Analiza kibernetičkih prijetnji povezanih s krađom identiteta u uvjetima pandemije COVID-19

Stančin, Domagoj

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:136120

Sveučilište u Zagrebu
Ekonomski Fakultet
Integrirani preddiplomski i diplomski sveučilišni studij
Poslovna ekonomija – smjer Menadžerska informatika

ANALIZA KIBERNETIČKIH PRIJETNJI POVEZANIH S KRAĐOM IDENTITETA U UVJETIMA PANDEMIJE COVID-19

Diplomski rad

Domagoj Stančin

Zagreb, srpanj 2022.

Sveučilište u Zagrebu
Ekonomski Fakultet
Integrirani preddiplomski i diplomski sveučilišni studij
Poslovna ekonomija – smjer Menadžerska informatika

ANALIZA KIBERNETIČKIH PRIJETNJI POVEZANIH S KRAĐOM IDENTITETA U UVJETIMA PANDEMIJE COVID-19

ANALYSIS OF CYBER THREATS RELATED TO IDENTITY THEFT IN THE CONTEXT OF THE COVID-19 PANDEMIC

Diplomski rad

Student: Domagoj Stančin
JMBAG studenta: 0035207438
Mentor: Prof. dr. sc. Mario Spremić

Zagreb, srpanj 2022.

SAŽETAK

Pandemija virusa SARS-CoV-2**,** uzročnika bolesti COVID-19, krajem 2019. i početkom 2020. godine drastično je utjecala na moderno društvo i načine na koji su se do tad odvijale aktivnosti u svim područjima ljudskog života. S obzirom na to da svakodnevne aktivnosti s ciljem suzbijanja zaraze poprimaju digitalni karakter, pojedinci i organizacije postaju izloženiji prijetnjama iz domene kibernetičkog kriminala. U radu se izlaže teorijska podloga kojom se pojašnjava formiranje pojma digitalnog identiteta, a potom se razlaže terminologija kibernetičkog kriminala i kibernetičke sigurnosti. Daje se detaljan pregled najčešćih prijetnji povezanih s krađom digitalnog identiteta, uz predstavljanje aktualnih pandemijskih trendova i analizu odabranih studija slučaja. Raspravljaju se i trenutačne metode zaštite od krađe digitalnog identiteta i predlažu nova rješenja koja bi uspješnost ovih prijetnji u budućnosti trebala svesti na minimum. Zaključuje se kako je riječ o prijetnjama visoke razine rizika čije aktualne metode suzbijanja nisu dovoljno efikasne, stoga je potrebno formiranje i kontinuirano usavršavanje napredne strategije obrane od povreda digitalnog identiteta.

Ključne riječi: digitalni identitet, pandemija COVID-19, krađa digitalnog identiteta, kibernetička sigurnost, mjere zaštite

SUMMARY

The pandemic of the SARS-CoV-2 virus, the cause of the COVID-19 disease that appeared at the end of 2019. and the beginning of 2020., drastically affected modern society and altered the ways in which everyday activities were carried out in all areas of human life. Given that with the aim of combating infection, those activities take on a digital character, individuals and organizations become more exposed to threats from the domain of cybercrime. The paper presents the theoretical background through which the formation of the concept of digital identity is clarified, and then the terminology of cybercrime and cyber security is explained. A detailed overview of the most common threats associated with digital identity theft is given, along with a presentation of current pandemic trends and an analysis of selected case studies. Current methods of protection against digital identity theft are also discussed and new solutions are proposed that should minimize the success of these threats in the future. It is concluded that digital identity theft threats are threats of a high level of risk, and that the current defence methods are not efficient enough. The formation and continuous improvement of an advanced defense strategy against breaches of digital identity is necessary.

