasprostranjeniji oblik phishinga. Napadač šalje e-mail koji izgleda kao da dolazi od pouzdane institucije – banke, pošte, online trgovine, IT servisa itd. Poruka najčešće sadrži:

- Upozorenje o sigurnosnom problemu ("Vaš račun je kompromitovan"),
- Poziv na hitnu akciju ("Potvrdite svoj identitet odmah"),
- Lažni link koji vodi na stranicu koja imitira original.

Na toj stranici korisnik unosi podatke misleći da su sigurni, ali oni odmah odlaze napadaču. Napadi ove vrste se šire masovno, na hiljade korisnika, s ciljem da barem manji broj „zagrize“ mamac.

Primjer:

E-mail koji izgleda kao da dolazi od PayPala s porukom: "Vaš račun je suspendovan zbog sumnjive aktivnosti. Kliknite ovdje da ga aktivirate ponovo."[4]

[4] https://encyclopedia.kaspersky.com/glossary/phishing/ Pristupljeno 24.06.2025.

3.2. SPEAR PHISHING (CILJANI PHISHING)

Za razliku od masovnog phishinga, spear phishing cilja određenu osobu, organizaciju ili instituciju. Ova vrsta napada zahtijeva pripremu – napadač prikuplja informacije o žrtvi (npr. ime, pozicija u firmi, prethodni kontakti), kako bi poruka izgledala uvjerljivo i legitimno.

Cilj: Prevariti žrtvu da klikne na link, preuzme maliciozni dokument ili otkrije osjetljive informacije, često poslovne prirode.

Primjer:

E-mail upućen direktoru finansija u firmi, navodno od generalnog direktora, sa zahtjevom za hitan prijenos sredstava dobavljaču.[5]

3.3. WHALING (PHISHING VISOKOG PROFILA)

Whaling je posebna forma spear phishinga, gdje su meta visoki rukovodioci – direktori, menadžeri, državni službenici ili druge uticajne osobe. Naziv potiče iz engleskog “whale” (kit), što implicira „veliku metu“.

Ovi napadi su izuzetno sofisticirani – koriste lažne e-mail domene, potpise pa čak i lažne telefonske pozive. Cilj je prikupiti veliki finansijski iznos, povjerljive dokumente ili kontrolu nad važnim sistemima.

Primjer:

Falsifikovani zahtjev za bankovni transfer koji izgleda kao da dolazi direktno od CEO-a kompanije.[6]

[5] https://www.kaspersky.com/resource-center/definitions/spear-phishing Pristupljeno 24.06.2025.
[6] https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/whaling-attack/ Pristupljeno 24.05.2025.

3.4. SMISHING (SMS PHISHING)

Smishing koristi tekstualne poruke (SMS) za phishing napad. Napadač šalje poruku koja izgleda kao obavještenje iz banke, pošte ili druge usluge, često s linkom koji vodi na lažnu stranicu.

Primjer:

"BH Pošta: Vaš paket je zaustavljen. Platite 2,99 KM putem sljedećeg linka da bismo nastavili isporuku."[7]

3.5. VISHING (VOICE PHISHING)

Vishing se oslanja na telefonske pozive. Napadač se predstavlja kao službenik banke, tehničke podrške ili policije i traži:

- podatke (broj kartice, PIN),
- instalaciju malicioznog softvera,
- potvrdu transakcije.

Primjer:

"Zovemo iz vaše banke. Uočili smo sumnjivu aktivnost. Recite nam zadnje četiri cifre vaše kartice i sigurnosni kod da bismo zaustavili uplatu."[8]

[7] https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it Pristupljeno 24.06.2025.
[8] https://www.proofpoint.com/us/blog/security-awareness-training/vishing-attacks-whos-really-line Pristupljeno 24.06.2025.

3.6. PHARMING

Pharming je tehnološki sofisticiran oblik phishinga. Napadač kompromituje DNS zapis – sistem koji prevodi adrese poput *www.mojabanka.ba* – zbog čega žrtva bude preusmjerena na lažnu stranicu koja izgleda identično kao prava.

Primjer:

Korisnik unosi ispravnu URL adresu banke, ali je preusmjeren na kopiju stranice kojom upravlja napadač.[9]

3.7. ANGLER PHISHING (PUTEM DRUŠTVENIH MREŽA)

Angler phishing se odvija preko društvenih mreža. Napadači kreiraju lažne profile (npr. podrške brenda), reagiraju na komentare korisnika i šalju linkove koji vode na phishing stranice.

Primjer:

Korisnik požali na uslugu u komentarima, a onda ga kontaktira lažni profil „podrške“ koji traži podatke ili šalje link za verifikaciju.[10]

[9] https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm Pristupljeno 24.06.2025.
[10] https://www.experian.com/blogs/ask-experian/what-is-angler-phishing-and-how-can-you-avoid-it/ Pristupljeno 24.06.2025.

