# ISTRAŽIVANJE O PREPOZNAVANJU E-MAIL PHISHINGA U POSLOVNIM ORGANIZACIJAMA

**Zvonarić, Alida Dina**

**VELEUČILIŠTE U RIJECI**

Alida Dina Zvonarić

# ISTRAŽIVANJE O PREPOZNAVANJU E-MAIL *PHISHINGA* U POSLOVNIM ORGANIZACIJAMA

specijalistički završni rad

Rijeka, 2022.

# VELEUČILIŠTE U RIJECI

Odjel sigurnosti na radu

Specijalistički diplomski stručni studij Sigurnost na radu


# ISTRAŽIVANJE O PREPOZNAVANJU E-MAIL *PHISHINGA* U POSLOVNIM ORGANIZACIJAMA

specijalistički završni rad


MENTOR

dr. sc. Bernard Vukelić, prof. v. š.

STUDENT

Alida Dina Zvonarić

MBS: 2426000091/20



Rijeka, 2022.

## Sažetak

*Phishing* je oblik socijalnog inženjeringa i kibernetičkog kriminala koji podrazumijeva krađu povjerljivih podataka (osobnih ili službenih) za ostvarivanje financijske koristi. To je jedan od najstarijih *cyber* prijetnji. Postoji široka paleta tehnika *phishing* napada, od kojih je većinom zastupljena ona koja se izvodi putem elektroničke pošte. Kada se otvaraju zlonamjerni privitci i poveznice ili šalje odgovor na poruku, postaju se žrtvom takve. Zaposlenici koji nemaju razvijenu svijest o *phishing* napadima, odgovornost te ne posjeduju znanje predstavlja potencijalnu opasnost za cjelokupno poslovanje organizacije. U ovom završnom radu opisano je istraživanje o prepoznavanju e-mail *phishinga* u poslovnim organizacijama na području Primorsko-goranske županije. Provedeno istraživanje pokazalo je da zaposlenici ne poznaju *phishing* napade u dovoljnoj mjeri, a ni sve navike koje pridonose nivou informatičke sigurnosti glede tih napada nisu zadovoljavajuće. Prilikom istraživanja koristile su se sljedeće znanstvene metode: metode indukcije i dedukcije, metoda sustavne analize i sinteze, apstrakcije i konkretizacije, generalizacije i specijalizacije te deskriptivna metoda. Za zaštitu od takvih napada organizacije trebaju, uz provođenja sigurnosnih tehničkih mjera, aktivno educirati djelatnike te povremeno provoditi testiranja.



**Ključne riječi: *phishing*, prepoznavanje, metoda, zaštita.**

## Sadržaj

# 1. Uvod

Svake godine bilježi se izniman porast *phishing* kampanja usmjeren na male i velike korporacije kako u svijetu tako i u Republici Hrvatskoj. Ovaj način napada i mediji preko kojih se isti odvija kroz godine se modificirao i napredovao. Ono što je od njegovog nastanka pa do danas ostalo nepromijenjeno su činjenice da od svih *cyber* aktivnosti je najzastupljeniji te da može uzrokovati ogromne i razne štete poslovnim organizacijama.

Za zaštitu od *phishing* napada poslovne organizacije moraju provesti niz tehničkih mjera. Međutim, usprkos provedenim tehničkim mjerama, vrlo često se događa da krivotvoreni mail dospije do zaposlenika te tada daljnje poslovanje organizacije ovisi o postupcima koje će on učiniti glede toga. Stoga je ključ zaštite od *phishing* napada praktično i teorijsko znanje zaposlenika. Osobito u današnje vrijeme kada su takvi napadi sve sofisticiraniji i učestaliji, a samo jedan pogrešan klik, odnosno nepažnja i/ili neznanje može ugroziti poslovanje cijele organizacije. U skladu s time, ovim radom istražuje se u kojoj mjeri radnici koji obavljaju uredske poslove prepoznaju *phishing* prijevare na području Primorsko-goranske županije.

Glavni cilj ovog rada je ispitati koliko su zaposlenici koji svakodnevno koriste računalno upoznati s *phishing* prijevarama koje se odvijaju putem elektroničke pošte, odnosno percipiraju li znakove koji upućuju na takve prijevare kada vide neke od autoritativnih pokazatelja, poznaju li obilježja koja upućuju na takve prijevare te jesu li njihove navike u skladu s mjerama za sprječavanje istih.

Svrha rada je ukazati na važnost kontinuiranog provođenja edukacije i povremenog testiranja zaposlenika u području *phishing* napada kako bi poslovne organizacije spriječile da oni postanu žrtve, a time i spriječili nepoželjni ishodi poslovanja.

Istraživanjem o prepoznavanju e-mail *phishinga* u poslovnim organizacijama postavljaju se sljedeća istraživačka pitanja:

- zaposlenici koji su odslušali predavanje o *phishing* prijevarama bolje prepoznaju *phishing* prijevare i imaju poželjnije navike,
- informatički obrazovani ljudi bolje prepoznaju *phishing* prijevare i imaju poželjnije navike.

U ovom radu koristile su se razne znanstvene metode. Radi izdvajanja bitnih svojstava odnosa i veza te uočavanja određenih između objekata istraživanja koristile su se metode indukcije i dedukcije, metoda sustavne analize i sinteze, apstrakcije i konkretizacije, generalizacije i specijalizacije te deskriptivna metoda. Rad se temelji na primarnim izvorima podataka.

U prvom dijelu rada elaboriraju se teorijska obilježja *phishing* napada i metode takvih napada. Također opisuju se osobne karakteristike ljudi koji su podložni krađi identiteta te povijest *phishinga*. Zatim se prikazuje statistika svih računalno sigurnosnih incidenata za 2021. godinu u kao i *phishing* kampanje u vremenskom razdoblju od 2017. do 2022. godine u Republici Hrvatskoj. Uz to govori se o posljedicama *phishing* napada koji je izvršen na poslovne organizacije. U drugom dijelu rada opisuje se provedeno istraživanje o prepoznavanju e-mail *phishinga* u poslovnim organizacijama na području Primorsko-goranske županije i dobiveni rezultati. Nakon toga se navode metode zaštite poslovnih organizacije od takvih napada i daje zaključak.

# 2. *Phishing*

*Phishing* je vrsta socijalnog inženjeringa, odnosno napad u kojem vršitelj manipulira ljudima kako bi došao do povjerljivih informacija, poput podataka o: kreditnoj kartici, telefonskom broju, poštanskoj adresi, tvrtki i slično (CyberSecurity & Infrastructure Security Agency, 2020.; Terranova Security by HelpSystems, n.d.). Taj podatak mu služi za preuzimanje žrtvina identiteta i počinjenja daljnjih kaznenih djela, odnosno izvlačenje financijskih sredstava (Terranova Security by HelpSystems, n.d.; CERT.hr, n.d.). To je jedan od najjeftinijih i najjednostavnijih kibernetičkih napada (IT Governance, n.d.).

Prema Certu *phishing* je „vrsta socijalnog inženjeringa koja se odnosi na prijevare, kojima se služe zlonamjerni korisnici šaljući lažne poruke koristeći pritom postojeće internet servise“ (CERT.hr, n.d.)

## 2.1. Metode *phishinga*

Kriminalci su razvili široku paletu tehnika koju koriste kao *phishing* napad za prikupljanje željenih informacija. Tehnike napada se prema složenosti prepoznavanja mogu svrstati u dvije skupine (Petrić, 2021.). U prvu skupinu spadaju *phishing* putem e-maila, *spear phishing* ili „lov kopljem“, *vishing*, *smishing* i *angler phishing* koja je sugestibilna, dok u drugu *pharming* (manipulacija prometom *web*-stranica), *phishing* korištenjem *pop-up* prozora (zlonamjerni kod smješten u obavijestima koje se pojavljuju prilikom posjeta *web*-stranici), *phishing* kloniranjem (simuliranje e-maila koji je poslan od strane legitimnih izvora), „zli blizanac“ *phishing* (korištenje lažne *Wifi hotspot), phishing* napad *„watering hole*“ (inficiranje jedinstvene internetske adrese ili engl. *Internet Protocol address* malicioznim kodovima ili preuzimanjima nekih sadržaja) koja je

visoko sofisticirana pa ju je skoro nemoguće uočiti (Petrić, 2021.; Kaspersky, n.d.; Oxford Web Studio, n.d.).

### 2.1.1. *Phishing* putem e-pošte

*Phishing* napad se najčešće izvodi putem e-pošte u kojem navode primatelja da prati upute oponašajući autoritativne organizacije pritom koristeći isti dizajn i logo kao i stvarna organizacija. (Cisco, 2022.; CERTNZ, n.d.). Kriminalci se najčešće predstavljaju da su iz: banaka, stranica društvenih medija, državnih agencija i dobrotvornih organizacija (CERTNZ, n.d.; CyberSecurity & Infrastructure Security Agency, 2020.). Najpopularnije marke koje koriste u svojim napadima su: PayPal (22%), Microsoft (19%), Facebook (15%), eBay (6%), Amazon (3%) (Fruhlinger, 2022.).

Hakeri većinom iskorištavaju trenutna zbivanja u svijetu kako bi zadobili povjerenje pošiljatelja, primjerice prirodne katastrofe (Uragan Katrina), epidemiju (COVID-19) i slično (CyberSecurity & Infrastructure Security Agency, 2020.). Slanjem e-maila kradu osobne podatke tražeći je da odgovori na dobivenu poruku, navodeći je na poveznicu koja je vodi na lažnu *web*-stranicu. Prvom varijantom osoba ispunjava tražene podatke na takvoj stranici, a drugom dolazi do ugradnje zlonamjernog virusa kao i kod otvaranja datoteka (Check Point, n.d.).

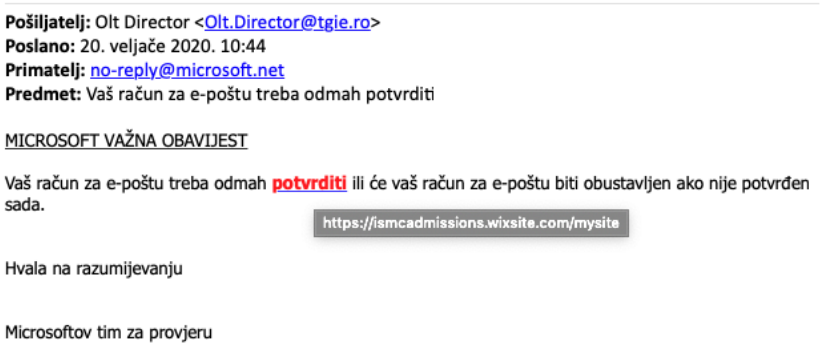
U svim prethodno navedenim varijantama e-*phishinga* osobi se nameće urgentna situacija koja zahtijeva njegovu neodloživu akciju. Primjerice ukoliko ona ne odgovori na mail sa svojim osobnim podatcima i adresom stanovanja zatvorit će joj se račun. Vršenjem pritiska korisnik je pod stresom te je skloniji pogrešci i slabijem rasuđivanju (Imperva, n.d.). Legitimne organizacije uglavnom daju dovoljno vremena korisniku da reagira prije nego mu neko pravo bude ukinuto.

Osim stavljanja korisnika u ozbiljnu situaciju, osjećaj hitnosti zna se primjenjivati u kombinaciji s pričom predobro da bi bilo istinito, koji je također jedan od pokazatelja phishing napada. Primatelju se nudi super ponuda uz ograničeno vrijeme trajanja tvrdeći da je osvojio mobitel, lutriju i slične nagrade (Phishing.org, n.d.).

#### 2.1.1.1. Lažni mail

U nastavku se prikazuje lažni mail slikom pod brojem 1 kojim se korisnika navodi da putem poveznice potvrdi račun e-pošte, u suprotnom će mu isteći račun i to odmah.

Slika 1. Primjer lažnog maila




Izvor: Šokić, T., 2021.

Primjećuju se sljedeći znakovi koji upućuju na pokušaj krađe identiteta:

1. pošiljatelj je nepoznat,
2. adresa pošiljatelja se ne poklapa s kontekstom maila,
3. u naslovu i u tekstu maila navodi se da je traženu radnju potrebno odmah učiniti,

4. *web*-mjesto na koje se upućuje ne podudara se s domenom pošiljatelja (dio adrese iza simbola @), a ni sa sadržajem maila kada se pređe mišem preko poveznice (Šokić, 2021.).

Klikom na poveznicu može doći do ugradnje zlonamjernog virusa ili preusmjeravanja na lažnu *web*-stranicu za prikupljanje osobnih podataka (Proofpoint, n.d. ).

#### 2.1.1.2. Lažna *web*-stranica

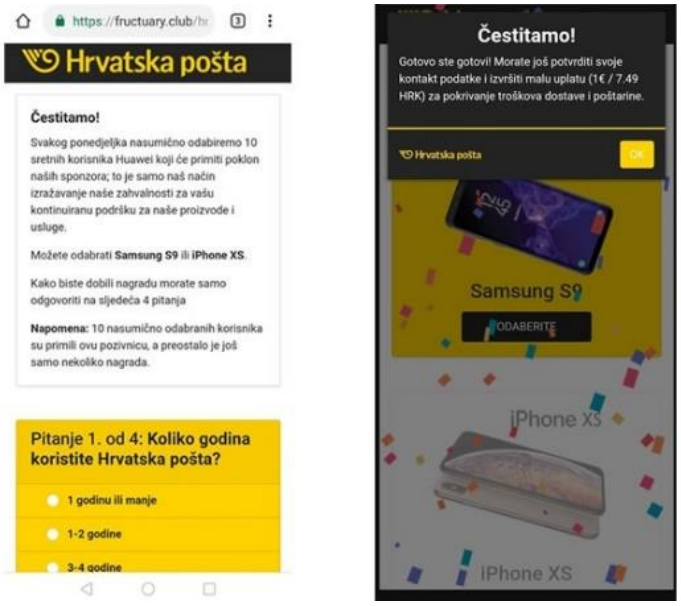
Veze unutar e-poruka koje preusmjeravaju korisnika na *web*-stranice nalikuju legitimnim organizacijama, a prepoznaju po pogrešnoj napisanoj domeni ili poddomeni. Na priloženoj slici 2. može se vidjeti razlika između stvarnog i lažne adrese ili *Uniform Resource Locator* (u daljnjem tekstu; URL) (Imperva, n.d.).

Slika 2. Primjer lažnog URL-a


Izvor: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (18. 6. 2022.)

Primjer lažne *web*-stranice koja koristi isti logo kao i stvarna organizacija prikazan je slikom pod brojem 3. Pokazatelji pokušaja krađe identiteta su lažan URL i predobro da bi bilo istinito.

Slika 3. Primjer lažne *web*-stranice




Izvor: https://www.posta.hr/lazne-poruke-na-drustvenim-mrezama/7795 (18. 6. 2022.)

### 2.1.2. *Spear phishing* ili „lov kopljem“

Za razliku od *phishing* napada putem e-maila, *spear phishingom* ili „lovom kopljem“ ciljaju se osobe unutar određene organizacije, a ne široka masa ljudi pretvarajući se da mail dolazi od druge osobe iz te organizacije (Cisco, 2022.). *Cyber* kriminalci prvotno pomoću „slobodnog softvera“ ili engl. *open source* izvora (Firefox, Chrome, OpenOffice, Linux i Android) prikupljaju informacije kao što su ime, mjesto rada, naziv radnog mjesta, e-mail adresa, konkretne informacije o njihovoj ulozi u poslu, kolegama i članovima obitelji iz objavljenih ili javno dostupnih izvora, odnosno putem društvenih mreža ili *web*-stranica tvrtke (Petrić, 2021.; If-Koubou, n.d.). Ovaj tip prijevare koji ima visoku autentičnost daje uspješnost čak i u 95% slučajeva (Cisco, 2022.). Široka je lepeza scenarija napada, a najgori su oni koji uključuju izvršne direktore kao pošiljatelja ili primatelja. Drugim riječima, u prvom slučaju radi se o napadima u kojima se osobe predstavljaju da su izvršni direktori, dok u drugom o napadima namijenjenim izvršnim direktorima korporacija.

S obzirom na to razlikujemo dva oblika *spear phishinga*. Prvi oblik zove se *BEC* prijevare (engl. *business e-mail compromise*), a drugi *whaling*, „lov na kitove“ ili *CEO* prijevare (IT Governance, n.d.).

### 2.1.3. Vishing

*Voice phishing* ili *vishing* je krađa osobnih podataka putem internetske telefonske usluge (engl. *Voice over IP* ili *VoIP*) te postoji od njenog nastanka (FraudWatch, 2019.; Stone, 2022.). Napadači na razne načine pokušavaju prevariti ljude da otkriju tražene podatke. Predstavljaju se da su iz vlade, poreznog odijela, policije ili banaka žrtve pritom koristeći lažne profile identifikacije pozivatelja ili ID pozivatelja (engl. *Calling Line Identification* ili *CLI*) kako bi njihov poziv u potpunosti izgledao vjerodostojnim (Terranova Security by HelpSystems, n.d.; FraudWatch, 2019.; Unuth, n.d.). U kombinaciji s uvjerljivom pričom i zastrašivanjem, žrtve se osjećaju kao da nemaju drugu mogućnost nego dati zahtijevane informacije (Terranova Security by HelpSystems, n.d.). Primjerice napadač se pretvara da je istražitelj prijevara za tvrtku kreditnih kartica ili banku obavještavajući žrtvu da je njihov račun hakiran te ju moli da mu kaže podatke o bankovnoj kartici za navodno potvrđivanje identiteta ili prebacivanje novca na sigurno mjesto (Check Point, n.d.). Događa se da ukoliko se osoba ne javi na telefonski poziv, dobije glasovnu poruku koja primatelja mami da poduzme hitnu reakciju, odnosno da nazove na ostavljeni broj i ostavi „potrebne“ podatke (FraudWatch, 2019.; Terranova Security by HelpSystems, n.d.).

### 2.1.4. *Smishing*

*SMS phishing* ili *smishing* je krađa osobnih podataka putem SMS-a ili tekstualnih poruka. Ljudi nisu svjesni da se *phishing* prijevare mogu odvijati i pomoću tekstualnih poruka i da je kriminalcima na taj način lakše pristupiti korisniku (Trend Micro, n.d.).

### 2.1.5. *Angler phishing*

Naziv *Angler phishing* dolazi od lika iz filma *Finding Nemo* (hrv. Potraga za Nemom) u kojemu riba po imenu *Anglerfish* upotrebljava odličan mamac pomoću kojeg privlači plijen i proždire ga. Za *angler phishing* kriminalci koriste društvene mreže preko kojih obično ciljaju nezadovoljne kupce. Nakon što se kupac požali nekoj kompaniji na društvenoj mreži, napadaču putem sustava upozorenja stiže obavijest o tome te on stupa u kontakt s tom osobom putem lažnog računa koji nalikuje službenom korisničkom računu tvrtke na društvenim mrežama. Najčešće se radi o računima tvrtki: BMW, Amazon, Starbucks, Sony i Samsung (Murillo, 2019.).

## 2.2. Osobne karakteristike koje ljude čine podložnijima *phishing* napadima

Razne studije proučavale su koji čimbenici utječu na podložnost *phishing* napada i razlog zašto se ljudi „upecaju“. Jednim od čimbenika koji najviše utječe na proces krađe identiteta smatra se ljudska priroda zbog čega svaka osoba potencijalno može biti žrtva ovog napada. Hakeri uz upotrebu tehničkih ranjivosti, koriste i specifične psihološke i emotivne okidače (Alkhalil et al., 2021. prema Keepnet Labs, 2018. i Crane, 2019.). Otprilike 99% *phishing* napada oslanja se na ljudsku pogrešku za prodor u sustave (Bartram, n.d.).

Izvješće od PhishMe iz 2017. godine ustanovilo je da su najčešći okidači koji potiču ljude da odgovore na napad radoznalost i hitnost. Na njihovo mjesto kasnije dolaze glavni emocionalni motivatori kao što su zabava, društvene mreže i nagrade. U svakom slučaju psihološki okidači velikim dijelom utječu na donošenje svjesnih odluka. Prisutnost stresa kod ljudi izaziva nemogućnost sagledavanja svih eventualnih scenarija koje prate njihove odluke (Alkhalil et al., 2021. prema Lininger, Vines, 2005.).

Pojedina istraživanja bavila su se korelacijom između krađe identiteta i dobnih skupina. Studije su pokazale da je dobna skupina raspona između 18 i 25 godina podložnija krađi od drugih dobnih skupina (Alkhalil et al., 2021 prema Williams, Hinds, Joinson, 2018.). Iz razloga što mlađi odrasli imaju više povjerenja u internetsku komunikaciju, a stariji sudionici su manje impulzivni (Alkhalil et al., 2021 prema Get Safe Online.org, 2017. i Arnsten,, Mazure, April, 2012.).