Keywords: digital identity, COVID-19 pandemic, digital identity theft, cyber security, protection measures

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad / seminarski rad / prijava teme diplomskog rada isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada / prijave teme nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada / prijave teme ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada / prijave teme nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

(vlastoručni potpis studenta)

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

(personal signature of the student)

(place and date)

SADRŽAJ

1. UVOD

1.1 Predmet i cilj rada

Digitalni identitet kompleksan je konstrukt koji se može opisati kao ukupnost ljudskih interakcija u digitalnoj sferi, ali i kao skup svih atributa i oznaka koje ga jednoznačno određuju u online okruženju (Bitdefender, 2022). S obzirom na to da trend prisustva u virtualnom svijetu raste, digitalni identitet pojam je koji dobiva na sve većoj važnosti. Od posebnog je interesa njegova kompromitacija i zaštita od iste, jer ona može dovesti do mnogobrojnih neželjenih posljedica, koje nerijetko mogu biti veće nego u materijalnom svijetu. Stoga krađe digitalnog identiteta zauzimaju posebno mjesto u terminologiji kibernetičkih rizika i kibernetičke sigurnosti. Dosadašnje mjere zaštite često su zastarjele i nedovoljno efikasne, što implicira potrebu za njihovim osuvremenjivanjem.

Aktualna pandemija bolesti COVID-19 dodatno je produbila promatrani problem. S obzirom na to da je većinu vremena od početka trajanja pandemije digitalni identitet bio jedini način identifikacije pojedinaca, manipuliranje njime zadobilo je posebnu pažnju kibernetičkih kriminalaca. Aktivnosti krađe digitalnog identiteta nikada u povijesti promatranja nisu bilježile tako visoke brojke, a njihova raznovrsnost i kompleksnost čini ih gotovo nemogućima za detekciju. Uzevši u obzir rastući interes kriminalaca za segmentima društva koji su zbog epidemiološke situacije pod dodatnim pritiskom, krađe digitalnog identiteta postaju izrazito štetnim oružjem kriminalaca. Opisana situacija postaje temeljem za raspravu o potrebi kreiranja novih metoda zaštite koje će biti djelotvornije u suprotstavljanju prijetnjama ovog tipa. Potaknut navedenom problematikom, ovaj rad za cilj ima provesti analizu kibernetičkih prijetnji povezanih s krađom identiteta u uvjetima aktualne pandemije. Analiza se nastoji provesti dokazivanjem četiriju temeljnih pretpostavki rada, a to su (1) dokazati da je u vremenskom razdoblju od ožujka 2020. godine do danas došlo do značajnog porasta navedenih vrsta kibernetičkog kriminala, (2) dokazati da su sami kibernetički napadi sofisticiraniji nego ranije, (3) dokazati da je u promatranom razdoblju došlo do promjene meta promatranih kibernetičkih napada, (4) dokazati da je nužno razviti i proaktivno koristiti napredne tehnologije prilikom zaštite digitalnog identiteta.

1.2 Izvori podataka i metode prikupljanja

U izradi rada korišteni su sekundarni izvori podataka prikupljeni putem Interneta te stručna i znanstvena literatura. Stručna i znanstvena literatura pretežito je ona korištena pri izvedbi kolegija s Katedre za informatiku Ekonomskog fakulteta u Zagrebu. Koriste se i znanstveni radovi stranih autora iz područja kibernetičke sigurnosti, posebice one povezane s oblicima krađe digitalnog identiteta, a poseban značaj imaju izvještaji regulatornih tijela i organizacija posvećenih borbi protiv ove vrste kriminala.

Temeljna metodologija korištena u radu je kvalitativna metodologija studije slučaja. U dokazivanju se koriste i sekundarni statistički podaci prikupljeni putem Interneta.