3.8. OSTALE I SAVREMENE VARIJACIJE PHISHINGA

- Business Email Compromise (BEC): Ciljani poslovni napadi koji imitiraju službenu komunikaciju radi prevare.
- Clone phishing: Napadač presretne i promijeni legitiman e-mail koji je već stigao, dodajući maliciozni link ili prilog.
- Man-in-the-Middle (MitM) phishing: Napadač presreće komunikaciju korisnika sa servisom da ukrade podatke.

4. MEHANIZMI I TEHNIKE PHISHINGA

Phishing napadi nisu samo slanje lažnih poruka – iza njih stoje pažljivo osmišljeni mehanizmi i tehnike koje koriste kombinaciju psihološke manipulacije, tehničkih trikova i automatizacije kako bi povećali vjerovatnoću uspjeha.

4.1. SOCIJALNI INŽENJERING

Socijalni inženjering je osnova svakog phishing napada. To je metoda manipulacije ljudima s ciljem da prekrše sigurnosne protokole i otkriju povjerljive informacije.

Phishing poruke ciljaju na emocije:

- osjećaj hitnosti (npr. „Vaš račun će biti zatvoren ako odmah ne reagujete“),
- strah (npr. „Otkriven je pokušaj prijave na vaš račun“),
- radoznalost (npr. „Pogledajte ovu fakturu koju niste platili“),
- povjerenje (poruka izgleda kao da dolazi od šefa ili banke).

Napadači koriste emocije da potaknu brzu odluku bez provjere autentičnosti. Dashessian i tim pokazuju kako phishing iskorištava strah i hitnost kao primarne faktore socijalnog inženjeringa.[11]

4.2. LAŽNE WEB STRANICE

Ključna komponenta phishinga su lažne (klonirane) web stranice koje izgledaju identično kao legitimne. Karakteristično je:

- identičan dizajn i logotipi,

[11] https://www.imperva.com/learn/application-security/social-engineering-attack/ Pristupljeno 24.06.2025.

- URL adrese koje nalikuju originalima (typosquatting – npr. paypal-secura.com vs paypal.com),
- forme za unos podataka usmjerene napadaču.

Check Point istražuje kako ove stranice zbunjuju nepažljive korisnike, koristeći čak i male greške u domeni.[12]

4.3. ZLONAMJERNI LINKOVI I PRILOZI

Phishing e-mailovi često sadrže:

- linkove ka zlonamjernim sajtovima,
- priloge (PDF, Word, ZIP) s makroima ili skriptama koje instaliraju malvere (ransomware, keyloggere).

Check Point Research naglašava sve veći broj PDF napada: "22 % svih cyber napada kreće iz weaponizovanih PDF fajlova".[13]

4.4. SPOOFING – LAŽNO PREDSTAVLJANJE

E-mail spoofing predstavlja tehniku kojom napadač lažno prikazuje adresu pošiljaoca e-maila, čineći da izgleda kao da je poruka poslana od legitimne organizacije ili osobe, iako to nije slučaj. Ova metoda je posebno opasna jer većina korisnika ne provjerava stvarnu adresu pošiljaoca, već samo prikazano ime („display name"), što omogućava napadaču da prevari korisnika bez potrebe za kompromitovanjem stvarnog računa.

Spoofing se često koristi u kombinaciji s drugim tehnikama, poput socijalnog inženjeringa, kako bi se postigao efekat hitnosti ili autoriteta – korisnik tako dobija poruku

[12] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ Pristupljeno 24.06.2025.
[13] https://blog.checkpoint.com/research/the-weaponization-of-pdfs-68-of-cyberattacks-begin-in-your-inbox-with-22-of-these-hiding-in-pdfs/ Pristupljeno 24.06.2025.

za koju misli da dolazi od banke, nadređenog ili tehničke podrške. Cilj može biti krađa pristupnih podataka, uvida u povjerljive informacije ili čak prevara putem zahtjeva za novčanom transakcijom (npr. lažni zahtjev za uplatu).

Ova metoda se koristi i u tzv. Business Email Compromise (BEC) napadima, gdje žrtve često izvršavaju finansijske transakcije vjerujući da postupaju po legitimnim instrukcijama.[14]

4.5. AUTOMATIZACIJA PHISHING KAMPANJA

Phishing napadi više nisu isključivo rezultat ručne aktivnosti pojedinaca. Danas se u velikoj mjeri koriste automatizovani alati koji omogućavaju masovno kreiranje i slanje e-mailova, uključujući personalizaciju poruka prema imenu, firmi, funkciji korisnika i drugim podacima dobijenim iz javnih izvora.