## 2.3. Povijest *phishinga*

Prvotno hakeri su se zvali *phreaks* (KnowBe4, n.d.). Pojam *phreaking* potječe od riječi *freak* (nakaza) i *phone* (mobitel) koji je nastao 1970-ih godina (Malwarebytes, n.d.). 80-ih godina prošlog stoljeća tehnike krađe identiteta se detaljno opisuju i dostavljaju *International HP Users Group, Interex* (KnowBe4, n.d.). 10-ak godina kasnije *America Online* (u daljnjem tekstu; AOL), postaje vrhunskim pružateljem internetskih usluga u Sjedinjenim Američkim Državama. Svakodnevno imao je milijun posjetitelja. AOL je zbog svoje popularnosti bio na meti *warez* zajednice (osnovana od strane hakera i trgovaca piratskim softverom) koja je „posijala prvo sjeme“ *phishing* napada. *Warez* zajednica je s *phishing* napadima krenula na sljedeći način kradući korisničke podatke (korisničko ime, lozinku i slično) i uz pomoć *AoHella*, Windows aplikacije koje su stvorili počeli su generirati nasumične brojeve kreditnih kartica (PhishProtection., 2019.; KnowBe4, n.d.). Te podatke su koristili za otvaranje lažnih AOL računa i za slanje neželjene pošte

drugim AOL članovima i za druga zla ili podvale. Par godina kasnije AOL je poduzeo sigurnosne mjere i uspio zatvoriti *AoHell*, no *phishere* to nije spriječilo u svome naumu (KnowBe4, n.d.). Nedugo nakon toga stvorili su *phishing* tehniku prisutnu i danas. Preko AOL *messangera* slali su lažne e-mailove predstavljajući se kao AOL zaposlenici tražeći od njihovih klijenata da verificiraju svoje osobne podatke i podatke o naplati. Ljudi su upadali u zamku jer su poruke imale iste boje, fontove i tekst koje se koriste u e-mailovima AOL te su izgledale legitimno (PhishProtection., 2019.). Situacija se pogoršala kada su kreirali AIM račune i putem njih izvodili *phishing* napade kako bi izbjegli kršenje prava AOL-a te nisu bili ukinuti od njihove strane. AOL je upozorio sve klijente e-pošte i instant messangera da ne otkrivaju lozinke ili podatke o naplati te da to od njih nikada neće tražiti AOL zaposlenici (KnowBe4, n.d.).

Izraz *phishing* potječe od pojma *fishing* (hrv. pecanje ili ribolov) koji ima slova ph umjesto f i u skladu sa izvornim značenjem riječi *fishing*, „pecaju“ se korisnička imena, lozinke i druge osjetljive informacije u „moru“ korisnika (PhishProtection, 2019.). Termin *phishing* prvi put se spominje 2. siječnja 1996. godine u grupi zvanoj AoHell (Phishing.org, n.d.).

Od 2000. godine hakeri se prilagođavaju globalnoj situaciji u kojoj dolazi do porasta e-trgovine te shodno tome svoje snage usmjeravaju u to područje (PhishProtection, 2019.). Prvi takav napad se dogodio u lipnju 2001. godine kada su pokušali ukrasti podatke o identitetu preko *web*-mjesto E-gold, no to je bilo neuspješno. Sve do kraja 2003. napadi hakera su se smanjili da bi potom putem softvera za računalne crve slali e-poruke korisnicima eBaya i PayPala. Sadržaj je bio lažna veze na *web*-mjesto koja je nalikovala navedenim online sustavima plaćanja tražeći od primatelja da upišu brojeve kreditnih kartica i druge osobne podatke. Iduće godine *phishing* napadi su doživjeli pravi procvat. Hakeri su za mete uzimali banke, poduzeća i njihove klijente što je u vremenskom periodu od svibnja 2004 godine pa do svibnja iduće godine rezultiralo u iznosu od oko 929 milijarde američkih dolara s pogođenim 1,2 milijuna korisnika računala u SAD-u. Zbog krađe podataka tvrtke su godišnje gubile 2 milijarde dolara godišnje (CanIPhish, n.d.). Tijekom 2006. godine *phisheri* su nastavili ciljati klijente banaka i usluge online plaćanja. Koristili su se

pričom koja je i danas popularna. Predstavljali su se da su porezna uprava *Internal Revenue Service* kako bi došli do osjetljivih podataka (KnowBe4, n.d.).

Prema izvješću Gartnera iz 2007. godine procjenjuje se da je između kolovoza 2006. i kolovoza 2007. 3,6 milijuna korisnika izgubilo 3,2 milijarde dolara (Malwarebytes, n.d.). Dvije godine nakon, u upotrebu su stavljeni bitcoin i druge kriptovalute što je povećalo upotrebu zlonamjernog softvera kao olakšicu *cyber* kriminalcima da tajnije i anonimnije uspiju prevariti žrtve (Leksikografski zavod Miroslava Krleže, 2021.; Government of Canada, 2021. prema Get Cyber Safe). *Anti-Phishing Working Group* obavijestila da je od strane potrošača zaprimila više od 115 tisuća prijava o *phishing* mailovima u trećem tromjesečju 2009. godine (KnowBe4, n.d.).

2011. godine na interno osoblje tvrtke u području računalne sigurnosti, RSA uspješno je izveden *phishing* napad (Centar informacijske sigurnosti (CIS), 2011.; KnowBe4, n.d.). Svrha napada bila je doći do njihovih podataka, budući da je tvrtka pružala svoje usluge i ministarstvu obrane SAD-a (Centar informacijske sigurnosti (CIS), 2011.).

U 2013 godini dogodila su se 3 velika napada. Prvi je bio u kolovozu kada je reklamna paltforma *Outbrain* bila napadnuta. Drugi je bio kada je Targetovim klijentima 110 milijuna zapisa o kreditnim karticama putem lažnog računa proizvođača što je rezultiralo otpuštanjem glavnog direktora i osoblja IT sigurnosti te kompanije (KnowBe4, n.d.). Trećim događajem se zarazilo 250 000 osobnih računala preko iznimno opasnog virusa, *Cryptolockera* (KnowBe4, n.d.; Doevan, 2019.).

2014. godina obilježena je sa 4 velike *phishing* kampanje. Najveći od njih bio je napad usmjeren *Home Depotu* kada su osobni podaci i podaci o kreditnim karticama više od 100 milijuna kupaca objavljeni za prodaju na *web*-stranicama za hakiranje (KnowBe4, n.d.).

2016. godine napadi su orijentirani na korisnike *World Anti-Doping Agency* i na američke glasače od strane ruskih hakera kako bi se manipuliralo rezultatima američkih izbora (KnowBe4, n.d.).

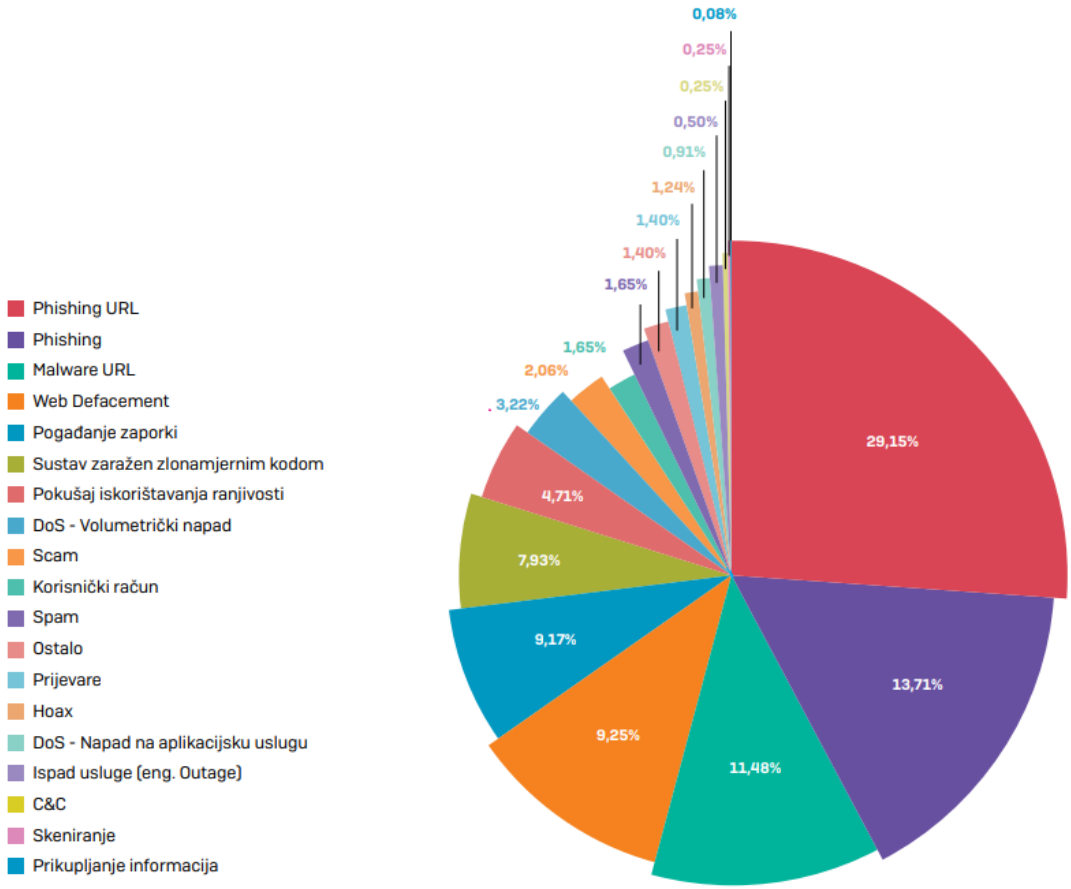
U 2017. *phishing* kampanje doživjele su pravi procvat. 76% organizacija je napadnuto, a pokazalo je da se svaki mjesec stvori 1,385 milijuna novih, jedinstvenih stranica za krađu identiteta. Najznačajniji gubitke pretrpjeli su računovodstveni odjeli Googlea i Facebooka prebacivši ukupno više od 100 milijuna dolara na bankovne račune napadača i tvrtka za kredite, *Equifax* kojoj su kompromitirani osobni podatci od otprilike 143 milijuna potrošača. U osobne podatke spadali su brojevi socijalnog osiguranja, puna imena, adrese, datumi rođenja pa čak i vozačke dozvole i brojevi kreditnih kartica. (KnowBe4, n.d.).

2018. godina obilježena je novom metodom krađe identiteta, a zove se otmica razgovora. Izvodi se tako da kriminalci u e-pošti najave žrtvi da će ju nazvati iz nekog vrlo bitnog i hitnog razloga praveći se autoritativnom organizacijom kako bi dobili željene podatke. Osim razvijene nove metode *phishing* napada, novi medij za napade koristi se Facebook messanger. Uz to *vishing* je vrlo raširena pojava *phishing* napad koja se povećala za 85% svake godine od 2011. godine (KnowBe4, n.d.). Sljedećih godina do današnjeg dana *phishing* bilježi znatno veće postotke porasta u odnosu na ostale cyber aktivnosti, a kriminalci sve više kao paravan koriste Microsoft Office 365 (KnowBe4, n.d.).

## 3. Statistika *phishing* napada u Republici Hrvatskoj u 2021. godini

Nacionalni CERT (engl. Computer Emergency Response Team) svake godine zaprima i obrađuje prijave koje se grupiraju kao računalno-sigurnosni incidenti te na temelju toga izrađuje godišnje izvještaje (CERT.hr, n.d.; Sullivan, 2021.). Godišnji izvještaj za 2021. godinu pokazuje da od ukupno prijavljenih 1211 računalnih incidenata, najveći udio čine *phishing* napadi i to preko 40% (gledajući *phishing* URL i *phishing*) što je i vidljivo iz grafikona 1. (CERT.hr, 2021.).

Grafikon 1. Raspodjela incidenata po tipu u 2021. godini




Izvor: https://www.cert.hr/wp-content/uploads/2022/03/CERT-godisnje-izvjesce-2021.pdf (18. 6. 2022.)

# 4. *Phishing* kampanje u Republici Hrvatskoj usmjerene poslovnim organizacijama

U vremenskom periodu od 2017. do 2022. godine u Republici Hrvatskoj *phishing* poruke putem e-maila bile su upućene širokom spektru poslovnih organizacija. Kroz godine su se neki scenarij poruka ponovili ili su bili vrlo slični, a ujedno je i njihov izgled bio sve vjerodostojniji.

## 4.1. *Phishing* kampanje od 2017. godine do 2021. godine

Prvi veći zabilježen napad koji se dogodio u 2017. godine bio je kada su se napadači prezentirali kao Porezna uprava tražeći od primatelja da preuzme dokument za novi pravni akt o poreznoj dobiti ukoliko pripadaju računovodstvenom odjelu tvrtke, a zapravo radilo se o preuzimanju zlonamjerne datoteke što je vidljivo na slici 4. (Tportal.hr, 2017.).

Slika 4. *Phishing* kampanja 2017. godine (Porezna uprava)


Poštovani,

Donosimo Vam nove izmjene o Porezu na Dobit.

Na snazi i primjenjuje se od 1. siječnja 2018. osim članka 7. stavka 1. točke 4. koja se primjenjuje od 1. siječnja 2019. godine.

Ovaj dio odnosi se isključivo na računovodstva u tvrtkama.
Ukoliko mislite da ste ovaj email dobili greškom prosljedite ga Vašem šefu računovodstva.

Preuzmite document na https://www.porezna-uprava.hr/hr_propisi/Zakon o Porezu na Dobit.pdf

Ukoliko Vam je jednostavnije preuzmite ga kao prilog u mailu.

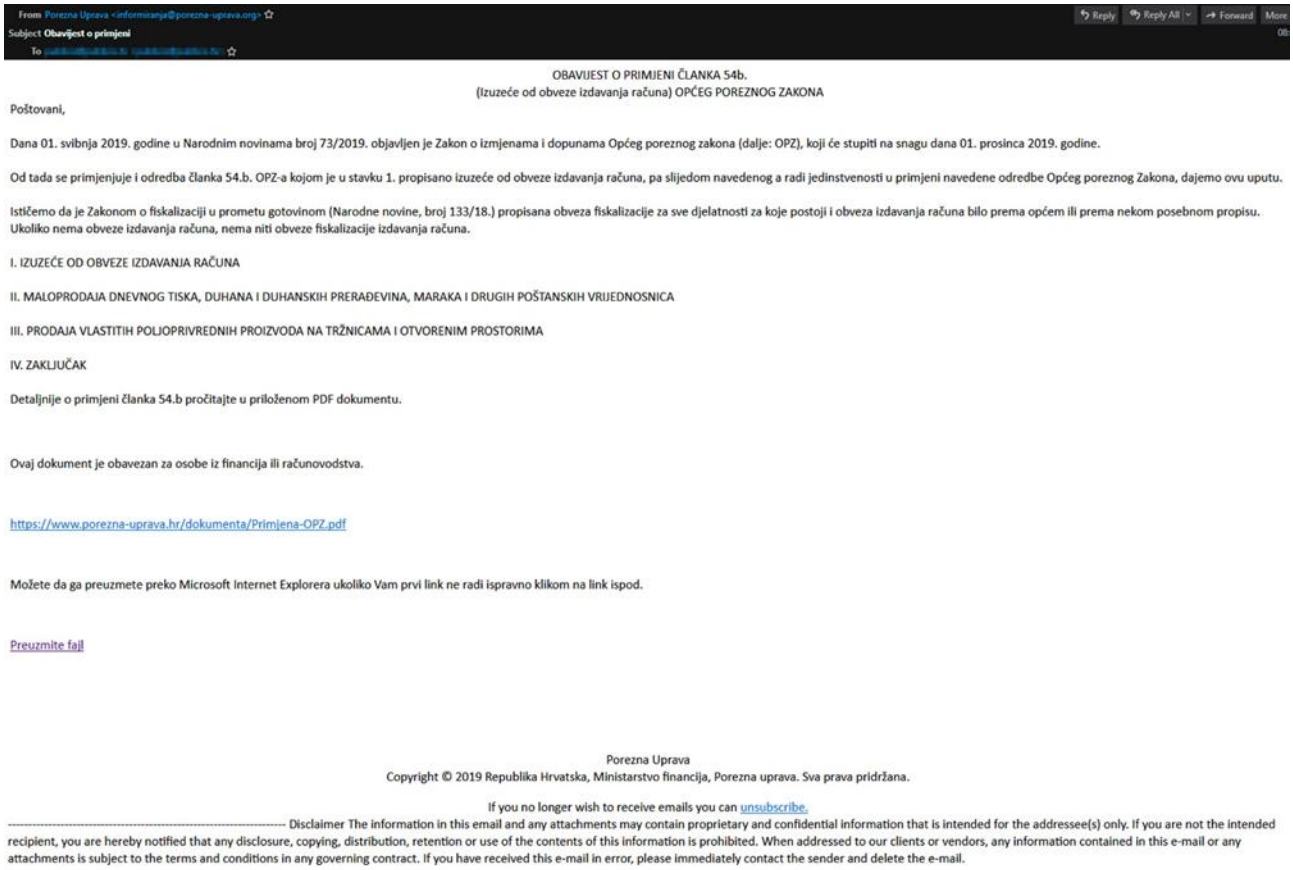
Preuzmite fajl

IZJAVA O ODRICANJU ODGOVORNOSTI: Ova elektronička pošta (i sve priložene datoteke) je povjerljiva i namijenjena je osobi ili osobama na koje je naslovljena. Ukoliko ste primili ovu poruku greškom, molimo Vas, obavijestite pošiljatelja, a poruku i sve njene privitke odmah, bez čitanja, trajno uklonite s računala. Bilo kakvo prenošenje, kopiranje ili distribucija informacija sadržanih u poruci trećim osobama je zabranjeno i može biti zakonski kažnjivo. Pošiljatelj ne prihvaća nikakvu odgovornost za bilo kakvu štetu ili gubitak podataka do kojeg može doći korištenjem ove elektroničke pošte. Sadržaj, stavovi i mišljenja izneseni u poruci su autorovi i ne predstavljaju nužno stavove Hrvatske gospodarske komore.

Izvor: https://www.tportal.hr/tehno/clanak/ne-nasjedajte-na-ovaj-lazni-mail-iz-porezne-mogli-biste-ostati-bez-podataka-20171201 (18. 6. 2022.)

Također i 2019. godine primatelji korporacija dobivaju sadržaj maila s malicioznim sadržajem čiji je „pošiljatelj“ Porezna uprava, vidljivo na slici 5. (CERT.hr, 2019.).

Slika 5. *Phishing* kampanja 2019. godine (Porezna uprava)


From Porezna Uprava <informiranja@porezna-uprava.org>
Subject Obavijest o primjeni
To

Reply Reply All Forward More

OBAVIJEST O PRIMJENI ČLANKA 54b.
(Izuzeće od obveze izdavanja računa) OPĆEG POREZNOG ZAKONA

Poštovani,

Dana 01. svibnja 2019. godine u Narodnim novinama broj 73/2019. objavljen je Zakon o izmjenama i dopunama Općeg poreznog zakona (dalje: OPZ), koji će stupiti na snagu dana 01. prosinca 2019. godine.

Od tada se primjenjuje i odredba članka 54.b. OPZ-a kojom je u stavku 1. propisano izuzeće od obveze izdavanja računa, pa slijedom navedenog a radi jedinstvenosti u primjeni navedene odredbe Općeg poreznog Zakona, dajemo ovu uputu.

Ističemo da je Zakonom o fiskalizaciji u prometu gotovinom (Narodne novine, broj 133/18.) propisana obveza fiskalizacije za sve djelatnosti za koje postoji i obveza izdavanja računa bilo prema općem ili prema nekom posebnom propisu. Ukoliko nema obveze izdavanja računa, nema niti obveze fiskalizacije izdavanja računa.

I. IZUZEĆE OD OBVEZE IZDAVANJA RAČUNA

II. MALOPRODAJA DNEVNOG TISKA, DUHANA I DUHANSKIH PRERAĐEVINA, MARAKA I DRUGIH POŠTANSKIH VRIJEDNOSNICA

III. PRODAJA VLASTITIH POLJOPRIVREDNIH PROIZVODA NA TRŽNICAMA I OTVORENIM PROSTORIMA

IV. ZAKLJUČAK

Detaljnije o primjeni članka 54.b pročitajte u priloženom PDF dokumentu.

Ovaj dokument je obavezan za osobe iz financija ili računovodstva.

https://www.porezna-uprava.hr/dokumenta/Primjena-OPZ.pdf

Možete da ga preuzmete preko Microsoft Internet Explorera ukoliko Vam prvi link ne radi ispravno klikom na link ispod.