1.3 Sadržaj i struktura rada

Struktura rada podijeljena je u osam dijelova. Rad započinje navođenjem predmeta i ciljeva rada, izvora podataka i metoda prikupljanja te sadržajem i strukturom rada. U drugom dijelu pojašnjava se pojam digitalnog identiteta, opisuje njegov razvoj i rizici koji proizlaze iz njegova korištenja. Treći dio dotiče se kibernetičkog kriminala. Ovdje se definira sam koncept kibernetičkog kriminala, navodi se njegova evolucija te načini i mjere zaštite od ovog vrsta kriminala. Slijede četvrti i peti dio koji promatraju trenutno najkorištenije metode krađe digitalnog identiteta. Riječ je o *phishingu* i društvenom inženjeringu, a u svakom od ova dva poglavlja promatra se pojmovno razgraničenje, povijesni razvoj, trendovi koji su se razvili u posljednje dvije godine i analizira se odabrana studija slučaja. U šestom dijelu predstavlja se novi, napredni oblik krađe identiteta, a riječ je o *deepfake* tehnologiji. Ona se pojašnjava te se navode pozitivni i negativni načini njezina korištenja. Poglavlje završava analizom studije slučaja. U sedmom poglavlju raspravljaju se moguća rješenja i mjere zaštite s organizacijskog i tehnološkog aspekta. U osmom dijelu rada sumira se navedeno i autor donosi zaključak.

2. KONCEPT DIGITALNOG IDENTITETA

2.1 Definiranje pojma digitalnog identiteta

Pojam identiteta, pa samim time i digitalnog identiteta, izrazito je složen konstrukt čije je definiranje od najranijih vremena predmetom filozofskih, sociooloških i psiholoških rasprava. Mnogi stručnjaci u ovim društvenim znanostima navode razne značajke i perspektive pomoću kojih bi jednoznačno odredili ovaj društveni fenomen. Nagy i Koles (2014) tako navode četiri glavne razine koje utječu na formiranje identiteta:

- individualni identitet – skup karakteristika koje pojedinac pripisuje sam sebi
- relacijski identitet – manifestira se kroz društvene interakcije
- socijalni (društveni) identitet – percipiran je kroz pripadnost društvenim skupinama, poštivanje normi i očekivanja
- materijalni identitet – materijalna dobra pomoću kojih je pojedinac prepoznat u društvu (stil odijevanja, automobil koji vozi i sl.).

Sve četiri razine podjednako su važne pri određivanju identiteta osobe, no samo njegovo shvaćanje u današnje vrijeme često se odmiče od apstraktnog, društvenog aspekta i promatra se isključivo kroz materijalnu prizmu. U svojoj raspravi o razvoju digitalnog identiteta, Bertino et al. (2009.) uvode pojam identifikatora. Navode kako je identifikator „određeni pojavni oblik atributa koji se vezuje uz osobu, odnosno oblik svojstva koje toj osobi pripada kao što je ime, datum rođenja, broj kreditne kartice, povijest transakcija i sl.“ (Bentino et al., 2009). Navedeni autori tako razlikuju tzv. jake i slabe identifikatore, ovisno o tome na koliko pojedinaca je njihovo postojanje primjenjivo (npr. isti datum rođenja može imati veći broj osoba, no određeni OIB pripada samo jednoj). Skup identifikatora naziva se parcijalnim identitetom jer samo djelomično određuje pojedinca (Bentino et al., 2009). Uzevši u obzir navedeno, može se zaključiti kako je identitet neke osobe skup njenih društvenih i materijalnih odrednica, koje pripadaju isključivo njoj i čine ju jedinstvenom u njezinom okruženju.

Paralelno intenzivnom razvoju i masovnom usvajanju računalne tehnologije i Interneta koji se bilježi proteklih desetljeća, javlja se i pojam digitalnog identiteta. Tehnološki napredak