Ovi alati omogućavaju i sofisticirane funkcionalnosti poput rotacije IP adresa i domena kako bi se izbjegli sigurnosni filteri, kao i automatsko praćenje aktivnosti korisnika – ko je otvorio poruku, kliknuo na link ili skinuo prilog. U naprednijim napadima koristi se čak i tzv. phishing-as-a-service (PhaaS), gdje kriminalci unajmljuju alate i infrastrukturu za napade, bez da posjeduju tehničko znanje.[15]

4.6. UPOTREBA LEGITIMNIH SERVISA ZA OBMANU

Zabrinjavajući trend u razvoju phishing tehnika je korištenje legitimnih platformi za distribuciju malicioznih sadržaja. Napadači često koriste servise poput Google Forms, Microsoft Forms, Dropbox, WeTransfer i sličnih alata, jer njihovi domeni ne izazivaju sumnju kod sigurnosnih sistema ni kod krajnjih korisnika.

[14] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing Pristupljeno 24.06.2025.
[15] https://attack.mitre.org/techniques/T1566/001/ Pristupljeno 24.06.2025.

Korisnicima se šalju poruke sa linkom koji vodi, recimo, na Google Formu sa zahtjevom da unesu svoje korisničko ime i lozinku – pošto se domena docs.google.com smatra pouzdanom, većina korisnika ne primjećuje opasnost.[16]

4.7. MOBILNI PHISHING I NAPADI PUTEM APLIKACIJA

Mobilni uređaji postaju sve češća meta phishing napada zbog njihove sveprisutnosti i slabijih zaštitnih mehanizama u odnosu na desktop računare. Poruke koje stižu putem aplikacija poput WhatsAppa, Vibera, Instagrama, pa čak i klasičnih SMS poruka, sadrže linkove ili datoteke koje vode do phishing stranica.

Zbog manjeg ekrana i smanjenog prikaza URL adresa, korisnici teško primijete da su prevareni. Osim toga, mobilne aplikacije često ne prikazuju sigurnosne certifikate ili punu strukturu linka.[17]

4.8. PHISHING PUTEM QR KODOVA

Quishing je sve češći oblik phishing napada u kojem napadači koriste QR kodove kako bi žrtvu preusmjerili na lažne web stranice. Ovi kodovi se mogu naći u e-mailovima, na plakatima, u restoranima ili kao dio digitalnih faktura. Korisnik skenira kod vjerujući da vodi na sigurnu stranicu, ali umjesto toga dolazi do stranice za krađu lozinki ili instalaciju malvera.

Posebno su opasni jer korisnici ne vide odmah URL iza QR koda, pa češće nesvjesno unesu podatke. Napadači često koriste i legitimne domene (npr. bing.com, google.com) za preusmjeravanje, čime dodatno prikrivaju krajnju destinaciju.[18]

---

[16] https://www.welivesecurity.com/en/scams/how-fraudsters-abuse-google-forms-spread-scams/ Pristupljeno 25.06.2025.
[17] https://www.it.cuimc.columbia.edu/information-security/dont-get-hooked Pristupljeno 25.06.2025.
[18] https://cofense.com/blog/malicious-actors-utilizing-qr-codes-to-deploy-phishing-pages-to-mobile-devices/ Pristupljeno 25.06.2025.

5. PRIMJERI PHISHING NAPADA IZ PRAKSE

Iako phishing napadi na prvi pogled mogu djelovati kao bezazlene poruke u elektronskoj pošti, stvarni primjeri pokazuju da su posljedice često katastrofalne – finansijski gubici, krađa identiteta, narušavanje ugleda kompanija i kompromitacija državnih institucija. U ovom poglavlju predstavljeni su najznačajniji primjeri phishing napada koji ilustriraju raznovrsnost i sofisticiranost ove prijetnje, kako na međunarodnom, tako i na regionalnom nivou.

5.1. NAPAD NA GOOGLE I FACEBOOK (2013-2015)

Jedan od najpoznatijih phishing incidenata desio se između 2013. i 2015. godine, kada je jedan napadač iz Litvanije, Evaldas Rimasauskas, uspio prevariti Google i Facebook i ukrasti preko 100 miliona dolara.

Napadač je kreirao lažnu firmu sa sličnim imenom kao legitimni azijski proizvođač opreme, zatim slao lažne fakture i e-mailove finansijskim odjelima Googlea i Facebooka. Zbog profesionalno izvedenog spear phishinga, obje kompanije su bez sumnje vršile uplate na njegove račune.[19]

5.2. PHISHING KAMPANJE PROTIV GRAĐANA U BIH I REGIONU

U Bosni i Hercegovini i susjednim državama, phishing napadi na građane najčešće dolaze u obliku:

- SMS poruka od "BH Pošte", "Pošte Srbije", "Crnogorske pošte";
- e-mailova banaka s lažnim obavještenjima;

[19] https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html Pristupljeno 25.06.2025.