Preuzmite fajl

Porezna Uprava
Copyright © 2019 Republika Hrvatska, Ministarstvo financija, Porezna uprava. Sva prava pridržana.

If you no longer wish to receive emails you can unsubscribe.

---------- Disclaimer The information in this email and any attachments may contain proprietary and confidential information that is intended for the addressee(s) only. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, retention or use of the contents of this information is prohibited. When addressed to our clients or vendors, any information contained in this e-mail or any attachments is subject to the terms and conditions in any governing contract. If you have received this e-mail in error, please immediately contact the sender and delete the e-mail.

Izvor: https://www.cert.hr/CUPOPOREZ (18. 6. 2022.)

2018. godine odabrane su obrazovne ustanove s ciljem kompromitiranja korisničkih računa zaposlenika kako bi se došlo do povjerljivih podataka. Pošiljatelj se predstavlja u ime e-mail administratora koji upozorava o premašenoj kvoti pohrane i navodi da se klikne na poveznicu i unesu korisnički podatci i lozinka kako bi se podatci mogli ažurirati, a time i primati nove e-poruke. Sadržaj poruke i izgled poveznice prikazani su u nastavku (slika 6.) (Mreža, 2018.).

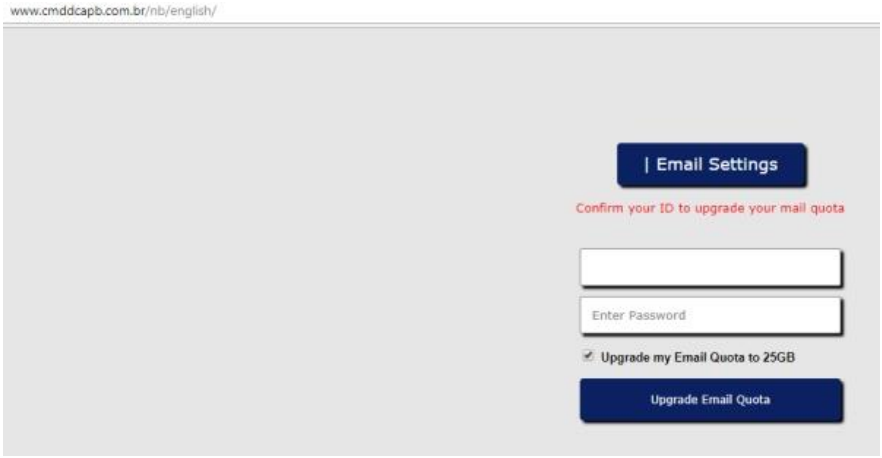
*„Webmail Aktivacija 4.5GB 0.5GB Premašili ste ograničenje pohrane spremnika kako ga postavlja administrator i nećete moći primati nove poruke e-pošte dok se ne aktivirate.*

*Ponovno aktiviraj klik*

*Pozdrav*

*Ažuriraj tim“*

Slika 6. *Phishing* kampanja 2018. godine na obrazovne ustanove



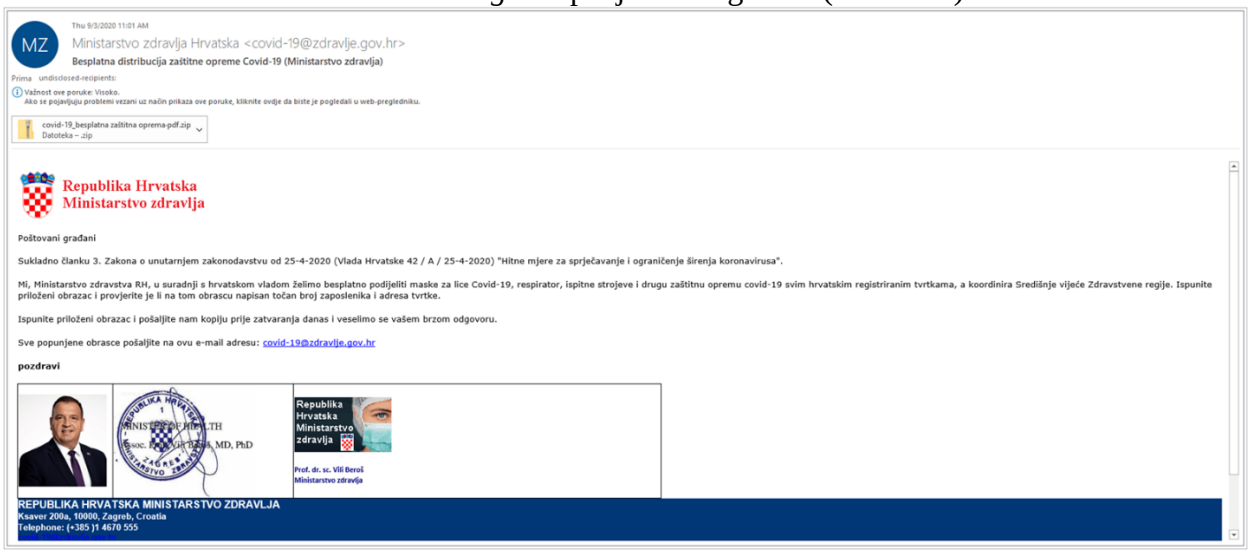

Izvor: https://mreza.bug.hr/napad-na-skolska-racunala/ (18. 6. 2022.)

2019. godine hrvatska državna tijela bila su na udaru *phishing* kampanje putem elektroničke pošte koja je sadržavala zlonamjernu poveznicu imitirajući službene stranice Hrvatske pošte. Zavod za sigurnost informacijskih sustava identificirao je dvije inačice zaražene datoteke, a radi se o zlonamjernim programima *Silent Trinity* i *Powershell Empire* koji omogućuju preuzimanje kontrole nad računalom (Jabuka.tv, 2019.).

Iste godine na udaru bio je i znatan broj trgovačkih društava od kojih se tražilo da se izvrši uplata na inozemni račun imitirajući da poruka dolazi od nadređenog (Ravnateljstvo policije, 2019.).

I 2020. godine bilježi se izniman porast *phishing* mailova upućena pravnim i fizičkim osobama za izvlačenje materijalne koristi upisivanjem korisničkih podataka. Na taj način je nepoznati počinitelj iz inozemstva uspio prevariti nekoliko soba (Samec, 2020.). Pored toga hakeri koriste aktualna zbivanja u vezi Covid-19 te se javljaju poruke sadržaja i izgleda Ministarstva zdravlja Hrvatske namijenjene hrvatskim firmama za „dodjelu“ besplatnih maski za lice i ostale opreme protiv pandemije te je u tu svrhu potrebno ispuniti obrazac, prikazano slikom 7. Otvaranjem priloženog obrasca pokreće se zlonamjerni sadržaj (Vrbanus, 2020.).

Slika 7. *Phishing* kampanja 2020. godine (Covid-19)



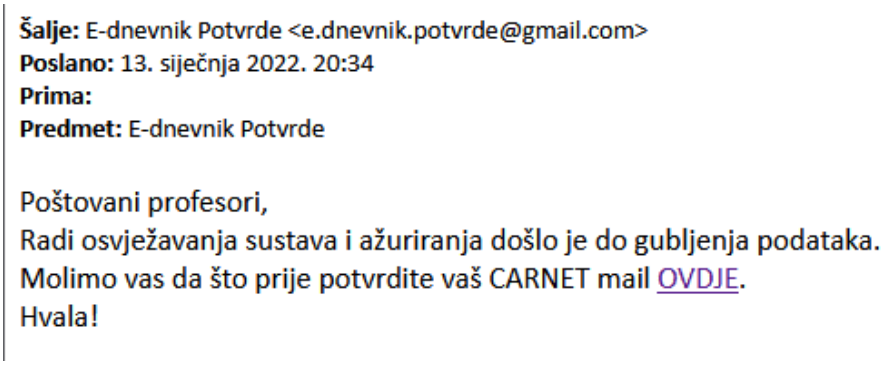
Izvor: https://www.bug.hr/sigurnost/u-hrvatskoj-aktivna-phishing-kampanja-vezana-uz-covid-19-16426 (18. 6. 2022.)

## 4.2. Phishing kampanje u 2022. godini

U ovoj 2022. godini *phishing* poruke vezana su uz zbivanja na istoku Europe upućena velikom broju tijela u Europskoj Uniji pa tako i u Hrvatskoj. U tekstu poruke spominju se Ukrajinske izbjeglice ili uplata financijskih sredstava kao donacije i slično kako bi naveli primatelja da pokrene maliciozni sadržaj (Marijanović, 2022.).

Kao i 2018. godine, mete su obrazovne ustanove s istim ciljem. U ovom slučaju razlog ispunjavanja korisničkih podataka, odnosno „potvrđivanja“ CARNET maila navodi se gubitak podataka koji se „dogodio“ uslijed osvježavanja i ažuriranja sustava, prikazano na slici 8. (Vrbanus, 2022.).

Slika 8. *Phishing* kampanja 2022. godine na obrazovne ustanove


**Šalje:** E-dnevnik Potvrde <e.dnevnik.potvrde@gmail.com>
**Poslano:** 13. siječnja 2022. 20:34
**Prima:**
**Predmet:** E-dnevnik Potvrde

Poštovani profesori,
Radi osvježavanja sustava i ažuriranja došlo je do gubljenja podataka.
Molimo vas da što prije potvrdite vaš CARNET mail OVDJE.
Hvala!

Izvor: https://www.bug.hr/sigurnost/nova-phishing-kampanja-u-hrvatskoj-ovoga-puta-cilja-ucitelje-25193 (18. 6. 2022.)

Poveznica vodi na lažnu stranicu koja koristi isti logo kao i prava stranica, kao što je i vidljivo u nastavku slike pod brojem 9 i 10.

Slika 9. *Phishing* kampanja 2022. godine (e-Dnevnik)


Izvor: https://www.bug.hr/sigurnost/nova-phishing-kampanja-u-hrvatskoj-ovoga-puta-cilja-ucitelje-25193 (18. 6. 2022.)

Slika 10. Originalan logo organizacije


Izvor: https://ocjene.skole.hr/login (18. 6. 2022.)

Osim toga zaprimljena je dojava policiji u Brodsko-posavskoj županiji od jedne tvrtke o gubitku nekoliko stotina tisuća kuna zbog *phishing* napada na način da se nepoznati počinitelj predstavio kao poslovni partner i slao je e-poruke podatke broja računa na koji treba uplatiti sredstva (Balen, 2022.).

# 5. Utjecaj *phishinga* na poslovne organizacije

Svake godine sve je više *phishing* napada na korporacije, neovisno radi li se o malim poduzećima ili onima svjetskih razmjera. Svjetska poduzeća mjesečno prime i do 1000 napada takve vrste (Packetlabs, 2020.). Kakvu posljedicu će imati uspješan napad krađe identiteta usmjeren na organizacije ovisi o različitim čimbenicima, kao što su veličina poduzeća i količina informacija koja je ugrožena (FraudWatch, 2021.). Potencijalni nepoželjni ishodi za organizaciju su financijski gubitci, gubitak intelektualnog vlasništva, reputacijski gubitak i poremećaj poslovanja (Packetlabs, 2020.).

## 5.1. Financijski gubitak

U slučaju da se organizacija postane žrtva krađe identiteta prva i najvažnija reperkusija su novčani troškovi koji mogu biti izravni i neizravni. Pod neizravne troškove podrazumijevaju se oni troškovi koji su rezultat „kršenja“ propisa pravnih akata poput Zakona o zaštitu osobnih podataka (Narodne novine, br. 106/2012) i drugih te naknada pogođenim klijentima. Ukupni troškovi lako mogu doseći iznimno visoke cifre (Packetlabs, 2020.).

## 5.2. Gubitak intelektualnog vlasništva

Najrazorniji gubitak za organizaciju predstavlja krađa intelektualnog vlasništva, tj. podatci o klijentima, poslovne tajne, istraživanja, informacije o nadolazećim lansiranjima proizvoda ili novim partnerstvima. Osobito ako se radi o firmama čija djelatnost obuhvaća tehnologiju, obranu,

farmaciju i slično. Primjerice krađa patenta za lijekove može uzrokovati milijunske štete što ujedno utječe i na konkurentsku prednost na tržištu (Packetlabs, 2020.).

## 5.3. Šteta ugleda

Tvrtke godinama grade i ulažu u povjerenje kupaca jer o tome u konačnici ovisi dugoročni uspjeh tvrtke. Studije pokazuju da je povjerenje drugi najvažniji čimbenik da će kupac odabrati firmu kojoj vjeruje (First Citizens Bank, 2021.). Povjerenjem kupaca firma od svoga proizvoda uspijeva stvoriti marku (engl. brand) i stječe ugled (Packetlabs, 2020.). Obje stavke koje proizlaze iz povjerenja kupaca, kao i samo povjerenje i to ne samo kupaca, već i cijelog lanca ljudi o kojima organizacija ovisi (dobavljači, investitori, zaposlenici) gubi ukoliko podatak da je na nju uspješno izveden *phishing* napad otkrije se u javnosti (Wallarm, n.d.). Nažalost, takvo novonastalo mišljenje je vrlo teško promijeniti u javnosti. Zbog toga je *cyber* sigurnost neophodna u svim fazama razvoja projekta. Istraživanja pokazuju da 40-ak % potrošača ne bi više koristili proizvode od firme na koju je uspješno izveden *phishing* napad (CybSafe, 2021.).

## 5.4. Poremećaj poslovanja

Uspješan *phishing* napad na firmu dovodi do poremećaja u poslovanju, pogotovo ako se radi o napadima koji uključuju zlonamjerni softver. Da bi organizacija radila kao i prije samog napada potrebno je neko vrijeme da se oporavi. Oporavak uključuje gašenje sustava, a sve rezultira smanjenjem produktivnosti, a time i novčanim gubicima (Wallarm, n.d.). Ukoliko se prekida poslovanje tvrtki koje pružaju usluge poput prijevoza, tehnologije, zbrinjavanje otpada i drugih kritičnih infrastruktura proistječu i gospodarski i društveni poremećaji (Wallarm, n.d.; (Packetlabs, 2020.).

# 6. Istraživanje o prepoznavanju e-mail *phishinga* u poslovnim organizacijama

U ovom poglavlju opisat će se provedeno istraživanje o e-mail *phishinga* u poslovnim organizacijama čiji zaposlenici obavljaju uredske poslove.

## 6.1. Podatci i metodologija istraživanja

Istraživanje o prepoznavanju e-mail *phishinga* u poslovnim organizacijama izvedeno je metodom ankete. Prema definiciji anketa predstavlja „prikupljanje mišljenja i podataka o nekoj pojavi među većim brojem osoba radi statistike, ispitivanja tržišta ili javnog mišljenja ili kao baza za neko daljnje proučavanje“ (Anić, et al., 2004., 119.).

Ono je provedeno u vremenskom razdoblju od 1. lipnja do 15. lipnja 2022. godine na području Primorsko-goranske županije. Ciljana skupina je radna populacija koja obavlja uredske poslove i u svakodnevnom radu koristi računalo. Anketiranje je izvedeno online, a za izradu ankete koristio se alat *LimeSurvey*. Poduzeća koja su pozvana na sudjelovanje u ovoj studiji obaviještena su da je ono anonimno, odnosno ukoliko odluče biti dijelom istraživanja neće se otkriti njihov identitet niti djelatnost kojom se bave. Sudjelovalo je 5 poduzeća različitih djelatnosti. Anketnom upitniku ukupno je pristupilo 214 osoba, a 190 (n = 190) riješilo je potpuno. Razmatraju se samo oni obrasci koji su u potpunosti ispunjeni.

Anketa se sastoji od 22 pitanja te je koncipirana s konkretnim pitanjima i odgovorima, osim zadnjeg pitanja u kojemu je bilo moguće izraziti svoj komentar u vezi ankete i *phishing* napada. Njome se ispituje znanje o *phishing* napadima putem e-maila, navike zaposlenika koje pridonose

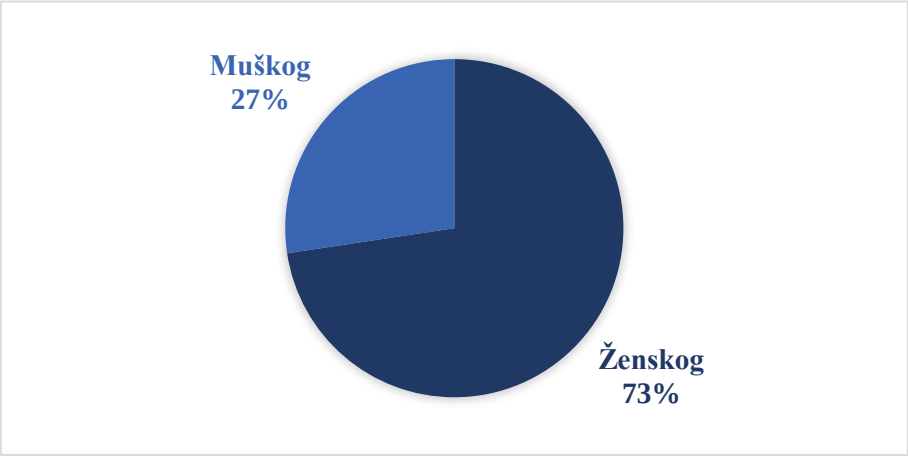
da oni budu „upecani“ te savjesnost osobe kao zaposlenika. Anketa se može podijeliti na 4 dijela te svaki od njih predstavlja sljedeće:

1. demografski podatci,
2. znanje iz područja *phishinga*,
3. navike kojima se povećava nivo informatičke sigurnosti: 4 stupnja učestalosti od kojih se „nikad“ i „ponekad“ svrstani u nepoželjne navike, a „često“ i „uvijek“ u poželjne navike, osim kod potpitanja „spremate svoje podatke za prijavu kada koristite *web* preglednik“ gdje su navike suprotno svrstane,
4. edukacija i savjesnost.

### 6.1.1. Demografski podatci

**Pitanje pod brojem 1 glasi: „Kojeg ste spola?“**

Grafikon 2. Spol ispitanika

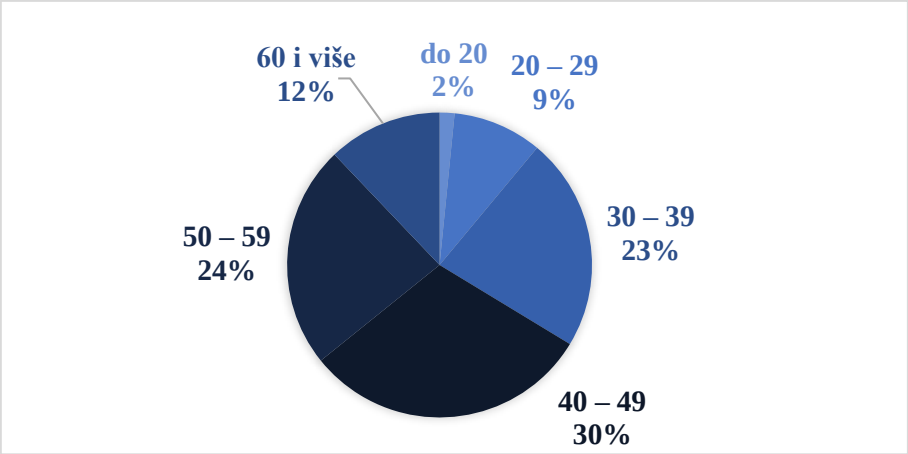



Izvor: Autorica

Iz grafikona je vidljivo da 73% osoba (138 ispitanika) pripada ženskom spolu, a 27% osoba (52 ispitanika) muškom.

**Pitanje pod brojem 2 glasi: „Koliko imate godina?“**

Grafikon 3. Dob ispitanika




Izvor: Autorica

Iz grafikona je vidljivo da 2% osoba (3 ispitanika) pripada skupini do 20 godina, 9% osoba (18 ispitanika) skupini od 20 do 29, 23% osoba (43 ispitanika) skupini od 30 do 39, 30% osoba (58 ispitanika) skupini od 40 do 49, 24% osoba (45 ispitanika) skupini od 50 do 59, a 12% osoba (23 ispitanika) skupini od 60 i više godina.