omogućio je da digitalne tehnologije budu dostupne svima, u svakom trenutku i na svakoj lokaciji. One su iz temelja promijenile načine na koje se većina najjednostavnijih svakodnevnih transakcija odvija, potpomogle su razvoju revolucionarnih načina komuniciranja i omogućile sasvim novu dimenziju interakcije između pojedinaca i zajednica u virtualnoj sferi. Postupno se kreira virtualni svijet koji, kao i onaj materijalni, zahtijeva identifikaciju svojih pripadnika putem digitalnog identiteta. Ovaj pojam zbog mogućnosti, ali i ograničenja koja digitalna sfera nudi, lakše je definirati nego u materijalnom svijetu pa stoga nije čudno što mišljenja stručnjaka oko njega konvergiraju više nego u prethodnim raspravama. Bentino et al. (2009) tako zaključuju da je digitalni identitet digitalni prikaz poznatih informacija o određenom pojedincu ili organizaciji. Majeed et al. (2020) navode kako je riječ o zbroju atributa, konotacija i simbola kojima se osoba definira u virtualnom prostoru, pa na temelju njega komunicira s drugima, a njegov sadržaj ne mora odgovarati identitetu u pravom, društvenom prostoru. Digitalni identitet sastoji se od karakteristika ili atributa podataka, kao što su: korisničko ime i lozinka, aktivnosti pretraživanja na mreži, elektroničke transakcije, datum rođenja, broj socijalnog osiguranja, medicinska povijest, povijest kupovanja ili ponašanja na Internetu i sl. Iz navedenog je vidljivo da je digitalni identitet, kao i u stvarnosti, agregat pojedinčevih interakcija i transakcija u digitalnom okruženju, nadopunjen svim podacima koji promatranog pojedinca pobliže opisuju (Techopedia, 2022).

Važno je imati na umu da sve naše internetske aktivnosti ostavljaju određeni trag koji je često trajan i nepromjenjiv. Čovjek nema potpunu kontrolu nad zapisima svojih digitalnih interakcija, zbog čega je moralno i odgovorno korištenje Internetom postalo imperativom današnjice. U virtualnom društvu koje funkcionira na opisani način, privatni podaci pojedinca postaju najvrijednija imovina 21. stoljeća čije posjedovanje dovodi do raznih prednosti, a njihova kompromitacija i maliciozno korištenje mogu dovesti do mnogih neželjenih posljedica.

2.2 Povijesni razvoj digitalnog identiteta

Povijesno gledano, identitet osobe najčešće je bio predstavljen njenim imenom, čija je namjena bila postizanje jedinstvenosti, odnosno osiguranja povjerenja i transparentnosti kao osnove za stvaranje društvenih ugovora i uspostavljanje društvenih odnosa. Može se reći kako je kroz velik dio ljudske povijesti ime bilo najkorišteniji identifikator u većini društvenih interakcija.

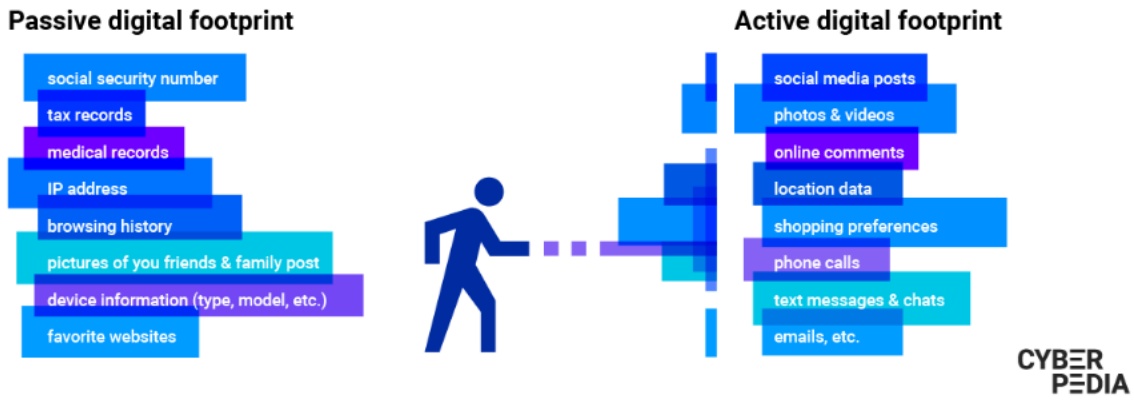
Imena imaju mogućnost predstavljanja određenih sposobnosti ili pojava, što ih čini prikladnim instrumentom kategorizacija ili davanja određenog značenja promatranim subjektima.