- lažnih nagradnih igara putem društvenih mreža.

"Vaš paket je stigao u skladište i ne može biti isporučen zbog nepotpune adrese. Molimo upotrijebite poveznicu u nastavku da potvrdite svoju adresu u roku od 12 sati" je samo primjer kakve poruke građani BiH redovno dobijaju.[20]

5.3. NAPAD NA AMERIČKU KOMPANIJU UBIQUITI (2021)

Kompanija Ubiquiti Networks, poznata po mrežnoj opremi, bila je meta velikog phishing napada 2021. godine. Prvobitno se smatralo da su hakeri izvana pristupili sistemima i pokušali iznuditi 50 miliona dolara prijeteći objavljivanjem osjetljivih podataka.

Međutim, kasnijom istragom otkriveno je da je napad iznutra organizovao bivši zaposlenik, koji je prvo stvorio lažni identitet napadača, a zatim iznutra omogućio pristup mreži. Ovo je bio kombinovani napad: korišteni su spear phishing, kompromitovani login podaci i interni pristup za ostvarivanje ucjene.[21]

5.4. COVID-19 I PHISHING PANEDMIJA

Tokom pandemije Covid-19, zabilježen je nagli porast phishing napada, jer su napadači koristili strah, nesigurnost i potrebu za informacijama da bi prevarili korisnike.

Širili su e-mailove s temama poput:

- "Besplatno testiranje" ili "prioritetno vakcinisanje",
- lažni PDF dokumenti sa "uputstvima WHO-a",

[20] https://www.bl-portal.com/drustvo/gradjani-bih-ponovo-na-meti-prevaranata-ukoliko-dobijete-ovakvu-sms-poruku-odmah-je-obrisite/ Pristupljeno 25.06.2025.
[21] https://www.cybereason.com/blog/whistleblower-accuses-ubiquiti-of-downplaying-major-data-breach Pristupljeno 25.06.2025.

- ponude državne pomoći koje zahtijevaju unos ličnih podataka.

Jedan od poznatijih primjera bila je lažna poruka u ime Svjetske zdravstvene organizacije (WHO) s linkom ka dokumentu koji je zapravo sadržavao maliciozni softver.[22]

5.5. RANSOMWARE PHISHING (NPR. WANNACRY)

WannaCry je ransomware napad koji je pogodio više od 230.000 računara u 150 zemalja, uključujući bolnice, državne agencije i privatne firme.

Iako je napad koristio tehničku ranjivost u Windows sistemima (EternalBlue), ulazna tačka su bili phishing e-mailovi sa privicima koji su korisnike navodili da otvore zaražene fajlove.

Jednom kada bi korisnik otvorio prilog, malver bi šifrirao sve podatke na računaru i tražio otkup u Bitcoinu. Napad je posebno pogodio NHS u Velikoj Britaniji, koji je morao otkazati stotine pregleda i operacija.[23]

[22] https://med.stanford.edu/news/insights/2022/01/research-explores-how-scammers-take-advantage-of-covid-19.html Pristupljeno 25.06.2025.
[23] https://www.england.nhs.uk/long-read/case-study-wannacry-attack/ Pristupljeno 25.06.2025.

6. POSLJEDICE PHISHING NAPADA

Phishing napadi, iako naizgled jednostavni, mogu imati dalekosežne i ozbiljne posljedice. One se ne mjere samo finansijskim gubicima, već uključuju i narušavanje privatnosti, povredu ugleda, pravne komplikacije i smanjenje povjerenja u digitalne servise. Ove posljedice mogu se osjetiti na individualnom, organizacionom, pa čak i državnom nivou.

6.1. FINANCIJSKI GUBICI

Najvidljivija i najčešće prijavljena posljedica phishing napada su direktni finansijski gubici. Kada korisnik nehotice otkrije podatke o svojoj kreditnoj kartici, pristupne podatke za e-bankarstvo ili autorizuje lažnu uplatu, napadači vrlo brzo izvuku novac.

Posljedice po pojedinca:

- gubitak novca sa ličnog računa,
- nemogućnost refundacije ukoliko se prevara ne prijavi na vrijeme,
- blokiranje računa, troškovi otvaranja novih.

Posljedice po kompanije:

- višemilionske krađe putem lažnih faktura (BEC napadi),
- troškovi obnavljanja sistema, interne istrage, angažovanja pravnih i IT stručnjaka,
- pad prihoda zbog gubitka reputacije i klijenata.