**Pitanje pod brojem 3 glasi: „Kojeg ste stupnja obrazovanja?“**

Grafikon 4. Stupanj obrazovanja

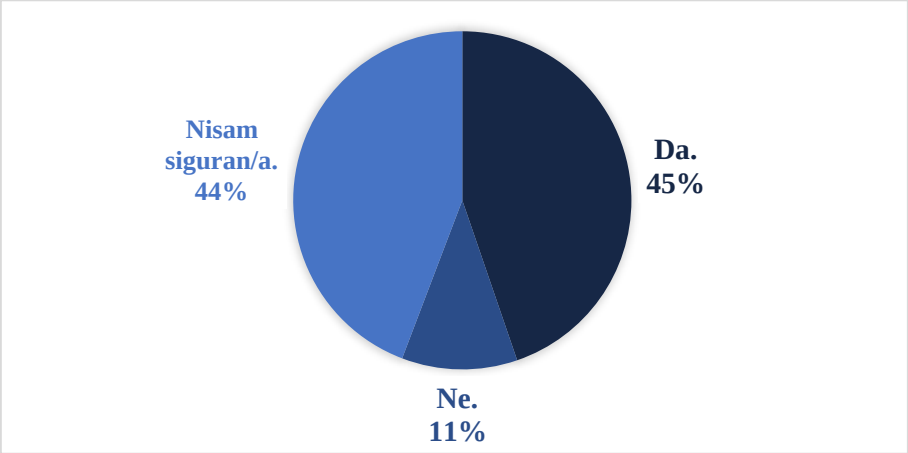

Izvor: Autorica

Iz grafikona je vidljivo da 0% osoba (0 ispitanika) ima osnovnoškolsko obrazovanje, 23% osoba (44 ispitanika) ima srednjoškolsko obrazovanje, 63% osoba (120 ispitanika) ima visokoškolsko ili fakultetsko obrazovanje, 14% osoba (26 ispitanika) ima magisterij ili doktorat.

### 6.1.2. Znanje iz područja „*phishinga*“

**Pitanje pod brojem 4 glasi: „Smatrate li da znate prepoznati *phishing* prijevaru?“**

Grafikon 5. Prepoznavanje prijevare

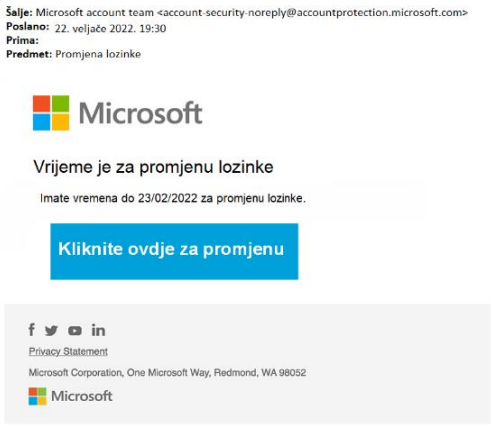



Izvor: Autorica

Iz grafikona je vidljivo da 45% osoba (85 ispitanika) smatra da zna prepoznati *phishing* prijevare, 11% osoba (21 ispitanika) smatra da ih ne zna prepoznati, a 44% osoba (84 ispitanika) nije sigurno.

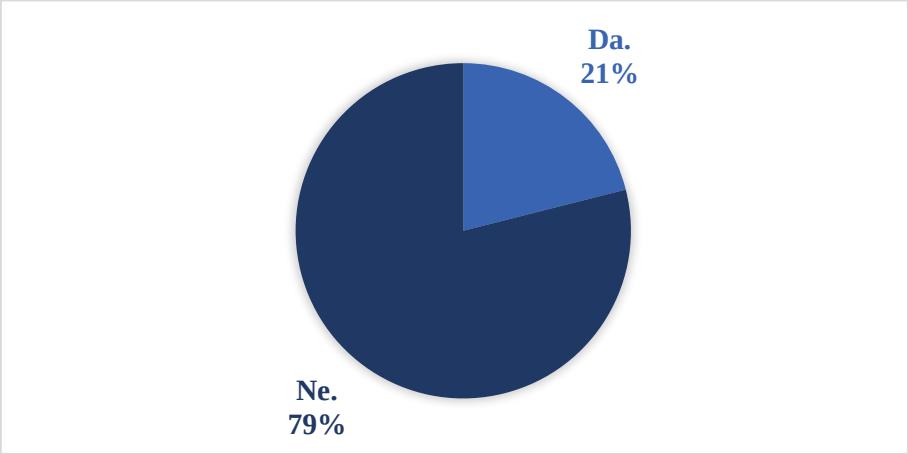
**Pitanje pod brojem 5 glasi: „Biste li pratili upute sljedećeg maila?“** Točan odgovor je: „Ne.“

Slika 11. Zadani mail za pitanje pod brojem 5




Izvor: pripremila autorica prema https://www.inky.com/en/blog/six-convincing-phishing-emails-that-just-might-fool-you (18. 6. 2022.)

Grafikon 6. Praćenje upute maila (Microsoft)

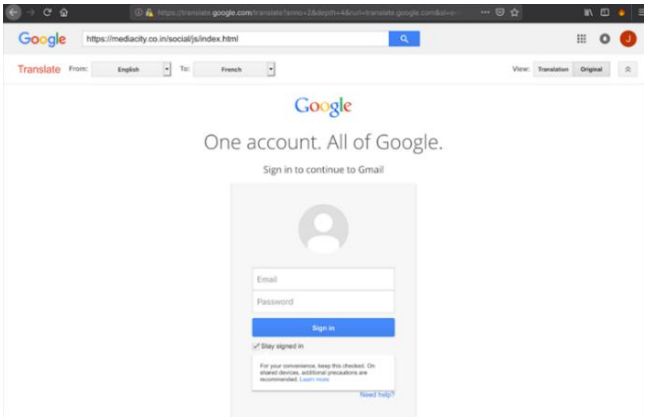



Izvor: Autorica

Iz grafikona je vidljivo da 21% osoba (40 ispitanika) pratila bi upute maila, a 79% osoba (150 ispitanika) ne.

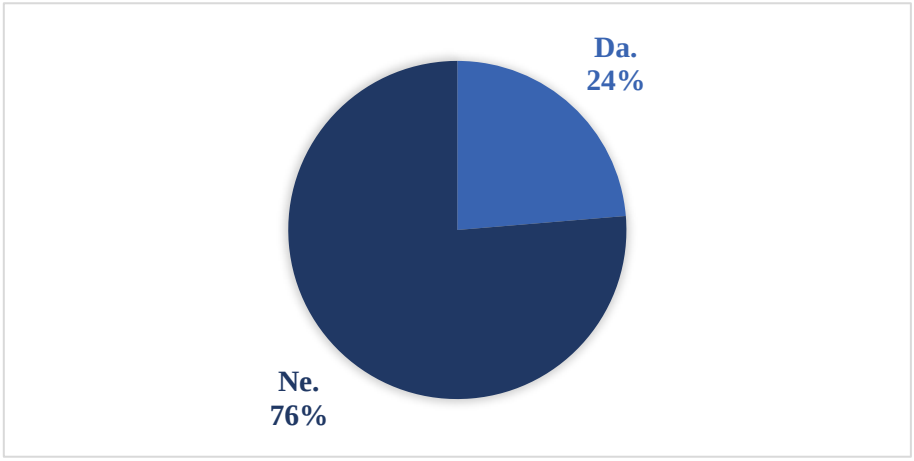
**Pitanje pod brojem 6 glasi: „Biste li se prijavili na sljedećoj stranici?“** Točan odgovor je: „Ne.“

Slika 12. Zadana *web*-stranica za pitanje pod brojem 6




Izvor: https://blog.knowbe4.com/new-phishing-attack-uses-google-translate-to-spoof-login-page-and-fool-victims (18. 6. 2022.)

Grafikon 7. Prijava na *web*-stranici (Google)

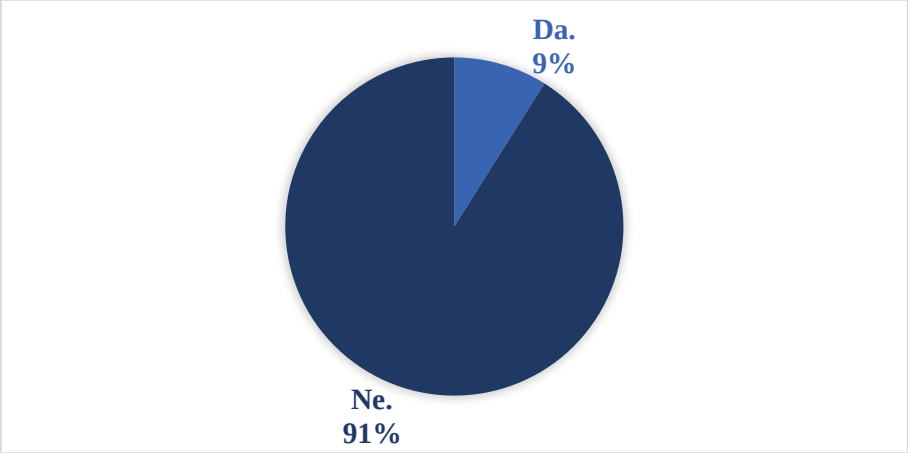



Izvor: Autorica

Iz grafikona je vidljivo da 24% osoba (45 ispitanika) prijavila bi se na *web*-stranicu, a 76% osoba (145 ispitanika) ne.

**Pitanje pod brojem 7 glasi: „Banka Vam šalje e-mail u kojem kaže da ukoliko odmah ne ažurirate osobne podatke da će Vam račun biti obustavljen, Vi ćete odgovoriti na takvu poruku:“** Točan odgovor je: „Ne.“

Grafikon 8. Praćenje upute maila (banka)

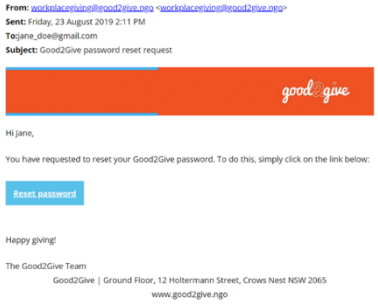



Izvor: Autorica

Iz grafikona je vidljivo da 9% osoba (17 ispitanika) pratila bi upute maila, a 91% osoba (173 ispitanika) ne.

**Pitanje pod brojem 8 glasi: „Biste li pratili upute ovog maila?“** (Australian Cyber Security Centre, n.d.) Točan odgovor je: „Da.“ jer je zadani mail legitiman.

Slika 13. Zadani mail za pitanje pod brojem 8


From: workplacegiving@good2give.ngo <workplacegiving@good2give.ngo>
Sent: Friday, 23 August 2019 2:11 PM
To: jane_doe@gmail.com
Subject: Good2Give password reset request

good2give

Hi Jane,

You have requested to reset your Good2Give password. To do this, simply click on the link below:

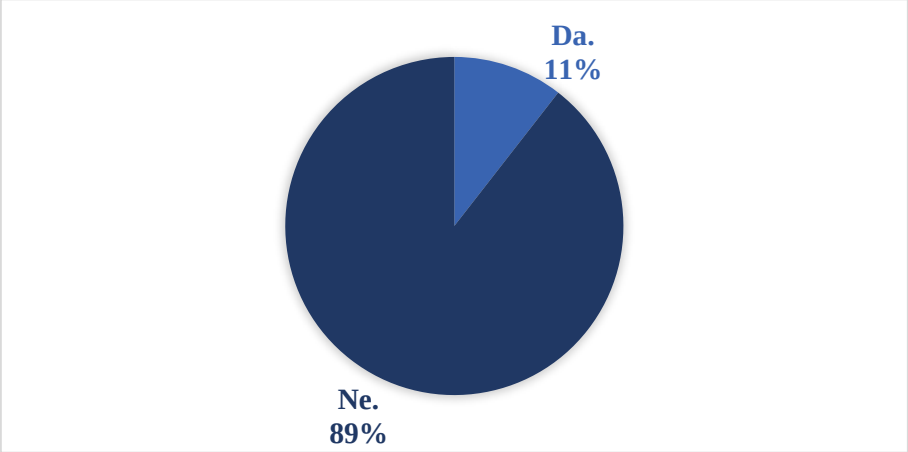
Reset password

Happy giving!

The Good2Give Team
Good2Give | Ground Floor, 12 Holtermann Street, Crows Nest NSW 2065
www.good2give.ngo

Izvor: https://www.cyber.gov.au/acsc/view-all-content/campaign/know-how-spot-phishing-scam-messages/scam-messages/quiz (18. 6. 2022.)

Grafikon 9. Praćenje upute maila *(Good2Give)*

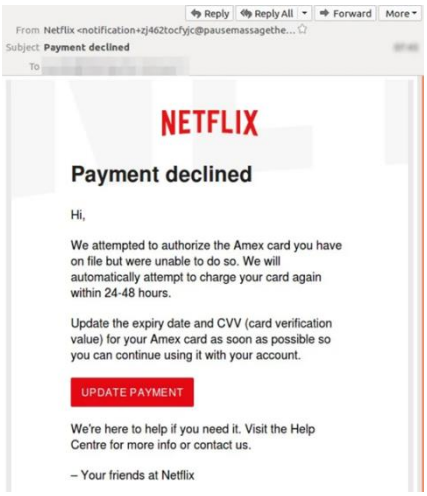



Izvor: Autorica

Iz grafikona je vidljivo da 11% osoba (20 ispitanika) pratila bi upute maila, a 89% osoba (170 ispitanika) ne.

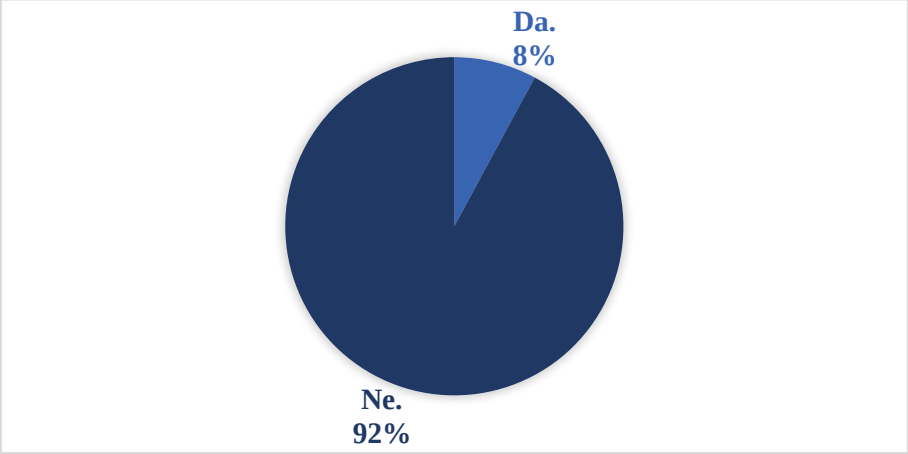
**Pitanje pod brojem 9 glasi: „ Biste li pratili upute sljedećeg maila:“** Točan odgovor je: „Ne.“

Slika 14. Zadani mail za pitanje pod brojem 9




Izvor: https://www.mailguard.com.au/blog/netflix-phishing-180110 (18. 6. 2022.)

Grafikon 10. Praćenje upute maila (Netflix)

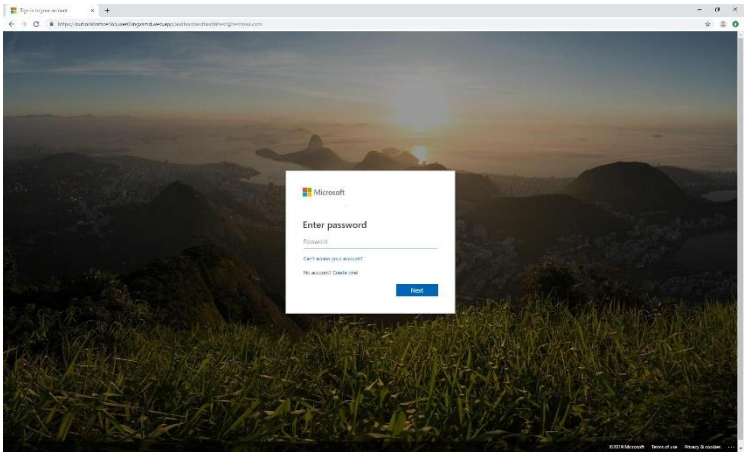



Izvor: Autorica

Iz grafikona je vidljivo da 8% osoba (15 Ispitanika) pratila bi upute maila, a 92% osoba (175 Ispitanika) ne.

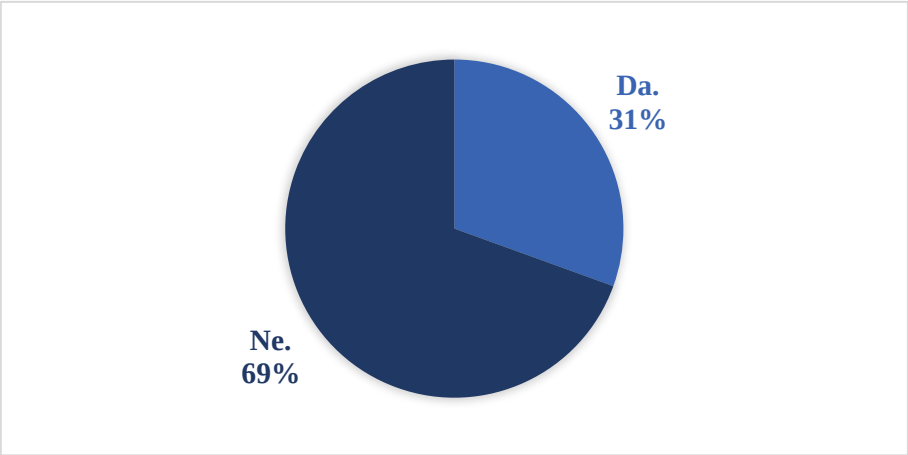
**Pitanje pod brojem 10 glasi: „Biste li se prijavili na sljedećoj stranici?“** Točan odgovor je: „Ne.“

Slika 15. Zadana *web*-stranica za pitanje pod brojem 10




Izvor: pripremila autorica prema https://sensorstechforum.com/phishing-fake-microsoft-login-404-page/ (18. 6. 2022.)

Grafikon 11. Prijava na *web*-stranici (Microsoft)

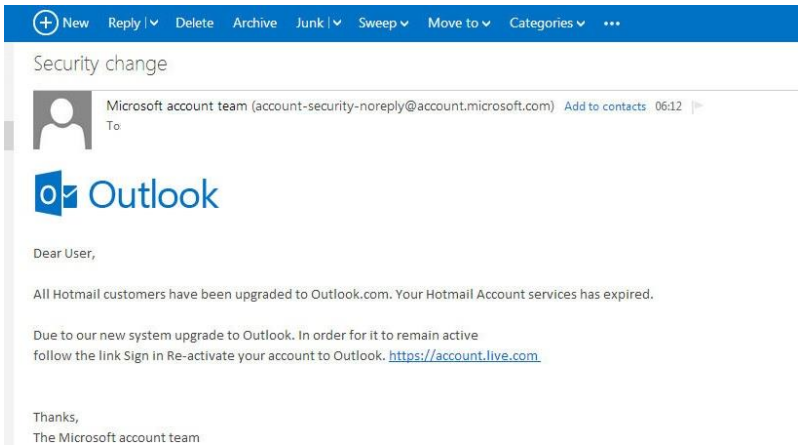



Izvor: Autorica

Iz grafikona je vidljivo da 31% osoba (58 ispitanika) prijavila bi se na *web*-stranicu, a 69% osoba (132 ispitanika) ne.

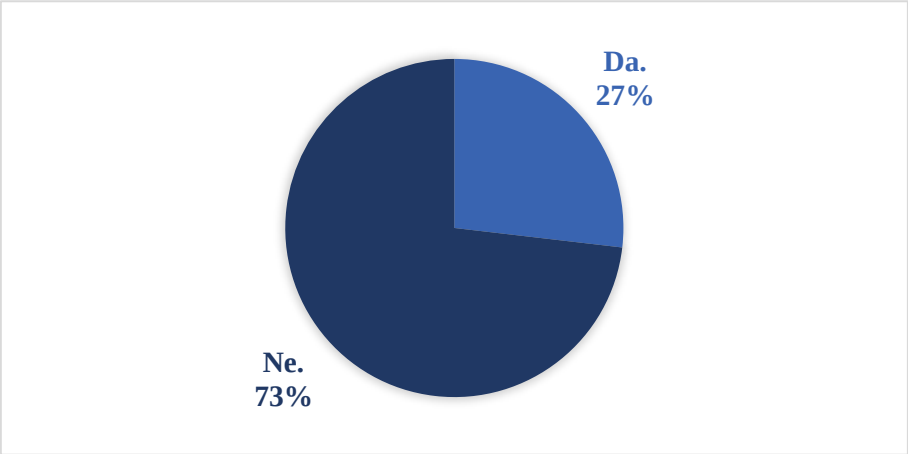
**Pitanje pod brojem 11: „ Biste li pratili upute sljedećeg maila:“** Točan odgovor je: „Ne.“

Slika 16. Zadani mail za pitanje pod brojem 11




Izvor: https://news.softpedia.com/news/Phishing-Alert-Hotmail-Customers-Have-Been-Upgraded-to-Outlook-com-429699.shtml (18. 6. 2022.)