Sama rasprava o digitalnom identitetu počinje stvaranjem golemih baza podataka od strane ustanova, čija je namjena bila kreiranje modela institucionalne stvarnosti. Prva ustanova takve namjene bila je američka Trgovačka agencija (*Mercantile Agency*, današnji Dun & Bradstreet), osnovana 1841. godine. Cilj joj je bio vođenje evidencije i pružanje informacija o kreditnoj sposobnosti kako bi olakšala donošenje odluka u trgovinskom poslovanju. Kompanija 1963. godine uvodi unificirani deveteroznamenkasti broj kojim označava subjekte, i koji ostaje temeljem njenog poslovanja do danas. U Ujedinjenom Kraljevstvu 1844. osniva se Kuća poduzeća (*Companies House*), koja je glavni regulator pri osnivanju, registraciji i praćenju podataka privatnih poduzeća. Obje institucije tako prikupljaju podatke o pojedincima i poduzećima, njihovim imenima, datumima rođenja, adresama, zanimanjima i nacionalnostima. Digitalizacijom baza podataka obiju ustanova nastali su digitalni zapisi o 285, odnosno 3.5 milijuna entiteta. Moderni državno regulirani sustavi identifikacije funkcioniraju po istom principu digitalizacije podataka. Tako zapisani podaci predstavljaju formalni, državno regulirani dio digitalnog identiteta (Breckenridge, 2018).

S druge strane, neformalni dio digitalnog identiteta usko je vezan uz intenzivnu integraciju Interneta u našu svakodnevicu. Posebno mjesto zauzimaju razni oblici virtualnih zajednica s društvenim mrežama kao glavninom nove dimenzije digitalnog identiteta. Najznačajniji predstavnik ove skupine je Facebook, izrazito moćna platforma koja objedinjuje trećinu svjetske populacije. Mogućnosti koje ova društvena mreža nudi svojim korisnicima praktički su neograničene, a samo neke od njih su razmjena mišljenja, stavova i ideja, dijeljenje svojih veza s drugim ljudima, objavljivanje povezanosti s institucijama, organizacijama, interesnim skupinama i sl. Raznovrsni podaci generirani na Facebooku čine ga najvećom svjetskom bazom podataka, koji se koriste u komercijalne, ali nerijetko i ilegalne svrhe, što kao rezultat ima povredu privatnosti korisnika i izaziva mnoge polemike oko samog regulatornog okvira. Facebook je tako najreprezentativniji primjer postupne migracije društava u virtualni svijet koji funkcionira na drugačiji način od stvarnog. Samo posjedovanje korisničkog profila promatra se kao svojevrsna privilegija koja znatno olakšava korištenje ostalih digitalnih usluga, kao što su prijave u mnoge virtualne poslovne modele bez prethodnog kreiranja korisničkog profila. Neformalni dio digitalnog identiteta tako postaje vodećim aspektom cjelokupnog digitalnog identiteta, što zbog nemogućnosti njegove regulacije nije odviše poželjna pojava.

Neizostavni pojam u raspravama o digitalnom identitetu osobe njezin je digitalni otisak. Riječ je o skupu svih informacija o osobi prikupljenih svim oblicima i načinima njenog korištenja Internetom, putem kojeg se te aktivnosti mogu direktno pripisati stvarnom identitetu osobe, zbog čega ga se još naziva „digitalnim dosjeom“, „digitalnom sjenom“, odnosno „digitalnim otiskom prsta“. Razlikuju se dvije temeljne vrste digitalnog otiska, aktivni i pasivni. Aktivna se odnosi na namjerno dijeljenje multimedija putem društvenih mreža, javno komentiranje sadržaja, komunikaciju i slične „dobrovoljne“ aktivnosti. Nad ovim dijelom korisnik ima umjerenu do visoku kontrolu. Oblici pasivnog digitalnog otiska su npr. bilježenje IP adrese, korištenih uređaja i povijesti pretraživanja. Razina kontrole ovdje je ograničena ili nepostojeća, ovisno o usluzi i tehnologiji koja je korištena. Samo neki od potencijalnih rizika koji proizlaze iz pasivnog digitalnog otiska su neovlašteno korištenje tako prikupljenih podataka od strane neautoriziranih osoba kako bi se naštetilo privatnom ili poslovnom životu i ugledu osobe, kompromitiralo njezin identitet ili izvukla (najčešće financijska) korist. Digitalni otisak koji kontinuirano ostavljamo za sobom uvijek je veći nego što mislimo, no uvijek postoje načini njegove redukcije i kontrole. Samo neke od metoda su korištenje pretraživača koji ne sakupljaju velike količine podataka (kao alternativa Google-u), korištenje antivirusnih programa i dodataka koji smanjuju pasivni digitalni otisak te općenito odgovorno ponašanje na Internetu (Bitdefender, 2022).