Statistički podatak:

Prema izvještaju FBI-ja iz 2023. godine, phishing je odgovoran za više od 3,3 milijarde dolara prijavljene štete samo u SAD-u.[24]

[24] https://dmarcian.com/2024-fbi-internet-crime-report-record-losses/ Pristupljeno 27.06.2025.

6.2. KRAĐA IDENTITETA

Phishing napadi često služe kao sredstvo za krađu identiteta – napadači prikupljaju lične podatke korisnika (ime, prezime, JMBG, broj pasoša, adrese, podatke s lične karte) kako bi ih zloupotrijebili:

- otvaranjem računa u banci na ime žrtve,
- zaduživanjem putem lažnih kredita,
- preprodajom podataka na crnom tržištu (Dark Web).

Posljedice:

- pravne komplikacije za žrtvu,
- višemjesečni postupci dokazivanja da nije odgovorna za prevaru,
- narušavanje privatnosti i osjećaj nesigurnosti.[25]

6.3. UGROŽAVANJE POSLOVNE I DRŽAVNE SIGURNOSTI

U kontekstu organizacija, posebno onih koje posluju s osjetljivim podacima (zdravstvo, vojska, vlada, banke), phishing napad može dovesti do:

- gubitka povjerljivih dokumenata, poslovnih planova i patenata,
- kompromitovanja državnih ili vojnih sistema,
- otkrivanja osobnih podataka hiljada ili miliona korisnika.

Takve posljedice imaju domino-efekt i mogu uzrokovati:

- međunarodne sporove,
- tužbe i odštetne zahtjeve,

[25] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime Pristupljeno 27.06.2025.

- povlačenje investitora ili partnera.[26]

6.4. GUBITAK UGLEDA I POVJERENJA KORISNIKA

Kada korisnici saznaju da je neka kompanija bila meta phishing napada – pogotovo ako su njihovi podaci kompromitovani – povjerenje u tu instituciju značajno opada.

Kompanije koje ne obezbijede adekvatnu zaštitu:

- gube postojeće klijente,
- otežano stiču nove,
- trpe reputacijsku štetu koju je teško ispraviti i godinama nakon incidenta.

U digitalnom dobu, reputacija je često važnija od same štete – jer korisnici biraju usluge koje percipiraju kao sigurne.[27]

6.5. PRAVNE I REGULATORNE POSLJEDICE

Organizacije koje su pogođene phishing napadima često imaju zakonsku obavezu da:

- prijave incident odgovarajućim institucijama (CERT, policija, regulatorna tijela),
- obavijeste korisnike čiji su podaci ugroženi,
- provedu unutrašnju reviziju i nadoknade štetu ako su bili nemarni.

U Evropskoj uniji, prema Općoj uredbi o zaštiti podataka (GDPR), firme mogu biti kažnjene do 20 miliona eura ili 4% godišnjeg prometa ako nisu osigurale adekvatnu zaštitu ličnih podataka.[28]

[26] https://dmarcian.com/2024-fbi-internet-crime-report-record-losses/ Pristupljeno 27.06.2025.
[27] https://www.verywellmind.com/how-to-cope-with-getting-scammed-8697566 Pristupljeno 27.06.2025.
[28] https://dmarcian.com/2024-fbi-internet-crime-report-record-losses/ Pristupljeno 27.06.2025.

6.6. PSIHOLOŠKE POSLJEDICE ZA ŽRTVE

Phishing napadi, osim što nanose materijalnu štetu, ostavljaju i emocionalne posljedice.

Pojedinci koji su prevareni često osjećaju:

- sram, krivicu, nesigurnost,
- gubitak povjerenja u digitalne tehnologije,
- strah od ponovnog korištenja internetskih servisa.

Posebno su pogođene starije osobe i one koje nisu digitalno pismene, jer im je teže prepoznati prijevaru i nositi se s njenim posljedicama.[29]

[29] https://www.cygenta.co.uk/post/psychological-impact-phishing Pristupljeno 27.06.2025.

7. ZAŠTITA OD PHISHING NAPADA

Iako phishing napadi postaju sve sofisticiraniji, zaštita od njih je moguća kombinovanjem tehničkih rješenja, edukacije korisnika i organizacionih politika sigurnosti.

7.1. TEHNIČKE MJERE ZAŠTITE

a) Antivirusni i anti-phishing softver

Moderni antivirusni programi sadrže ugrađene module za detekciju phishing sadržaja, koji analiziraju e-mailove, linkove i priloge prije nego što korisnik stupi u kontakt s njima.