Grafikon 12. Praćenje uputa maila (Outlook)




Izvor: Autorica

Iz grafikona je vidljivo da 27% osoba (51 ispitanik) pratila bi upute maila, a 73% osoba (139 ispitanika) ne.

**Pitanje pod brojem 12 glasi: „Dobili ste e-mail od šefa koji od Vas hitno traži da pošaljete svoje ime i prezime te broj korisničkog računa kako bi Vam mogao isplatiti plaću za ovaj mjesec. Mail ste dobili nekoliko dana prije isplate plaće. Vi ćete učiniti sljedeće:“** Točan odgovor je: „ignorirat ćete poruku.“

Grafikon 13. Praćenje upute maila (šef)

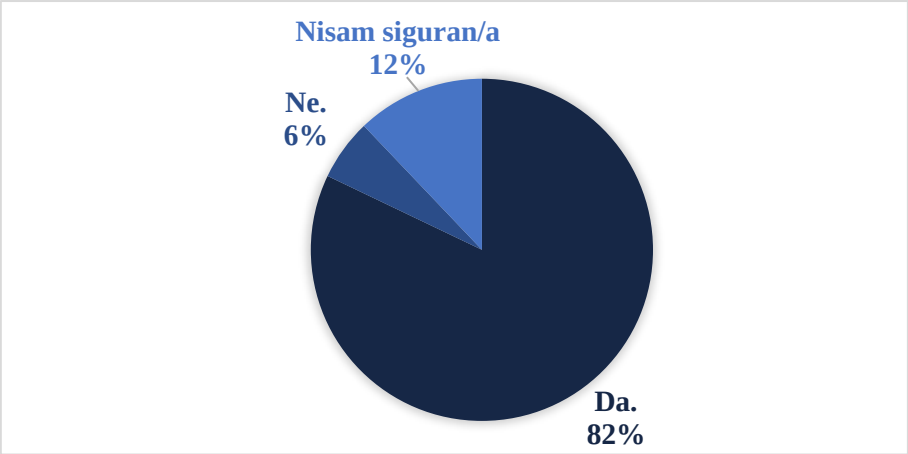

Izvor: Autorica

Iz grafikona je vidljivo da 3% osoba (5 ispitanik) odgovorila bi odmah na takav mail, 12% osoba (23 ispitanik) ne bi odgovorila na poruku dok ne provjere je li njihov kolega to učinio, 46% osoba (87 ispitanik) ukoliko je u mailu ostavljen broj šefovog ureda, nazvala bi ga i na taj način mu ostavila tražene podatke jer je to najsigurnije, a 39% osoba (75 ispitanik) ignorirala bi takvu poruku.

**Pitanje pod brojem 13 glasi: „Znakovi *phishing* prijevara su:**

**a) potreban je hitan odgovor.“** Točan odgovor je: „Da.“

Grafikon 14. Hitan odgovor

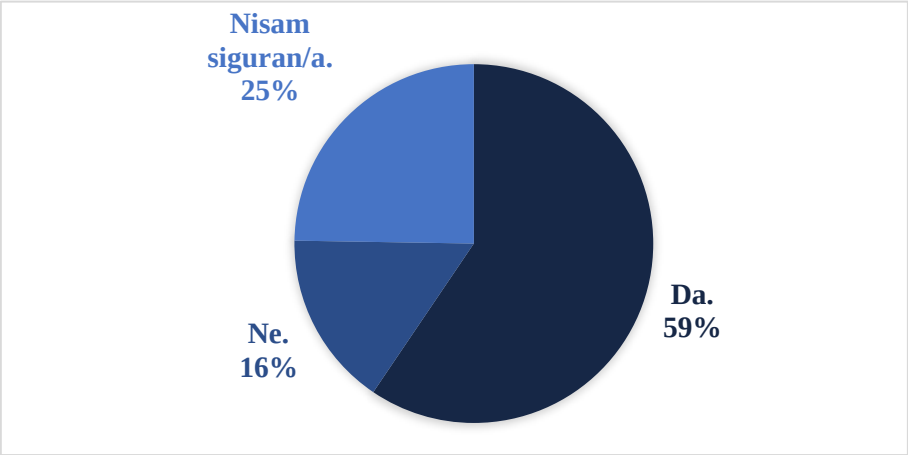



Izvor: Autorica

Iz grafikona je vidljivo da 82% osoba (156 ispitanika) prepoznaje obilježje *phishing* prijevare, 6% osoba (11 Ispitanika) ne, a 12% osoba (23 ispitanika) nije sigurno.

b) **„ generički pozdrav upućen primatelju (npr. Dragi korisniče).“** Točan odgovor je: „Da.“

Grafikon 15. Generički pozdrav

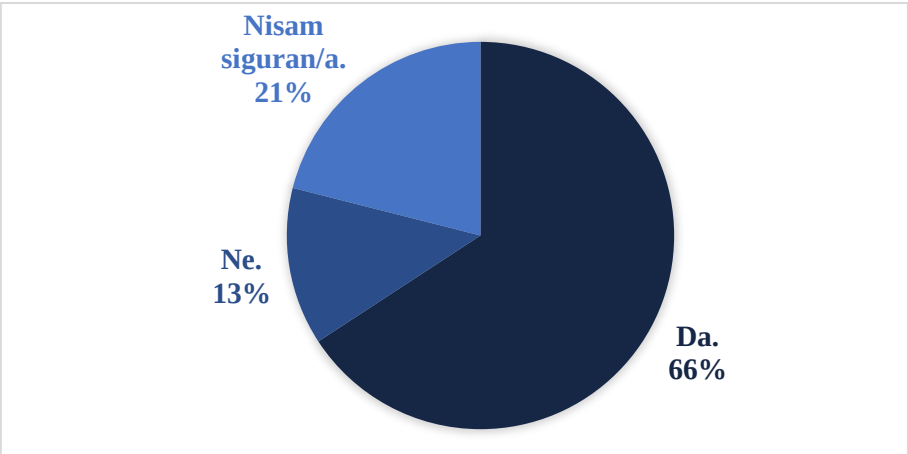



Izvor: Autorica

Iz grafikona je vidljivo da 59% osoba (113 ispitanika) prepoznaje obilježje *phishing* prijevare, 16% osoba (30 ispitanika) ne, a 25% osoba (46 ispitanika) nije sigurno.

c) **„pravopisne i gramatičke pogreške.“** Točan odgovor je: „Da.“

Grafikon 16. Pravopisne i gramatičke pogreške



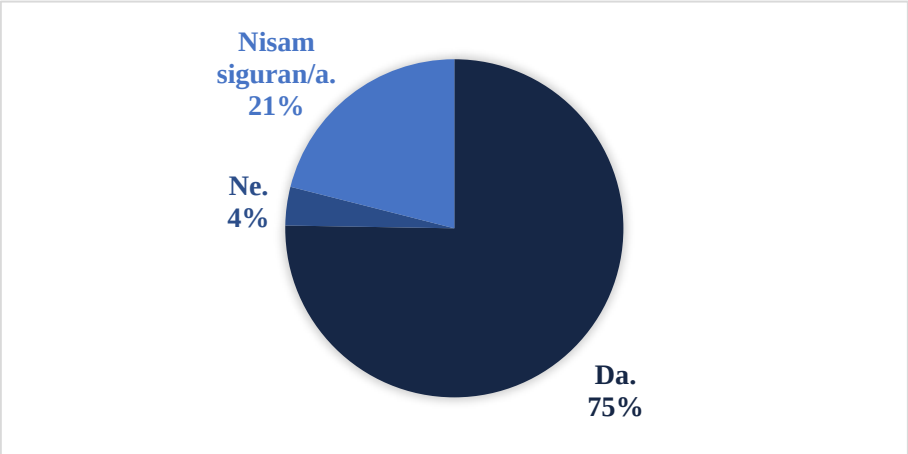

Izvor: Autorica

Iz grafikona je vidljivo da 66% osoba (125 ispitanika) prepoznaje obilježje *phishing* prijevare, 13% osoba (25 ispitanika) ne, a 21% osoba (40 ispitanika) nije sigurno.

**d) „mail čiji sadržaj Vas obavještava o zatvaranju ili brisanju korisničkog računa.“**

Točan odgovor je: „Da.**“**

Grafikon 17. Zatvaranje ili brisanje korisničkog računa

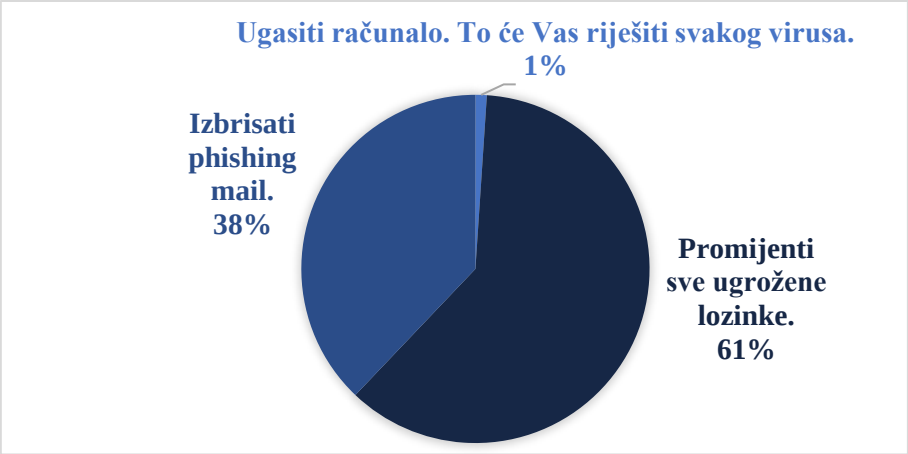



Izvor: Autorica

Iz grafikona je vidljivo da 75% osoba (143 ispitanika) prepoznaje obilježje *phishing* prijevare, 4% osoba (7 ispitanika) ne, a 21% osoba (40 ispitanika) nije sigurno.

**Pitanje pod brojem 14 glasi: „ Kako ćete postupiti u slučaju da postanete žrtva *phishing* napada?“** prema Federal Trade Commission, n.d. Točan odgovor je: „Promijeniti sve ugrožene lozinke.“

Grafikon 18. Daljnji postupak



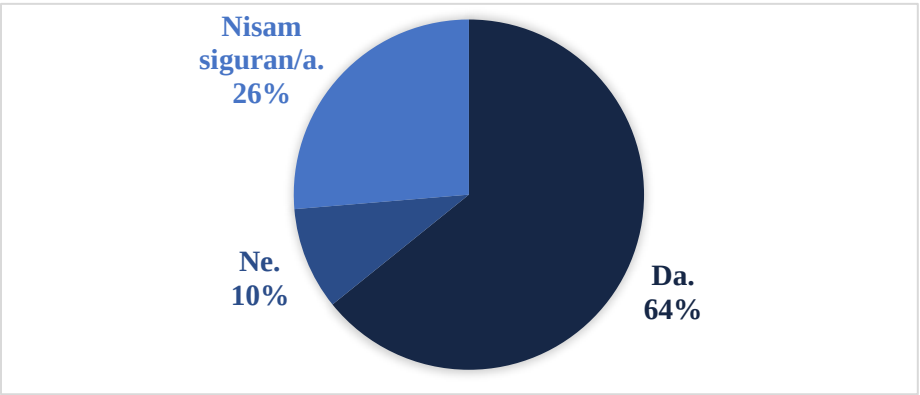

Izvor: Autorica

Iz grafikona je vidljivo da 1% osoba (2 ispitanika) ugasila bi računalo, 61% osoba (116 ispitanika) promijenila bi ugrožene lozinke, a 38% osoba (72 ispitanika) izbrisala bi *phishing* mail.

**Pitanje pod brojem 15 glasi: „Sljedeće aktivnosti sprječavaju *phishing* napad ili ne dovode u opasnost:**

**a) redovito ažuriranje operativnog sustava**“ Točan odgovor je: „Da.“

Grafikon 19. Redovito ažuriranje sustava

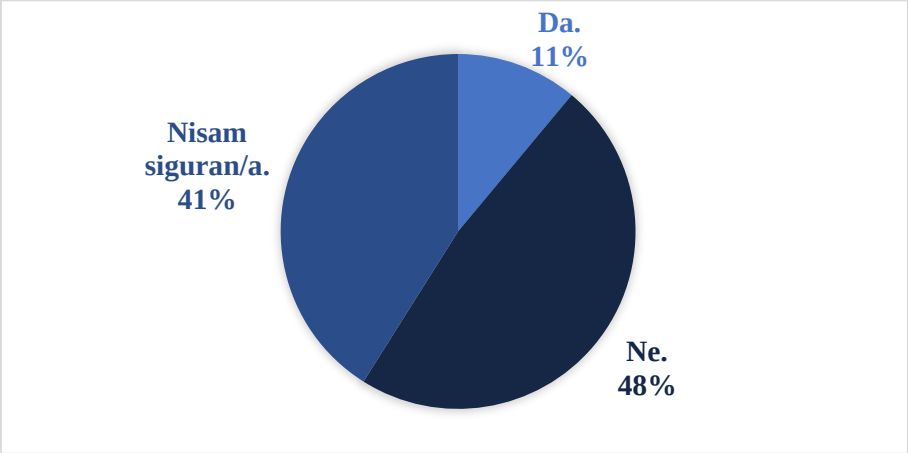



Izvor: Autorica

Iz grafikona je vidljivo da 64% osoba (122 ispitanika) zna da redovito ažuriranje sustava sprječava *phsihing* napad, 10% osoba (18 ispitanika) ne zna, a 26% osoba (5 ispitanika) nije sigurno.

**b) „klikanje na omogući sadržaj/enable editing u sustavima Microsoft Offica“** Točan odgovor je: „Ne.“

Grafikon 20. Klikanje na omogući sadržaj

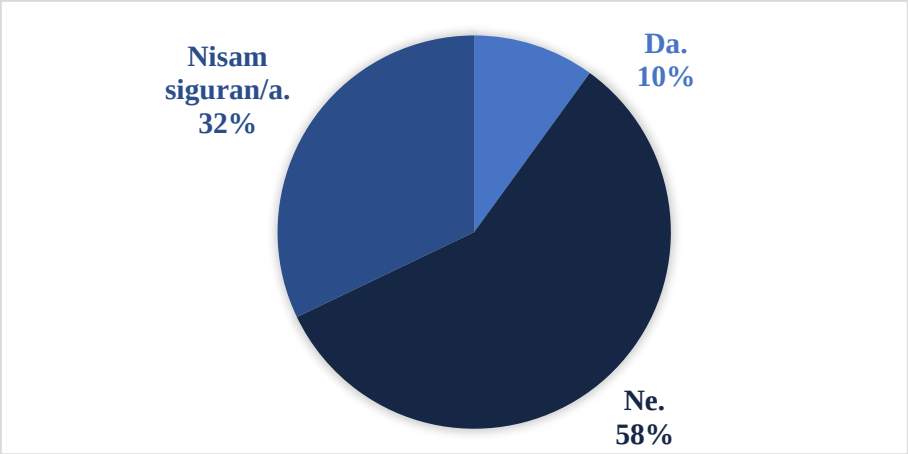



Izvor: Autorica

Iz grafikona je vidljivo da 11% osoba (21 ispitanika) ne zna da takva radnja dovodi u opasnost, 48% osoba (91 ispitanika) zna, a 41% osoba (78 osiguranika) nije sigurno.

**c) „otvaranje tekstualne datoteke (datoteka s nastavkom .txt).“** Točan odgovor je: „Ne.“

Grafikon 21. Otvaranje tekstualne datoteke

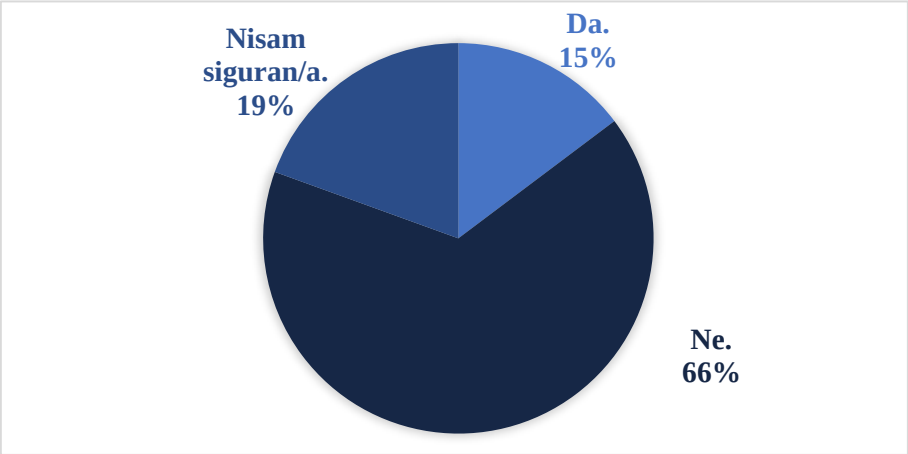



Izvor: Autorica

Iz grafikona je vidljivo da 10% osoba (19 ispitanika) ne zna da otvaranje tekstualne datoteke dovodi u opasnost, 58% osoba (110 ispitanika) zna, a 32% osoba (61 ispitanika) nije sigurno.

**d) „slanje podatka o PIN-u bankovne kartice, samo ako to traži Vaša matična banka.“** Točan odgovor je: „Ne.“

Grafikon 22. Slanje podataka o PIN-u banci




Izvor: Autorica

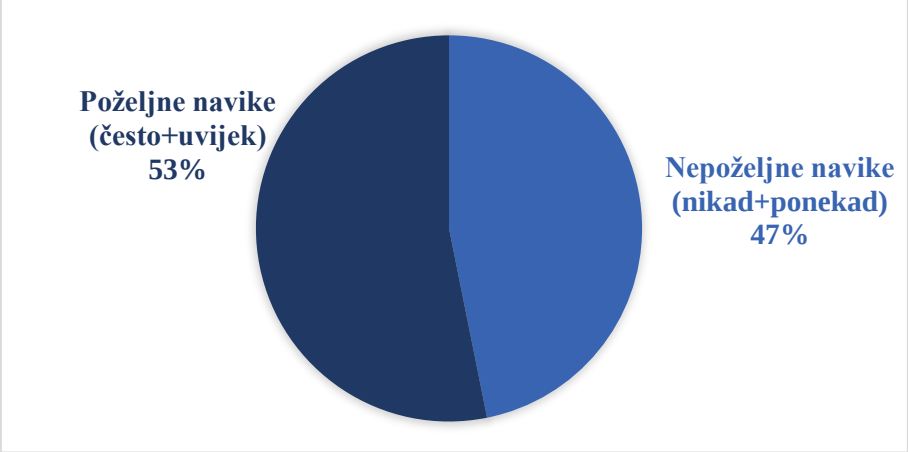
Iz grafikona je vidljivo da 15% osoba (28 ispitanika) ne zna da ne smije slati podatke o PIN-u ako to traži matična banka, 66% osoba (125 ispitanika) zna, a 19% osoba (37 ispitanika) nije sigurno.

### 6.1.3. Navike kojima se povećava nivo informatičke sigurnosti

**Pitanje pod brojem 16 glasi: „Na skali od 1 do 4 koliko često provodite sljedeće aktivnosti:**

**a) provjeravate je li uistinu pošiljatelj maila onaj za koji se predstavlja prije nego što otvorite priloženi link (ili poveznicu).“**

Grafikon 23. Provjera pošiljatelja

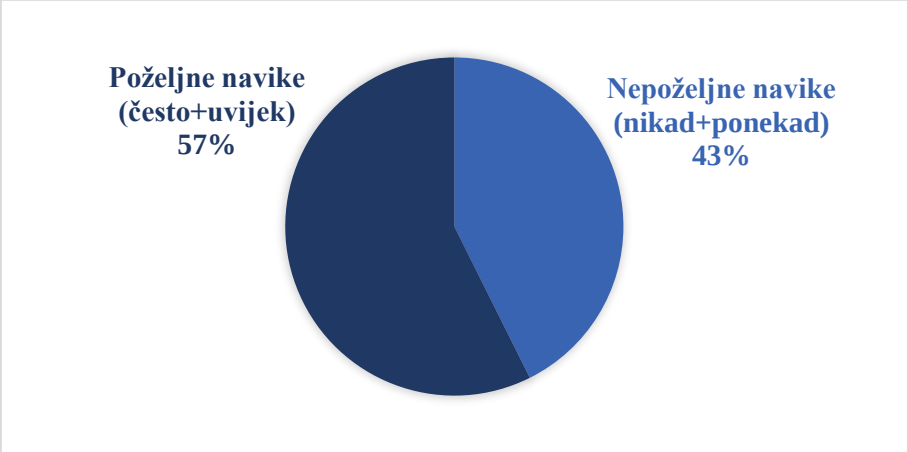



Izvor: Autorica

Iz grafikona je vidljivo da 53% osoba (91 ispitanika) ima poželjne navike za provjeravanje pošiljatelja maila prije nego što otvori priloženi link, a 47% osoba (89 ispitanika) nepoželjne navike.

**b) „ažurirate operativni sustav odmah kad Vam sustav pruža tu mogućnost.“**

Grafikon 24. Ažuriranje operativnog sustava

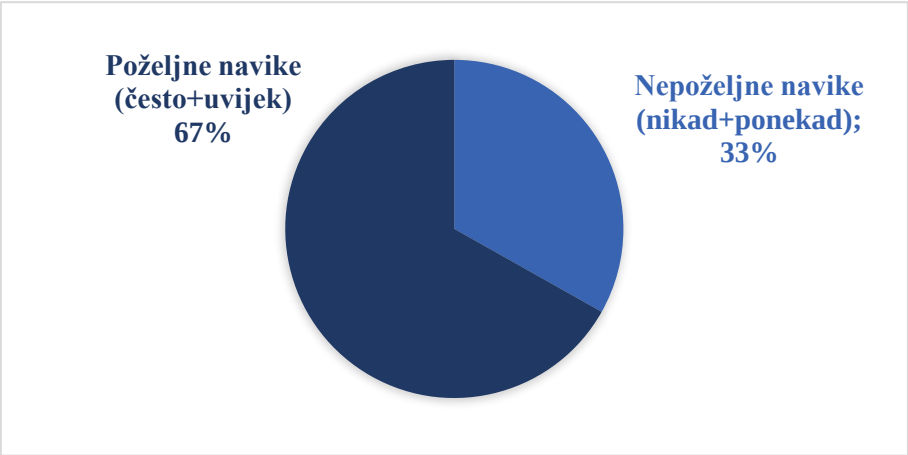



Izvor: Autorica

Iz grafikona je vidljivo da 57% osoba (109 ispitanika) ima poželjne navike za ažuriranje operativnog sustava, a 43% osoba (81 ispitanika) nepoželjne navike.

**c) „obraćate pažnju na pravopis i gramatiku dobivenog maila.“**

Grafikon 25. Pravopis i gramatika

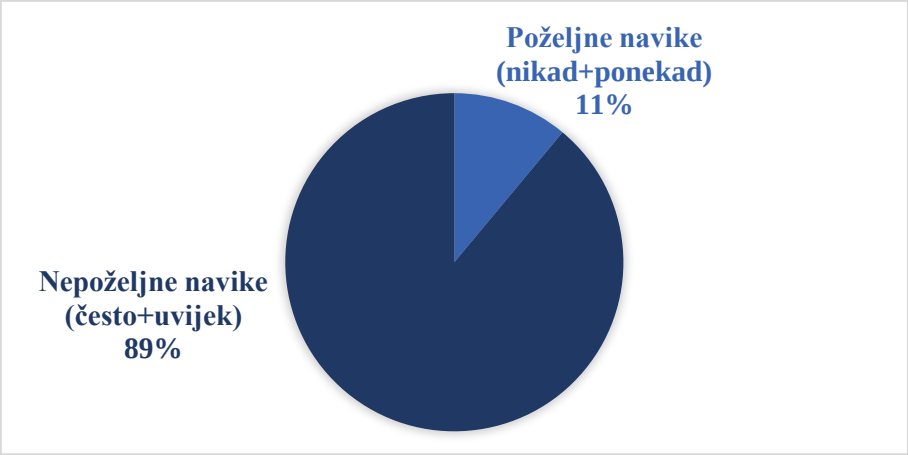



Izvor: Autorica

Iz grafikona je vidljivo da 67% osoba (127 ispitanika) ima poželjne navike za provjeravanje pravopisa i gramatike, a 33% osoba (63 ispitanika) nepoželjne navike.

**d) „pratite stanje Vaših računa za obavljanje novčanih transakcija."**

Grafikon 26. Praćenje stanja novčanih računa

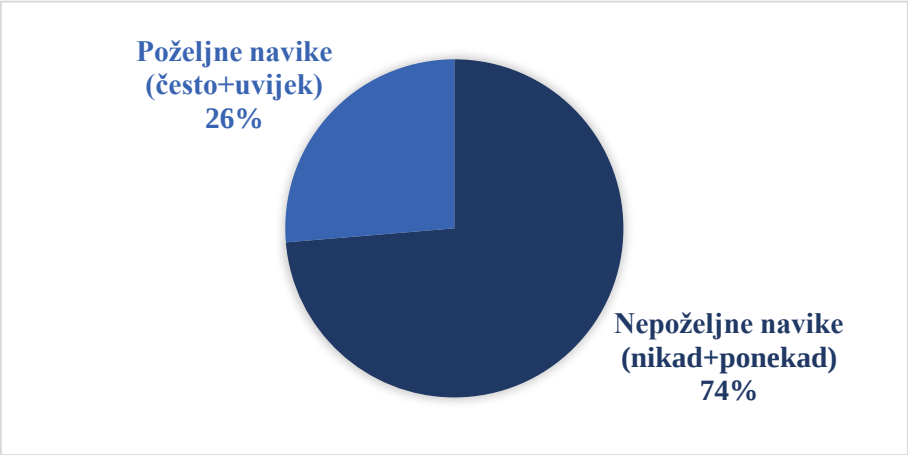



Izvor: Autorica

Iz grafikona je vidljivo da 11% osoba (21 ispitanika) ima poželjne navike za praćenje stanja novčanih računa, a 89% osoba (169 ispitanika) nepoželjne navike.

**e) „pratite informacije o *phishing* napadima.“**

Grafikon 27. Informacije o napadima

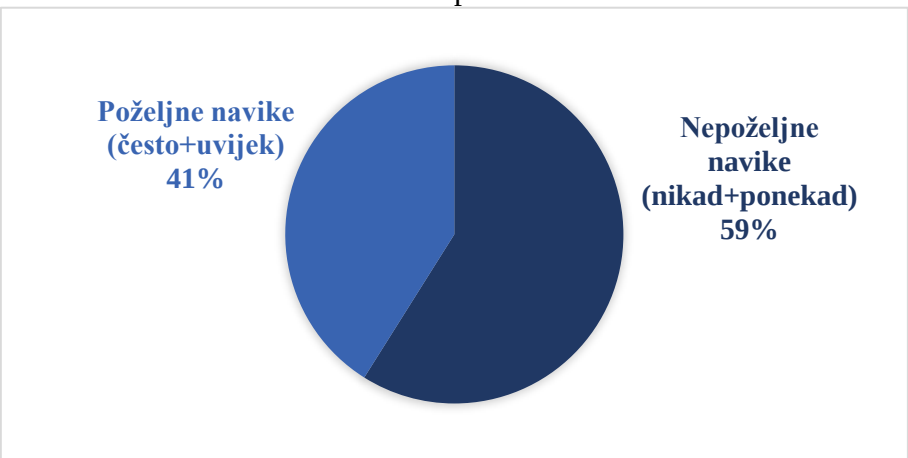



Izvor: Autorica

Iz grafikona je vidljivo da 26% osoba (50 ispitanika) ima poželjne navike za praćenje informacija o *phishing* napadima, a 74% osoba (140 ispitanika) nepoželjne navike.

**f) „provjeravate koristi li *web*-stranica preko koje unosite povjerljive podatke HTTPS protokol (da stranica počinje s https:// umjesto http://).“**

Grafikon 28. HTTPS protokol *web*-stranice

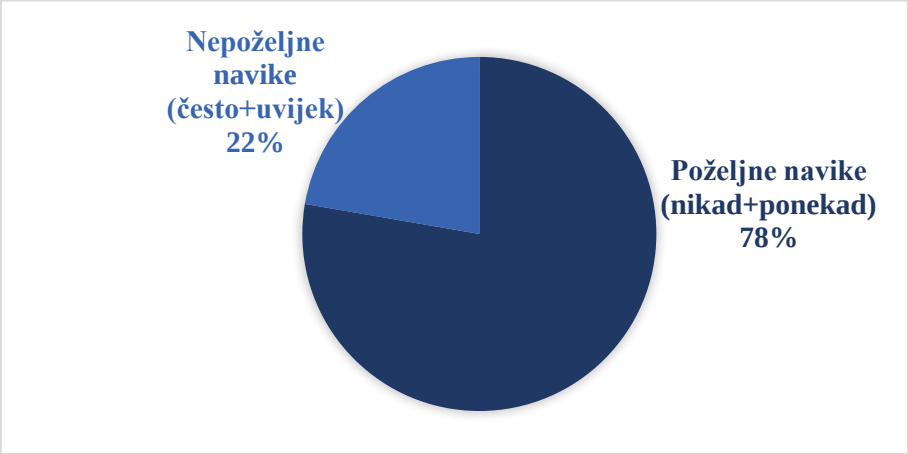



Izvor: Autorica

Iz grafikona je vidljivo da 41% osoba (78 ispitanika) ima poželjne navike za provjeravanje HTTPS protokola *web*-stranice, a 59% osoba (112 ispitanika) nepoželjne navike.

**g) spremate svoje podatke za prijavu kada koristite *web* preglednik;**

Grafikon 29. Spremanje podataka

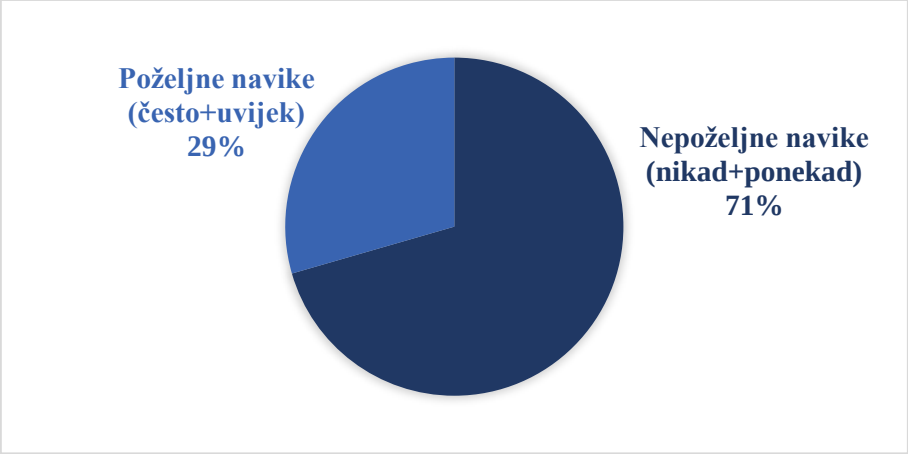



Izvor: Autorica

Iz grafikona je vidljivo da 22% osoba (43 ispitanika) ima poželjne navike za spremanje svojih podataka, a 78% osoba (147 ispitanika) nepoželjne navike.

**h) „mijenjate lozinke.“**

Grafikon 30. Mijenjanje lozinki

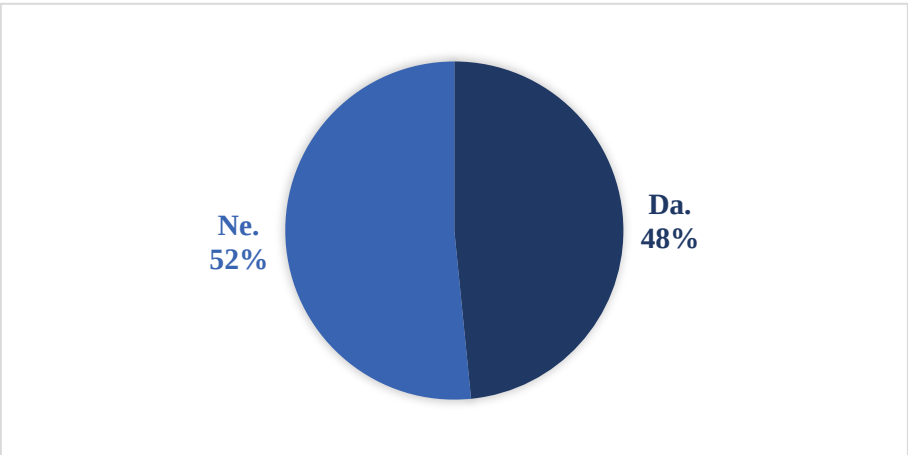



Izvor: Autorica

Iz grafikona je vidljivo da 29% osoba (56 ispitanika) ima poželjne navike za mijenjanje lozinke, a 71% osoba (134 ispitanika) nepoželjne navike.

**Pitanje pod brojem 17 glasi: „Koristite li iste lozinke na više različitih online mjesta (mail, društvene mreže, ulazak u kompjuter, pristup bankovnim računima i slično)?“**

Grafikon 31. Iste lozinke



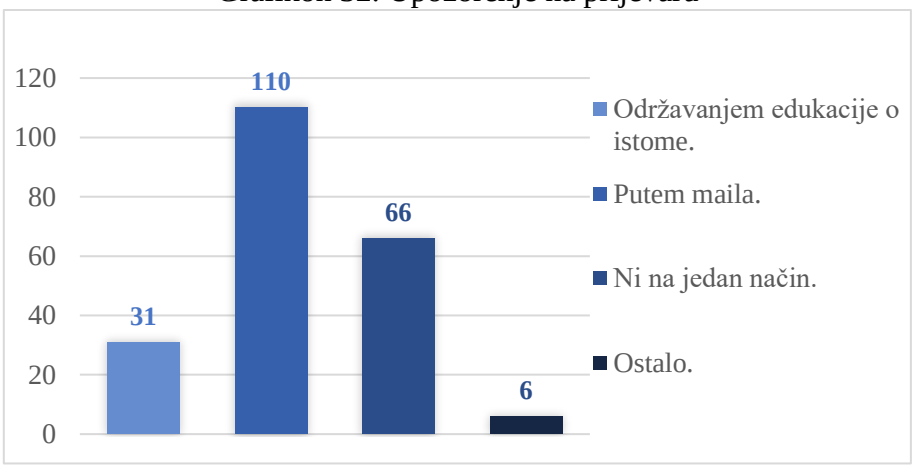

Izvor: Autorica

Iz grafikona je vidljivo da 48% osoba (92 ispitanika) koristi iste lozinke za više različitih online mjesta, a 52% osoba (98 ispitanika) ne.

### 6.1.4. Edukacija i savjesnost

**Pitanje pod brojem 18 glasi: „Je li Vaša organizacija na neki od sljedećih načina Vas upozorila na *phishing* prijevaru?“**

Grafikon 32. Upozorenje na prijevaru

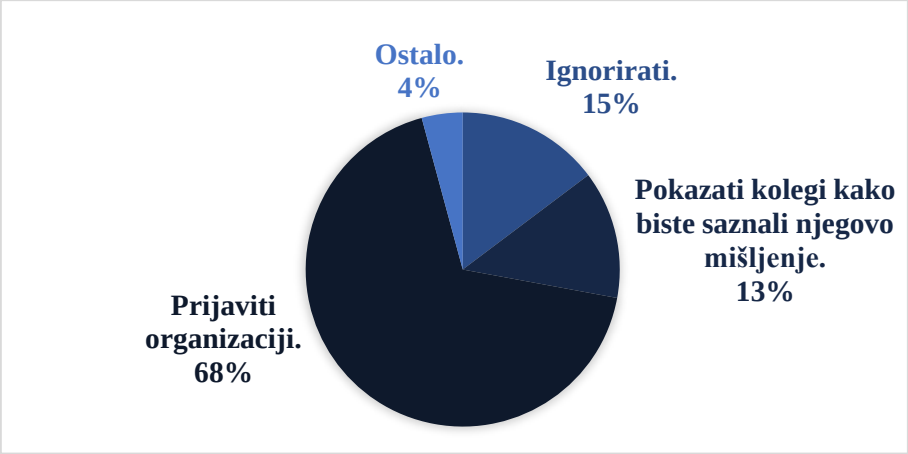



Izvor: Autorica

Iz grafikona je vidljivo da 31 ispitanik je odslušao edukaciju o *phishing* napadu, 110 ispitanika putem maila, a 66 ispitanika ni na jedan način.

**Pitanje pod brojem 19 glasi: „ Što ćete kao zaposlenik učiniti ukoliko sumnjate da ste dobili *phishing* poruku putem elektroničke pošte?“** prema Cisco, 2022.

Grafikon 33. Sumnja na poruku

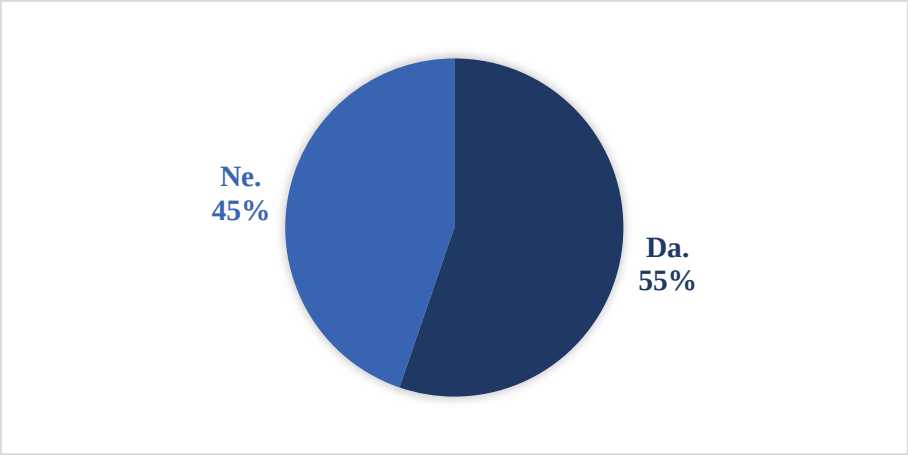



Izvor: Autorica

Iz grafikona je vidljivo da 68% osoba (129 ispitanika) prijavila bi organizaciji sumnjivu poruku, 15% osoba (28 ispitanika) ignorirala bi, 13% osoba (25 ispitanika) pokazala bi kolegi, a 4% osoba (8 ispitanika) učinila bi nešto drugo.

**Pitanje pod brojem 21 glasi: „ Biste li željeli odslušati predavanje o *phishing* prijevarama?“**

Grafikon 34. Slušanje predavanja

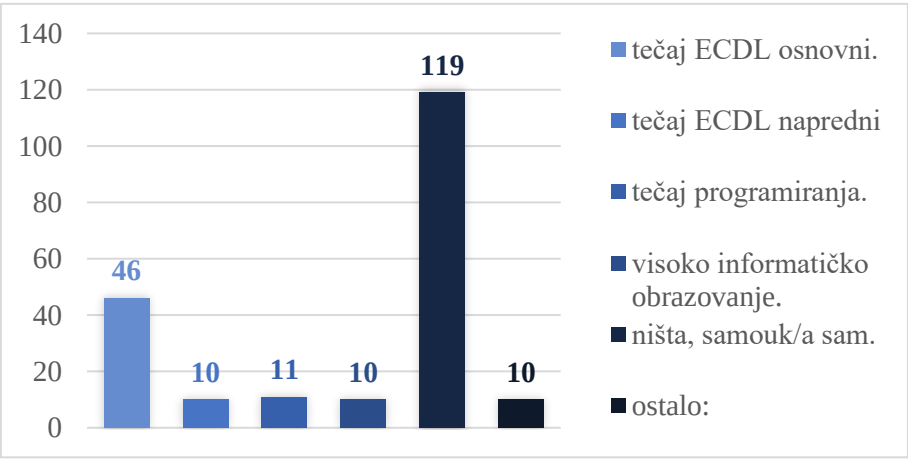



Izvor: Autorica

Iz grafikona je vidljivo da 55% osoba (105 ispitanika) želi odslušati predavanje o *phishing* napadima, a 45% osoba (85 Ispitanika) ne.

**Pitanje pod brojem 21 glasi: „ Pohađao/la sam sljedeće:“ Na to pitanje ispitanici su mogli izabrati više ponuđenih odgovora.**

Grafikon 35. Informatički tečajevi

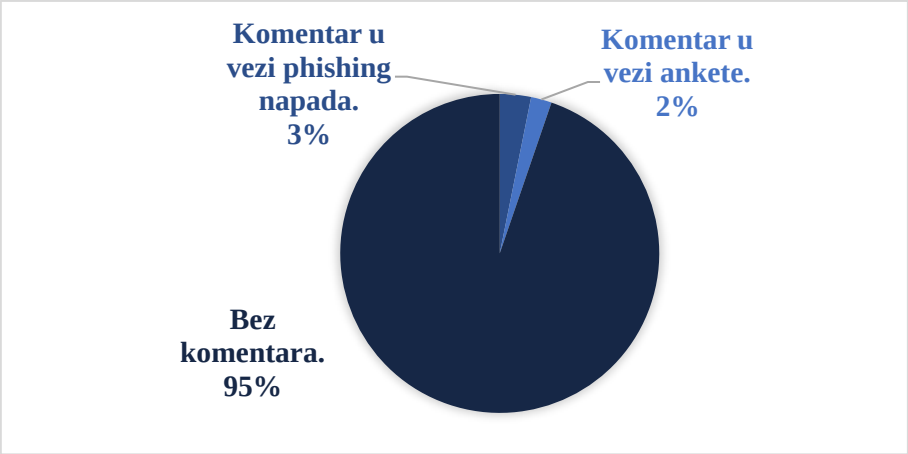



Izvor: Autorica

Iz grafikona je vidljivo da  samo 10 ispitanika ima visoko informatičko obrazovanje, a samouko je 119 ispitanika.