- Preporučuje se redovno ažuriranje antivirusnog softvera i aktivacija zaštite u realnom vremenu.
- Postoji i specijalizovani anti-phishing alati i proširenja za pretraživače koji analiziraju URL adrese i obavještavaju korisnika o sumnjivim stranicama.[30]

b) Filtar za e-mail (spam filteri)

E-mail sistemi (Gmail, Outlook, Yahoo i dr.) koriste složene algoritme za prepoznavanje i filtriranje sumnjivih poruka. Uvođenjem SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) i DMARC protokola značajno se smanjuje mogućnost spoofinga. Organizacije trebaju implementirati ove protokole u svojoj e-mail infrastrukturi. Korisnici trebaju provjeravati zaglavlja poruka i izbjegavati e-mailove iz „Unknown sender“ izvora.[31]

[30] https://www.memcyco.com/anti-phishing-tools-for-2025/ Pristupljeno 27.06.2025.
[31] https://www.mimecast.com/content/dkim-spf-dmarc-explained/ Pristupljeno 27.06.2025.

c) Višefaktorska autentifikacija (MFA/2FA)

Višefaktorska autentifikacija zahtijeva od korisnika da se, osim lozinke, identifikuje pomoću dodatnog faktora:

- SMS kod,
- aplikacija za verifikaciju (npr. Google Authenticator),
- biometrija (otisak prsta, prepoznavanje lica).

Iako MFA nije 100% sigurna, značajno otežava napadaču pristup čak i ako posjeduje lozinku.[32]

d) Redovno ažuriranje softvera i sistema

Zastarjeli softver često sadrži sigurnosne propuste koje napadači mogu iskoristiti. Zato je neophodno:

- ažurirati operativni sistem,
- koristiti posljednje verzije pretraživača,
- izbjegavati piratske aplikacije.[33]

7.2. EDUKACIJA KORISNIKA I DIGITALNA PISMENOST

Jedna od najsnažnijih zaštita protiv phishinga jeste svijest korisnika. Edukacija o prepoznavanju znakova phishing napada može drastično smanjiti broj žrtava.

Ključne edukativne poruke:

- Ne otvaraj e-mailove i priloge od nepoznatih pošiljalaca.

[32] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MFA-Microsoft-Research-Paper-update.pdf?country=ca&culture=en-ca Pristupljeno 27.06.2025.
[33] https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/ Pristupljeno 27.06.2025.

- Ne ulazi na linkove u porukama koji traže unos ličnih podataka.
- Provjeri URL adresu stranice prije unosa lozinke (https, pravopis, domena).
- Nikada ne šalji lozinke putem e-maila.
- Ne vjeruj porukama koje zahtijevaju hitnu akciju („račun će biti blokiran“, „posljednja opomena“).

Posebno je važno edukovati starije korisnike, djecu i one koji tek stiču digitalne vještine.[34]

7.3. ORGANIZACIONE SIGURNOSNE POLITIKE

Organizacije moraju imati jasno definisane sigurnosne protokole i procedure, uključujući:

- Trening zaposlenika – Redovne edukacije i simulacije phishing napada mogu pripremiti osoblje da bolje prepoznaju sumnjive poruke.
- Pravila pristupa i ovlasti – Ne dozvoljavati svim zaposlenima pristup svim podacima – ograničiti pristup na osnovu uloge u firmi (princip najmanje privilegije).
- Incident response plan – U slučaju da phishing napad uspije, potrebno je imati plan reakcije: izolacija sistema, reset lozinki, obavještavanje nadležnih organa, informisanje korisnika.
- Redovan backup – Sigurnosne kopije podataka treba praviti redovno i čuvati ih na lokacijama nedostupnim mrežnim napadima. To omogućava oporavak u slučaju ransomware napada.[35]

[34] https://www.knowbe4.com/press/knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86 Pristupljeno 27.06.2025.
[35] https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy Pristupljeno 27.06.2025.

7.4. PRAVNA I INSTITUCIONALNA ZAŠTITA

U većini država postoji zakonski okvir koji tretira elektronski kriminal i pokušaje krađe identiteta. U BiH i zemljama regiona djeluju institucije poput:

- CERT BiH – Centar za odgovore na računarske incidente,
- Agencija za zaštitu ličnih podataka BiH,
- MUP i odjeli za visokotehnološki kriminal.

Građani i firme treba da prijave svaki pokušaj phishinga kako bi se omogućilo šire upozorenje javnosti i potencijalno otkrivanje počinilaca.[36]

7.5. ULOGA KORISNIKA U PREVENCIJI

Na kraju, najvažniji „firewall“ nije tehnički – već ljudski. Korisnici su posljednja linija odbrane, i zato se moraju ponašati odgovorno:

- Redovno mijenjaj lozinke.
- Ne koristi iste lozinke za više servisa.
- Ne odgovaraj na sumnjive poruke, čak ni iz znatiželje.
- Prijavi svaki sumnjivi e-mail ili poruku IT odjelu ili nadležnima.[37]

[36] https://www.nixonpeabody.com/insights/articles/2021/08/27/new-cisa-guidance-provides-practical-tips-for-preventing-and-responding-to-ransomware-attacks Pristupljeno 27.06.2025.
[37] https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof Pristupljeno 27.06.2025.

8. TRENDOVI I BUDUĆNOST PHISHING NAPADA

Phishing napadi se ne smanjuju – naprotiv, postaju sve sofisticiraniji zahvaljujući napretku tehnologije i vještačke inteligencije. Umjesto tradicionalnih generičkih e-mailova, napadi su sada personalizovani, bazirani na prethodnom ponašanju korisnika, te često automatizovani uz pomoć AI alata. Napadači koriste generativne modele da kreiraju uvjerljive poruke koje oponašaju stil pisanja poznatih osoba, čime značajno povećavaju uspješnost napada. Tehnologije poput deepfake videa i sintetizovanog glasa omogućavaju stvaranje uvjerljivih lažnih poziva i poruka koje izgledaju kao da dolaze od nadređenih, banaka ili članova porodice, što dodatno zbunjuje korisnike.

Također, razvoj interneta stvari (IoT), pametnih uređaja i virtualnih okruženja kao što je metaverzum otvara nove prostore za phishing – od lažnih avatara do manipulacije glasovnim komandama i QR kodovima. Mobilni uređaji postaju primarna meta, jer napadači koriste notifikacije, push poruke i aplikacije za prenošenje lažnih poruka koje korisnici teže prepoznaju zbog malih ekrana i ograničenog prikaza linkova.

Opasnost dodatno raste jer je danas phishing dostupan i kao usluga (Phishing-as-a-Service – PhaaS), što znači da čak i tehnički neobučen pojedinac može kupiti kompletne alate za napad putem dark weba. To uključuje gotove skripte, hosting za lažne stranice, baze e-mailova i čak AI-generisane poruke.

S druge strane, i obrambene mjere napreduju. Razvijaju se adaptivne strategije zasnovane na vještačkoj inteligenciji, biometrijskoj autentifikaciji bez lozinki, real-time analizama i Zero Trust modelima sigurnosti. Organizacije ulažu u sigurnosne edukacije i simulacije napada kako bi pripremile korisnike na savremene prijetnje.

U budućnosti, borba protiv phishinga neće se oslanjati samo na tehnologiju, već i na jačanje zakonodavstva, međunarodnu saradnju i kontinuiranu edukaciju korisnika, jer je ljudski faktor i dalje ključna linija odbrane u digitalnom prostoru.

9. ZAKLJUČAK

Phishing napadi predstavljaju jednu od najrasprostranjenijih i najopasnijih prijetnji savremenom digitalnom društvu. Ovaj oblik sajber kriminala temelji se na manipulaciji i obmani korisnika s ciljem krađe povjerljivih informacija, finansijske dobiti ili kompromitacije digitalnih sistema. Kroz rad smo analizirali ne samo osnovne pojmove, vrste i tehnike phishing napada, već i njihove posljedice, zakonske aspekte i načine zaštite, uz poseban osvrt na aktuelne trendove i budućnost ovog vida prijetnji.

Kroz pregled historije phishinga uočava se da se, iako su prve forme bile jednostavne i masovne, današnji napadi sve više oslanjaju na sofisticirane metode – posebno zahvaljujući razvoju vještačke inteligencije, automatizacije i tehnologije imitacije identiteta (deepfake). Napadi postaju personalizovaniji, brži i teže otkrivi, što dodatno komplikuje zaštitu korisnika i organizacija.

Vrste phishinga, od klasičnih e-mail poruka do SMS poruka, glasovnih napada (vishing), QR phishinga i spear phishinga, pokazuju raznolikost metoda i dokazuju da niti jedna platforma više nije sigurna bez proaktivne zaštite. Primjeri iz prakse, uključujući slučajeve velikih tehnoloških kompanija, regionalnih privrednih subjekata i običnih građana, potvrđuju da phishing ne bira metu – svi su potencijalne žrtve.

Posljedice phishing napada nisu ograničene na finansijski gubitak. One uključuju krađu identiteta, narušavanje reputacije, pravne posljedice, gubitak povjerenja korisnika i psihološke traume žrtava. Na organizacionom nivou, posljedice se mogu proširiti na poslovnu sigurnost, zakonske sankcije i dugoročnu štetu po kredibilitet.

Uprkos ozbiljnosti problema, phishing se može ublažiti odgovarajućim mjerama zaštite. Tehnička rješenja, poput antivirusnih sistema, više faktorske autentifikacije, naprednih filtera i sigurnosnih politika, pružaju prvu liniju odbrane. Međutim, ključni faktor ostaje edukacija korisnika – njihova sposobnost da prepoznaju prijetnje i odgovorno postupaju u digitalnom prostoru. Uz to, važna je i zakonska regulativa, koja mora pratiti tempo tehnološkog razvoja i obezbijediti efikasnu zaštitu i procesuiranje počinilaca.