**Pitanje pod brojem 22 glasi: „Ukoliko imate bilo kakvu kritiku, sugestiju, savjet u vezi s ovom anketom ili u vezi *phishing* napada, molim Vas upišite ovdje:**“

Grafikon 36. Komentari




Izvor: Autorica

Iz grafikona je vidljivo da 2% osoba (4 ispitanika) komentiralo samo anketu,  3% osoba (6 ispitanika) komentiralo *phishing* napad, a 95% osoba (180 ispitanika) je bez komentara. Dobiveni komentari ne utječu na rezultate istraživanje.

## 6.2. Rezultati istraživanja

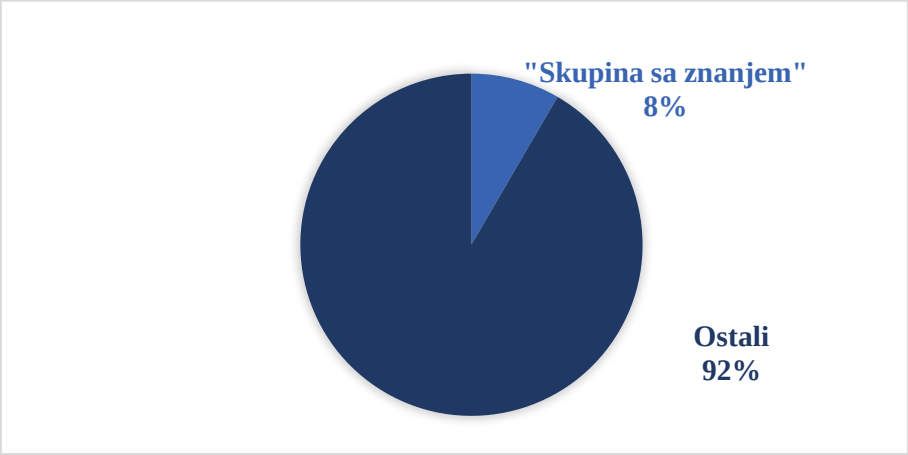
Anketa je razvrstana u četiri osnovna dijela:

1. demografski podatci: pitanja pod rednim brojem 1, 2, 3 i 4 što čini ukupno 4 pitanja,
2. znanje iz područja *phishinga*: pitanja pod rednim brojem 5, 6, 7, 8, 9, 10, 11, 12, 13 (s 4 potpitanja), 14 i 15 (s 4 potpitanja) što čini ukupno 17 pitanja,

3. navike kojima se povećava nivo informatičke sigurnosti: 4 stupnja učestalosti od kojih se „nikad“ i „ponekad“ svrstani u nepoželjne navike, a „često“ i „uvijek“ u poželjne navike, osim kod potpitanja „spremate svoje podatke za prijavu kada koristite *web* preglednik“ gdje su navike suprotno svrstane; pitanja pod rednim brojem 16 (sa 8 potpitanja) i 17 što čini ukupno 9 pitanja,
4. edukacija i savjesnost: pitanja pod rednim brojem 18, 19, 20 i 21 što čini ukupno 4 pitanja.

Većina osoba u anketi ima 3 i više grešaka u neprepoznavanju phishing prijevara i znanja o istome. Cijeli točan test je riješila samo jedna osoba, s jednom greškom također samo jedna, a s dvije greške 14 osoba. Dakle, radi se o 16 osoba koja su točno riješili test, dok 174 osobe nije prepoznalo phishing. Izraženo u postotku 8% prepoznaje takve napade, što je zabrinjavajući podatak prema grafikonu 36.

Grafikon 37. Prepoznavanje *phishinga*




Izvor: Autorica

Po dobnoj skupini svrstani su ispitanici u tri kategorije:

- mlađu skupinu (do 39. godine života) sačinjava 34% osoba (64 ispitanika),
- zrelu skupinu (od 40. do 59. godine života) sačinjava 54% osoba (103 ispitanika),
- staru skupinu (60 godina i više) sačinjava 12% osoba (23 ispitanika).

Od 17 pitanja znanja određena je aritmetička sredina po postotku točnosti rješenja i dobiveni su sljedeći rezultati:

- mlađa skupina ima prosječan rezultat testa znanja 74% (najbolji rezultati),
- zrela skupina ima prosječan rezultat testa znanja 63%,
- stara skupina ima prosječan rezultat testa znanja 51%.

# 7. Zaštita poslovnih organizacija od *phishing* napada

Pretpostavka je da se u tijeku godine poduzeća s relativno dobrim poslovanjem suočavaju sa stotinama e-mail *phishing* napadima što predstavlja veliku potencijalnu kibernetičku opasnost. Da bi se to svelo na minimum potrebno je u okviru politike kibernetičke sigurnosti staviti poseban naglasak na zaštitu elektroničke pošte. Pogotovo u današnje vrijeme kada je to glavni medij za provođenje zlonamjernih aktivnosti usmjerenih prema poduzećima (xorlab AG, 2022.).

Za prevenciju i otkrivanje *phishing* napada organizacije svoje napore trebaju orijentirati u sljedeća dva ključna područja: tehničku zaštitu i edukaciju zaposlenika. Oba pristupa neophodno je primjenjivati jer ni jedan pristup sam po sebi nije dovoljan. Zbog toga što ni svaki obrambeni sustav ne može uvijek prepoznati prijetnju te je i blokirati, a obučeni zaposlenici ponekad ne mogu prepoznati nelegitiman mail (xorlab AG, 2022.).

## 7.1. Tehnička zaštita

Tehnička zaštita na razini poslovnih organizacija odnosi se na:

- uvođenje antivirusne zaštite, programa vatrozida i filtra za neželjenu poštu koji djeluje kao antivirusni sustav unutar pristigle pošte, što znači da detektira e-poštu sa zlonamjernim poveznicama, privitcima ili općenito neželjenom poštom (Bartram, n.d.; Helilxtstorm, n.d.),
- planiranje i redovito provođenje ažuriranja koje se preporučuje za sigurnosni softver, operativne sustave, internet preglednike i aplikacije što je nužan preduvjet za postizanje zadovoljavajućeg stupnja sigurnosti (Helilxstorm, n.d.; CERT.hr u suradnji s LS&S, 2015.),

- planiranje i redovito mijenjanje lozinke, primjerice svakih 60 dana uz definiranje i pridržavanje pravila koja se odnose na sadržaj lozinke poput minimalne duljine, brojeva, simbola i slično, (Helilxstorm, n.d.),
- planiranje i konstantnu provedbu sigurnosnog kopiranja podataka, a ako to nije moguće učiniti sa svim datotekama potrebno je selektirati one najkritičnije (Helilxstorm, n.d.; Lider media, 2016.),
- uvođenje višefaktorske provjere autentičnosti za prijavu zaposlenika na račune tvrtke (Helilxstorm, n.d.),
- korištenje SMTP (engl. *Simple Message Transfer Protocol*), komunikacijskog protokola za zaštitu od *ransomwarea* za krađu identiteta, sigurnosti ulazne e-pošte i hiperveza na zlonamjerne *web*-stranice koje se šalju putem *phishing* poruka e-pošte (Concept Phones, 2022.; CERT.hr, 2006.),
- korištenje virtualne privatne mreže (skraćenica VPN) i uključivanje radnika koji rade od kuće (Concept Phones, 2022.; Helilxstorm, n.d.).

## 7.2. Edukacija zaposlenika

Obuka zaposlenika treba se sastojati od aktivnosti upoznavanja sa znakovima zlonamjernih e-mailova te ukoliko sumnjaju da su zaprimili takvu, istu proslijede informatičkom odijelu unutar firme (Helilxstorm, n.d.). Najbolje bi bilo da firme imaju internu adresu čija bi jedina svrha bila zaprimanje prijava potencijalnih napada te će tako imati uvid u sve pokušaje zaobilaženja tehničkih mjera (Hill Country Tech Guys, n.d.).

Osim obuke radnika, poželjno je i provođenje povremenog testiranja istih slanjem e-poruka koje imaju elemente pokušaje krađe identiteta što je najbolji pokazatelj na čemu je potrebno dodatno poraditi u samoj edukaciji (Hill Country Tech Guys, n.d.).

### 7.2.1. Provjera dobivenog maila

Zaposlenici nakon što zaprime elektroničku poruku trebali bi obratiti pažnju na sljedeće stavke:

- adresu pošiljatelja, npr. pošiljatelj se predstavlja kao firma eBay, a adresa je ebay@online-ducani.eu umjesto „@ebay.com“, (Šokić, 2021.),
- naslov e-poruke koji izgleda kao „HITNO“, „VAŽNO“, „UPOZORENJE“ i slično što vjerojatno upućuje na *phsihing* prijevaru, (Šokić, 2021.),
- način obraćanja primatelju, ako je općenitog (generičkog) tipa (primjerice „Dragi korisniče…“) automatski je pokazatelj da se radi o *phishing* napadu (CERT.hr, n.d.),
- pravopisne i gramatičke pogreške, premda u posljednje vrijeme gramatički ispravan mail u cijelosti ne može se smatrati legitimnim, (Šokić, 2021),
- sadržaj maila, poput dobitka mobitela i drugih nagrada ili zahtjev za promjenu lozinke ako to niste tražili ukazuje na pokušaj krađe identiteta kao i potražnja iznimno puno osobnih podataka jer legitimne organizacije većinom ne traže osobne podatke od korisnika putem elektroničke pošte (Šokić, 2021.; Helilxstorm, n.d.).

### 7.2.2. Postupci kada sumnjate na e-mail *phishing*

Ukoliko djelatnici nisu sigurni trebaju li pratiti upute dobivenog maila nakon provedene provjere potrebno je da učine navedene korake:

- za pristiglu hipervezu potrebno je preći mišem iznad iste kako bi se pokazao stvarni URL kojem ćete pristupiti nakon što kliknete na nju. Ona može biti potpuno ili djelomično drugačija od legitimne, primjerice www.bankofarnerica.com umjesto slova „m“ napisana su slova „r“ i „n“ (Phishing.org, n.d.). Također može se otvoriti novi prozor internetskog preglednika i upisati URL u adresnu traku (Helilxstorm, n.d.),

- za stranicu preko koje se unose povjerljivi podatci potrebno je provjeriti HTTPS protokol, odnosno da stranica počinje s https:// umjesto http:// (CERT.hr, n.d.), premda ni to nije uvijek pokazatelj te je potrebno provjeriti i cijeli URL (Imperva, 2021.),
- ne otvarati pristigle privitke posebno one koje imaju nastavke .exe, .jar, .bat, .cmd i .vbs pa ni one koje vode na dokumente u sustav Miscrosoft Office. Prva skupina su iznimno opasne datoteke te se nikako ne smiju preuzimati, a što se tiče druge ako se to i učini, ništa se neće dogoditi dok se ne klikne na „omogući sadržaj“ ili *enable editing*. (CERT.hr, n.d., 18. 6. 2022.; Bartram, n.d.). Donedavno se jedino sigurnom datotekom smatrala tekstualna datoteka (datoteka s nastavkom .txt), ali to više nije slučaj (Aver, 2021.).

# 8. Zaključak

Rezultati rada su u skladu s ciljem rada jer je dokazano da većina ispitanika koji svakodnevno koriste računalo nisu upoznati s s *phishing* prijevarama, odnosno ne percipiraju znakove i obilježja koju upućuju na takve prijevare. Njih preko 90% ne bi prošli tzv. pitanja znanja. Uz to ni sve navike koje pridonose nivou informatičke sigurnosti nisu zadovoljavajuće.

Najbolje rezultate u testu znanja je postigla mlađa skupina, što se može povezati s boljim poznavanjem informacijsko-komunikacijske tehnologije i prepoznavanjem *phishing* prijevara. Premali je uzorak onih koji su odslušali predavanje o *phishing* prijevarama (31 ispitanik) da bi se to moglo staviti u korelaciju s prepoznavanjem *phishing* prijevarama i poželjnijim navikama. Osim toga, premali je uzorak ispitanika s visokim informatičkim obrazovanjem (10 ispitanika) da bi se to moglo staviti u korelaciju s boljem prepoznavanjem *phishing* prijevara i poželjnijim navikama.

Nažalost, ono što je poslodavac aktivno učinio u odnosu na zaposlenike u anketi (edukacija na temu *phishing* napada) je zanemarivo gledajući cijeli anketni uzorak (16%). Tako „loši“ rezultati po poznavanju *phishing* prijevara od strane zaposlenika nisu neočekivani. U ispitivanom uzorku, manje od 6% osoba (visoko informatičko obrazovanje) može se smatrati u potpunosti spremno i obučeno da se nose sa svakodnevnim izazovima *phishing* prijevara. Od osoba koje nemaju visoko informatičko obrazovanje ne može se očekivati da mogu biti zaštitni faktor koji može odgovoriti na *phishing* prijevare jer one postaju svakim danom sofisticiranije i složenije. Uz to i sam poslodavac ne prepoznaje navedene potencijalne opasnosti i ne poduzima aktivne mjere kojim bi podigao nivo informatičke zaštite. Sama svjesnost ispitanika o *phishing* napadima i njihovom „znanju“ je također na niskom nivou jer tek nešto više od polovice ispitanika su zainteresirane za predavanja na navedenu temu.

*Phishing* napadi su u trendu, to je i najjednostavniji i najjeftiniji način za cyber kriminalce da u kratkom vremenskom razdoblju dođu do znatne materijalne koristi. Kod *phishing* „napada“ dva su oblika zaštite ključni, tehnički i ljudski. Tehnički oblik zaštite je najčešće u obliku instaliranja moćnog antivirusnog softvera uz tehničku podršku profesionalnog davaoca usluga. Druga razina je ljudski faktor. Otprilike 99% *phishing* napada oslanja se na ljudsku pogrešku za prodor u sustave. Nedostatak svijesti o *phishing* napadima, zatim nemarnost i nedostatak znanja su tri točke zbog kojih se upada u zamku krađe identiteta. Ljudski faktor je vrlo promjenjiva varijabla koja najprije treba imati svijest o navedenim napadima, zatim odgovornost i na kraju potreban nivo znanja da isti prepoznaju. Vidjelo se i u ovom istraživanju kako je sama svijest i odgovornost nisu previše razvijeni (gotovo polovina smatra da znaju prepoznati *phishing* napade, a predavanja bi slušalo tek nešto više od polovice). Pokazano znanje je još na nižem nivou. Jedini način za unapređenje ljudskog faktora je trajna edukacija i proaktivni odnos od strane poslodavca prema zaposlenicima u informatički sve zahtjevnijim vremenima.

Prilog 1. Anketa

**Istraživanje o prepoznavanju e-mail phishinga u poslovnim organizacijama**

Dobar dan!

Anketa se provodi u okviru izrade specijalističkog završnog rada „Istraživanje o prepoznavanju e-mail phishinga u poslovnim organizacijama".

Ova anketa je anonimna.

1 Spol:

- ○ ženskog
- ○ muškog

2 Koliko imate godina?

- ○ do 20
- ○ 20 – 29
- ○ 30 – 39
- ○ 40 – 49
- ○ 50 – 59
- ○ 60 i više

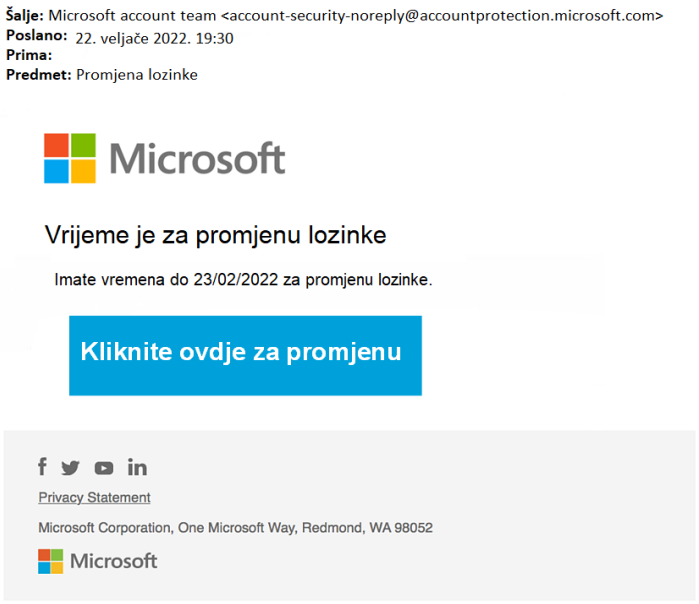
3 Vaše obrazovanje:.

- ○ osnovna škola.
- ○ srednja škola.
- ○ viša škola ili fakultet.
- ○ magisterij ili doktorat.

4 Smatrate li da znate prepoznati phishing prijevaru?

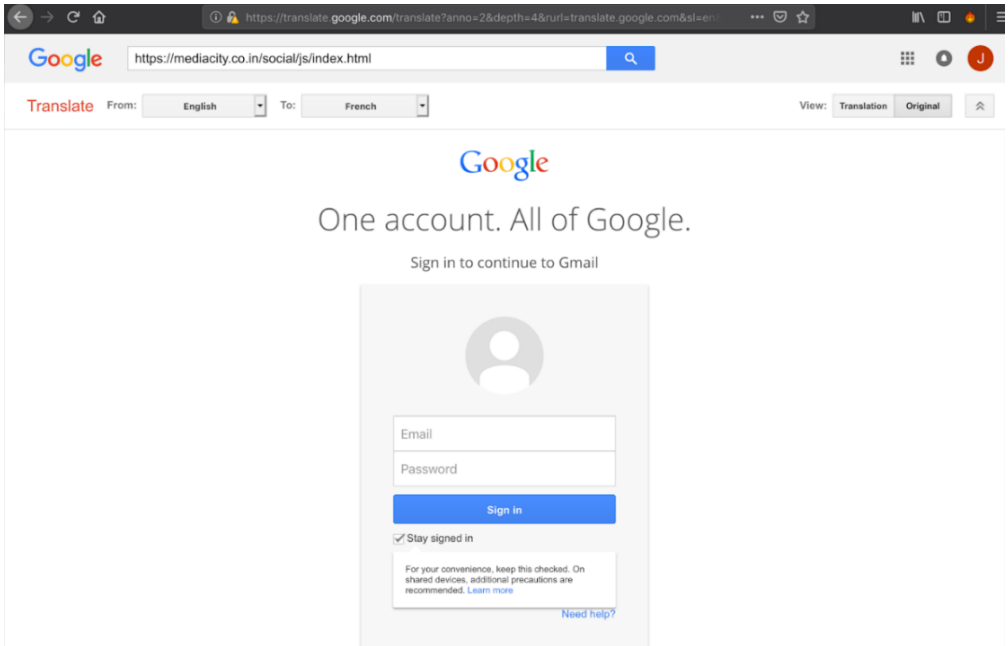
- ○ Da.
- ○ Ne.
- ○ Nisam siguran/a.

5 Biste li pratili upute sljedećeg maila?




- ◯ Da.
- ◯ Ne.

6 Biste li se prijavili na sljedećoj stranici?




- ◯ Da.
- ◯ Ne.

7 Banka Vam šalje e-mail u kojem kaže da ukoliko odmah ne ažurirate osobne podatke da će Vam račun biti obustavljen, Vi ćete odgovoriti na takvu poruku: *

- ○ Da.
- ○ Ne.

8 Biste li pratili upute sljedećeg maila:

**From:** workplacegiving@good2give.ngo <workplacegiving@good2give.ngo>
**Sent:** Friday, 23 August 2019 2:11 PM
**To:**jane_doe@gmail.com
**Subject:** Good2Give password reset request


Hi Jane,

You have requested to reset your Good2Give password. To do this, simply click on the link below:

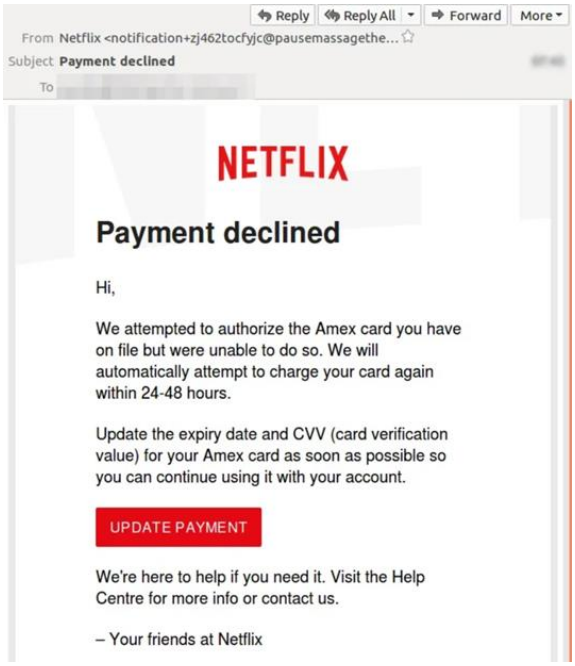
**Reset password**

Happy giving!