Gledajući u budućnost, phishing napadi će se nesumnjivo prilagoditi novim digitalnim okruženjima – metaverzumu, IoT uređajima, AI komunikaciji i mobilnim aplikacijama. Zbog toga je važno da borba protiv phishinga ne bude statična, već dinamična, proaktivna i zasnovana na saradnji između korisnika, institucija i država.

Zaključno, borba protiv phishing napada zahtijeva sinergiju znanja, tehnologije, zakonodavstva i svijesti. Samo cjelovit pristup može osigurati sigurnu budućnost u sve digitalizovanijem svijetu.

Ovaj rad predstavlja teorijske osnove iz phishing napada. Hipoteze postavljene na samom početku su dokazane i potvrđene.

10. LITERATURA

Internet izvori:

1. https://attack.mitre.org/techniques/T1566/001/ Pristupljeno 24.06.2025.
2. https://blog.checkpoint.com/research/the-weaponization-of-pdfs-68-of-cyberattacks-begin-in-your-inbox-with-22-of-these-hiding-in-pdfs/ Pristupljeno 24.06.2025.
3. https://www.bl-portal.com/drustvo/gradjani-bih-ponovo-na-meti-prevaranata-ukoliko-dobijete-ovakvu-sms-poruku-odmah-je-obrisite/ Pristupljeno 25.06.2025.
4. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MFA-Microsoft-Research-Paper-update.pdf?country=ca&culture=en-ca Pristupljeno 27.06.2025.
5. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ Pristupljeno 24.06.2025.
6. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html Pristupljeno 25.06.2025.
7. https://cofense.com/blog/malicious-actors-utilizing-qr-codes-to-deploy-phishing-pages-to-mobile-devices/ Pristupljeno 25.06.2025.
8. https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/whaling-attack/ Pristupljeno 24.05.2025.
9. https://www.cybereason.com/blog/whistleblower-accuses-ubiquiti-of-downplaying-major-data-breach Pristupljeno 25.06.2025.
10. https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof Pristupljeno 27.06.2025.
11. https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/ Pristupljeno 27.06.2025.
12. https://www.cygenta.co.uk/post/psychological-impact-phishing Pristupljeno 27.06.2025.
13. https://dmarcian.com/2024-fbi-internet-crime-report-record-losses/ Pristupljeno 27.06.2025.

14. https://encyclopedia.kaspersky.com/glossary/phishing/ Pristupljeno 23.06.2025.
15. https://www.england.nhs.uk/long-read/case-study-wannacry-attack/ Pristupljeno 25.06.2025.
16. https://www.experian.com/blogs/ask-experian/what-is-angler-phishing-and-how-can-you-avoid-it/ Pristupljeno 24.06.2025.
17. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing Pristupljeno 24.06.2025.
18. https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy Pristupljeno 27.06.2025.
19. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full Pristupljeno 23.06.2025.
20. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime Pristupljeno 27.06.2025.
21. https://www.imperva.com/learn/application-security/social-engineering-attack/ Pristupljeno 24.06.2025.
22. https://www.it.cuimc.columbia.edu/information-security/dont-get-hooked Pristupljeno 25.06.2025.
23. https://www.kaspersky.com/resource-center/definitions/spear-phishing Pristupljeno 24.06.2025.
24. https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it Pristupljeno 24.06.2025.
25. https://www.knowbe4.com/press/knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86 Pristupljeno 27.06.2025.
26. https://med.stanford.edu/news/insights/2022/01/research-explores-how-scammers-take-advantage-of-covid-19.html Pristupljeno 25.06.2025.
27. https://www.memcyco.com/anti-phishing-tools-for-2025/ Pristupljeno 27.06.2025.
28. https://www.mimecast.com/content/dkim-spf-dmarc-explained/ Pristupljeno 27.06.2025.
29. https://www.nixonpeabody.com/insights/articles/2021/08/27/new-cisa-guidance-provides-practical-tips-for-preventing-and-responding-to-ransomware-attacks Pristupljeno 27.06.2025.

30. https://www.phishing.org/history-of-phishing Pristupljeno 23.06.2025.
31. https://www.proofpoint.com/us/blog/security-awareness-training/vishing-attacks-whos-really-line Pristupljeno 24.06.2025.
32. https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm Pristupljeno 24.06.2025.
33. https://www.verywellmind.com/how-to-cope-with-getting-scammed-8697566 Pristupljeno 27.06.2025.
34. https://www.welivesecurity.com/en/scams/how-fraudsters-abuse-google-forms-spread-scams/ Pristupljeno 25.06.2025.