The Good2Give Team
Good2Give | Ground Floor, 12 Holtermann Street, Crows Nest NSW 2065
www.good2give.ngo

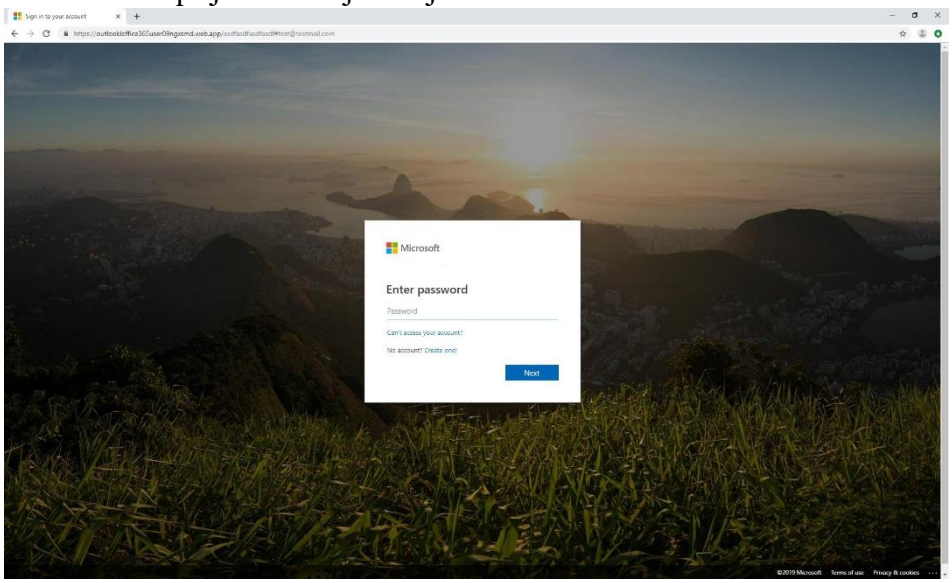
- ○ Da.
- ○ Ne.

9 Biste li pratili upute sljedećeg maila:



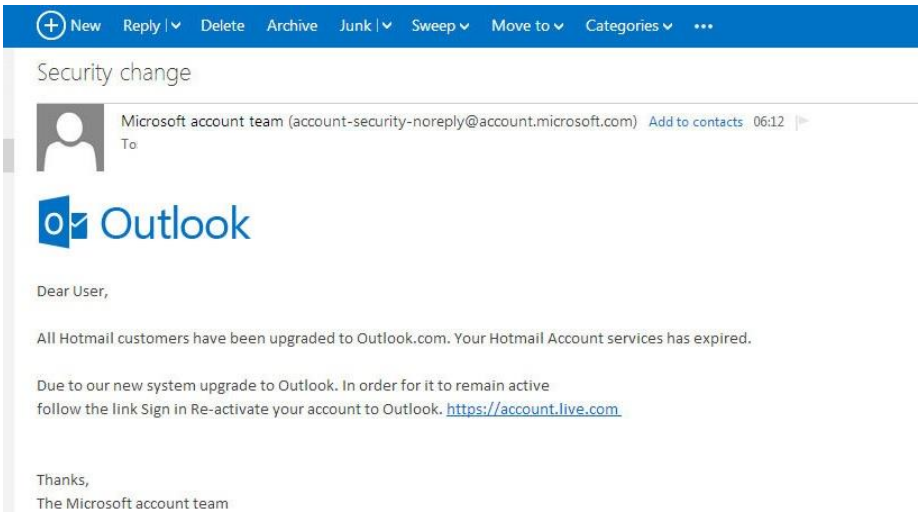

- ○ Da.
- ○ Ne.

10 Biste li se prijavili na sljedećoj web-stranici:.




- ○ Da.
- ○ Ne.

11 Biste li pratili upute sljedećeg maila?




- Da.
- Ne.

12 Dobili ste e-mail od šefa koji od Vas hitno traži da pošaljete svoje ime i prezime te broj korisničkog računa kako bi Vam mogao isplatiti plaću za ovaj mjesec. Mail ste dobili nekoliko dana prije isplate plaće. Vi ćete učiniti sljedeće: Molim izaberite **samo jedan** od ponuđenih odgovora.

- odmah ćete odgovoriti na takav mail.
- nećete odgovoriti na poruku dok ne provjerite je li Vaš kolega odgovorio na istu poruku.
- ukoliko je u mailu ostavljen broj mobitela šefovog ureda, nazvat ćete ga i na taj način mu ostaviti tražene podatke jer je to najsigurnije.
- ignorirat ćete poruku.

13 Znakovi phishing prijevara su:

| | Da. | Ne. | Nisam siguran/a. |
|---|---|---|---|
| potreban je hitan odgovor. | ○ | ○ | ○ |
| generički pozdrav upućen primatelju (npr. Dragi korisniče). | ○ | ○ | ○ |
| pravopisne i gramatičke pogreške. | ○ | ○ | ○ |
| mail čiji sadržaj Vas obavještava o zatvaranju ili brisanju korisničkog računa. | ○ | ○ | ○ |

14 Kako ćete postupiti u slučaju da postanete žrtva phishing napada? Molim izaberite samo jedan od ponuđenih odgovora.

○ Ugasiti računalo. To će Vas riješiti svakog virusa.

○ Promijeniti sve ugrožene lozinke.

○ Izbrisati phishing mail.

15 Sljedeće aktivnosti sprječavaju phishing napad ili ne dovode u opasnost:

| | Da. | Ne. | Nisam siguran/a. |
|---|---|---|---|
| redovito ažuriranje operativnog sustava. | ○ | ○ | ○ |
| klikanje na omogući sadržaj/enable editing u dokumentima sustava Microsoft Office. | ○ | ○ | ○ |
| otvaranje tekstualne datoteke (datoteka s nastavkom .txt). | ○ | ○ | ○ |
| slanje podatka o PIN-u bankovne kartice, samo ako to traži Vaša matična banka. | ○ | ○ | ○ |

16 Na skali od 1 do 4 koliko često provodite sljedeće aktivnosti:

| | (1) nikad | (2) ponekad | (3) često | (4) uvijek |
|---|---|---|---|---|
| provjeravate je li uistinu pošiljatelj maila onaj za koji se predstavlja prije nego što otvorite priloženi link (ili poveznicu) | ○ | ○ | ○ | ○ |

| | | | | |
|---|---|---|---|---|
| ažurirate operativni sustav odmah kad Vam sustav pruža tu mogućnost. | ○ | ○ | ○ | ○ |
| obraćate pažnju na pravopis i gramatiku dobivenog maila. | ○ | ○ | ○ | ○ |
| pratite stanje Vaših računa za obavljanje novčanih transakcija. | ○ | ○ | ○ | ○ |
| pratite informacije o phishing napadima. | ○ | ○ | ○ | ○ |
| provjeravate koristi li web-stranica preko koje unosite povjerljive podatke HTTPS protokol (da stranica počinje s https:// umjesto http://). | ○ | ○ | ○ | ○ |
| spremate svoje podatke za prijavu kada koristite web preglednik. | ○ | ○ | ○ | ○ |
| mijenjate lozinke. | ○ | ○ | ○ | ○ |

17 Koristite li iste lozinke na više različitih online mjesta (mail, društvene mreže, ulazak u kompjuter, pristup bankovnim računima i slično)?

○ Da.

○ Ne.

18 Je li Vaša organizacija na neki od sljedećih načina Vas upozorila na phishing prijevaru?

Možete izabrati **više** odgovora

☐ Održavanjem edukacije o istome.

☐ Putem maila.

☐ Ni na jedan način.

☐ Ostalo: _____

19 Što ćete kao zaposlenik učiniti ukoliko sumnjate da ste dobili phishing poruku putem elektroničke pošte?

- ○ Ignorirati.
- ○ Pokazati kolegi kako biste saznali njegovo mišljenje.
- ○ Prijaviti organizaciji.
- ○ Ostalo: _____

20 Biste li željeli odslušati predavanje o phishing prijevarama?

- ○ Da.
- ○ Ne.

21 Pohađao/la sam sljedeće:

Možete izabrati **više** odgovora

- ☐ tečaj ECDL osnovni.
- ☐ tečaj ECDL napredni.
- ☐ tečaj programiranja.
- ☐ visoko informatičko obrazovanje.
- ☐ ništa, samouk/a sam.
- ☐ Ostalo: _____

22 Ukoliko imate bilo kakvu kritiku, sugestiju, savjet u vezi s ovom anketom ili u vezi phishing napada, molim Vas upišite ovdje

Molimo unesite svoj odgovor ovdje:

_____
_____

**Hvala Vam što ste izdvojili dio svog dragocjenog vremena i ispunili ovaj anketni upitnik.**

## Popis literature


Natuknica u enciklopediji, leksikonu, rječniku

Anić, V. et al., Natuknica **anketa**, Hrvatski enciklopedijski rječnik, drugo izdanje, EPH d.o.o. Zagreb i Novi Liber d.o.o. Zagreb, Zagreb, 2004., svezak 1., str. 119.

Članak na *web*-stranici (autor teksta nepoznat)

CARNet CERT i LS&S, Phishing napadi, CCERT, 2005., https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2005-01-106.pdf (18. 6. 2022.)

CCERT, Godišnji izvještaj nacionalnog CERT-a za 2021. godinu, CCERT, 2021., https://www.cert.hr/wp-content/uploads/2022/03/CERT-godisnje-izvjesce-2021.pdf (18. 6. 2022.)

Internetski izvori (autor teksta poznat)

Alkhalil et al., Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers Media S.A., 2021., https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full (18. 6. 2022.)

Aver, H., Are text files safe?, Kaspersky, 2021., https://www.kaspersky.com/blog/is-txt-file-safe/39256/ (18. 6. 2022.)

Balen, V., Nepoznati počinitelji korištenjem phishing e-poruke iz tvrtke izvukli stotine tisuća, Večernji list, 2022., https://www.vecernji.hr/vijesti/prevarant-e-porukom-iz-tvrtke-izvukao-vise-stotina-tisuca-kuna-policija-upozorava-na-takve-prijevare-1561708 (18. 6. 2022.)

Bartram, M., Top 6 Ways to Protect Businesses from Phishing Attacks, Telstra Ventures, n.d., https://telstraventures.com/ways-to-protect-businesses-from-phishing-attacks/ (18. 6. 2022.)

Doevan J., Ukloni CryptoLocker (Vodič za uklanjanje) - ažurirano srp 2019, Virusi.hr, 2019., https://virusi.hr/cryptolocker/ (18. 6. 2022.)

Fruhlinger, J., What is phishing? Examples, types, and techniques, CSO, 2022., https://www.csoonline.com/article/2117843/what-is-phishing-examples-types-and-techniques.html (18. 6. 2022.)

Marijanović, N., Upozorenje o povećanoj phishing aktivnosti, Sveučilište Sjever, 2022., https://www.unin.hr/2022/03/upozorenje-o-povecanoj-phishing-aktivnosti-2/ (18. 6. 2022.)

Murillo, K., Upozorenje o povećanoj phishing aktivnosti, Master DC, 2019., https://www.masterdc.com/blog/what-is-angler-phishing/ (18. 6. 2022.).

Petrić, I. , Phishing napadi – koje sve vrste postoje i kako ih prepoznati?, Duplico IT, 2021., https://duplico.io/phishing-napadi-koje-sve-vrste-postoje-i-kako-ih-prepoznati/ (18. 6. 2022.)

Samec, B., Policija upozorila građane na internetske prijevare tzv. phishing kampanje, Sesvete Danas, 2020., https://www.sesvete-danas.hr/hrvatska-i-svijet/zagreb/policija-upozorila-gradane-na-internetske-prijevare-tzv-phishing-kampanje-11500 (18. 6. 2022.)

Stone, K, What is VoIP? Voice Over Internet Protocol Explained, GetVoIP, 2022., https://getvoip.com/library/what-is-voip/ (18. 6. 2022.)

Sullivan, P., DEFINITION Computer Emergency Response Team (CERT), TechTarget, 2021., https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team, (18. 6. 2022.)

Šokić, T., Kako prepoznati e-mail prijevaru (phishing)?, Csi.hr, 2021., https://csi.hr/2021/04/29/kako-prepoznati-e-mail-prijevaru-phishing-2/ (18. 6. 2022.)

Unuth, N., Objašnjen je ID pozivatelja, eYewated,, https://hr.eyewated.com/objasnjen-je-id-pozivatelja/ (18. 6. 2022.).

Vrbanus, S., Nova phishing kampanja u Hrvatskoj, ovoga puta cilja učitelje, Bug.hr, 2022., https://www.bug.hr/sigurnost/nova-phishing-kampanja-u-hrvatskoj-ovoga-puta-cilja-ucitelje-25193 (18. 6. 2022.)

Vrbanus, S., U Hrvatskoj aktivna phishing kampanja vezana uz COVID-19, Bug.hr, 2020., https://www.bug.hr/sigurnost/u-hrvatskoj-aktivna-phishing-kampanja-vezana-uz-covid-19-16426 (18. 6. 2022.)

Internetski izvori (autor teksta nepoznat)

Australian Cyber Security Centre, Quiz, n.d., https://www.cyber.gov.au/acsc/view-all-content/campaign/know-how-spot-phishing-scam-messages/scam-messages/quiz (18. 6. 2022.)

CanIPhish, The history of phishing, n.d., https://caniphish.com/phishing-resources/history-of-phishing (18. 6. 2022.)

CERT.hr, O nacionalnom CERT-u, n.d., https://www.cert.hr/onama/ (18. 6. 2022.)

CERT.hr, Phishing, n.d., https://www.cert.hr/phishing/ (18. 6. 2022.)

CERT.hr, SMTP protokol, 2006., https://www.cert.hr/NCSMTPpro (18. 6. 2022.))

CERTNZ, Phishing, n.d., https://www.cert.govt.nz/individuals/common-threats/phishing/ (18. 6. 2022.)

Check Point, What is Phishing?, n.d., https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/# (18. 6. 2022.)

CIS, RSA mijenja tokene zabrinutim korisnicima, 2011., https://www.cis.hr/vijesti/vijesti-za-svakoga/1098-rsa-mijenja-tokene-zabrinutim-korisnicima.html (18. 6. 2022.)

Cisco, What Is Phishing?, 2022., https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~phishing-awareness-quiz (18. 6. 2022.)

CyberSecurity & Infrastructure Security Agency, Avoiding Social Engineering and Phishing Attacks, 2020., https://www.cisa.gov/uscert/ncas/tips/ST04-014 (18. 6. 2022.)

CybSafe, How can phishing affect a business?, 2021., https://www.cybsafe.com/community/blog/how-can-phishing-affect-a-business/ (18. 6. 2022.)

Federal Trade Commission, Phishing Quiz, n.d., https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/phishing (18. 6. 2022.)

First Citizens Bank, How Does Phishing Affect a Business?, 2021., https://www.firstcitizens.com/small-business/insights/security/how-does-phishing-affect-a-business (18. 6. 2022.)

FraudWatch, What is the business impact of phishing attack, 2021. https://fraudwatch.com/what-is-the-business-impact-of-a-phishing-attack/ (18. 6. 2022.)

FraudWatch, What is Vishing? Voice Phishing Scams Explained & How to prevent them, 2019. https://fraudwatch.com/what-is-vishing-voice-phishing-scams-explained-how-to-prevent-them/

Government of Canada, The history of phishing, 2021., https://www.getcybersafe.gc.ca/en/resources/history-phishing (18. 6. 2022.)

Helixstorm, Phishing protection: 11 ways to protect your business from phishing emails, n.d., https://www.helixstorm.com/blog/phishing-protection-tips/ (18. 6. 2022.)

Hill Country Tech Guys, Gone phishing: How to protect your business from phishing attempts, n.d., https://hctechguys.com/gone-phishing/ (18. 6. 2022.)

If-Koubou, Što je Open Source softver i zašto je to bitno?, n.d., https://hr.if-koubou.com/articles/how-to/what-is-open-source-software-and-why-does-it-matter.html (18. 6. 2022.)

Imperva, Phishing attacks, n.d.https://www.imperva.com/learn/application-security/phishing-attack-scam/ (18. 6. 2022.)

IT Governance, What is Phishing? Techniques & examples, n.d., https://www.itgovernance.co.uk/phishing (18. 6. 2022.)

Jabuka.tv, Hrvatske državne institucije dva mjeseca bile na udaru hakera, a još se ne zna tko stoji iza napada, 2019., https://www.jabuka.tv/hrvatske-drzavne-institucije-dva-mjeseca-bile-na-udaru-hakera-a-jos-se-ne-zna-tko-stoji-iza-napada/ (18. 6. 2022.)

Kaspersky, What Is Pharming and How to Protect Yourself, n.d., https://www.kaspersky.com/resource-center/definitions/pharming (18. 6. 2022.)

KnowBe4, Phishing Attacks, n.d., https://www.knowbe4.com/phishing (18. 6. 2022.)

Leksikografski zavod Miroslava Krleže, bitcoin, 2021., https://www.enciklopedija.hr/natuknica.aspx?id=70775 (18. 6. 2022.)

Lider media, Kako zaštititi sebe i svoju organizaciju od ransomwarea?, 2016., https://lidermedia.hr/aktualno/kako-zastititi-sebe-i-svoju-organizaciju-od-ransomwarea-122207 (18. 6. 2022.)

Malwarebytes, What is phishing?, n.d., https://www.malwarebytes.com/phishing (18. 6. 2022.)

Mreža, Napad na školska računala, 2018., https://mreza.bug.hr/napad-na-skolska-racunala/ (18. 6. 2022.)

Oxford Web Studio, Šta je IP adresa, n.d., https://www.oxfordwebstudio.com/da-li-znate/sta-je-ip-adresa.html (18. 6. 2022.)

Packetlabs, What is the business impact of a Phishing Attack?, 2020., https://www.packetlabs.net/posts/impact-of-phishing-attack/ (18. 6. 2022.)

Phishing.org, History of Phishing, n.d., https://www.phishing.org/history-of-phishing (18. 6. 2022.)

Phishing.org, What Is Phishing?, n.d., https://www.phishing.org/what-is-phishing (18. 6. 2022.)

PhishProtection, History of Phishing: How Phishing Attacks Evolved From Poorly Constructed Attempts To Highly Sophisticated Attacks, 2019., https://www.phishprotection.com/resources/history-of-phishing/ (18. 6. 2022.)

Proofpoint, What is Phishing?, n.d., https://www.proofpoint.com/us/threat-reference/phishing (18. 6. 2022.)

Ravnateljstvo policije, Phishing poruka elektroničke pošte i pokušaj različitih oblika internetskih prijevara, 2019., https://policija.gov.hr/vijesti/phishing-poruka-elektronicke-poste-i-pokusaj-razlicitih-oblika-internetskih-prijevara/1843 (18. 6. 2022.)

Terranova Security by HelpSystems, What is phishing?, n.d., https://terranovasecurity.com/what-is-phishing/ (18. 6. 2022.)

Terranova Security by HelpSystems, What is vishing?, n.d., https://terranovasecurity.com/what-is-vishing/ (18. 6. 2022.)

Tportal, Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka, 2017., https://www.tportal.hr/tehno/clanak/ne-nasjedajte-na-ovaj-lazni-mail-iz-porezne-mogli-biste-ostati-bez-podataka-20171201https://www.cert.hr/CUPOPOREZ (18. 6. 2022.)

Trend Micro, What Is Smishing?, n.d., https://www.trendmicro.com/en_us/what-is/phishing/smishing.html (18. 6. 2022.)

Wallarm, Types Of Phishing Attacks And Business Impact, n.d., https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact (18. 6. 2022.)

xorlab AG, How to Protect Your Organization against Spear Phishing Attacks, 2022. https://www.xorlab.com/blog/protect-against-spear-phishing/ (18. 6. 2022.)

## Popis pokrata

AOL – *America Online*

URL – *Uniform Resource Locator*

## Popis grafikona

## Popis slika

## Popis priloga