Slika 1. Vrste digitalnog otiska

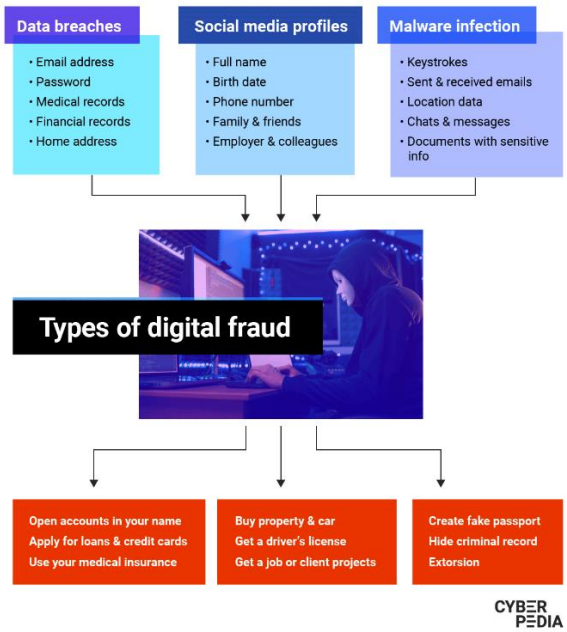


Bitdefender (2022): What is your digital footprint, *https://www.bitdefender.com/cyberpedia/what-is-digital-footprint/, pristupljeno 11.6.2022*

2.3 Rizici vezani uz digitalni identitet

Rastući digitalni otisak i sve veća prisutnost u digitalnoj sferi čine pojedinca i organizacije izrazito ranjivima. Neki od najvećih rizika, koji proizlaze iz promatranih trendova, vezani su uz krađu identiteta. Krađom identiteta smatra se krađa ili neovlašteno korištenje identifikacijskih informacija od strane nekog neautoriziranog subjekta s namjerom počinjenja prevare lažnim predstavljanjem i krajnjim ciljem ostvarenja financijskih ili nekih drugih koristi, ili nekim drugim oblikom počinjenja štete. Ovaj oblik kriminala moguć je kako u fizičkom, tako i u virtualnom okruženju. Osnovno zajedničko obilježje je način rada kriminalaca, koji podrazumijeva dugotrajno i temeljito otkrivanje povjerljivih informacija o žrtvi kako bi ju se s vremenom moglo eksploatirati. Motivi su u oba slučaja stjecanje financijske ili neke druge koristi, dokazivanje moći ili ideološka pozadina. Konačno, posljedice svake krađe identiteta dugotrajne su financijske i/ili emotivne posljedice na pojedinca. Jednom kad povjerljive informacije osobe, pomoću kojih se ona svakodnevno identificira, budu otuđene, kriminalci s njima mogu činiti radnje kao što su otvaranje nove kreditne kartice ili čak nove kreditne linije, obavljanje neovlaštenih kupnji, podnošenje porezne prijave kako bi ostvarili povrat poreza, korištenje zdravstvenog osiguranja s ciljem ostvarivanja medicinske njege, iznajmljivanje nekretnina i drugih oblika imovine i sl. (Norton, 2022).

Slika 2. Načini krađe i korištenje podataka vezanih uz digitalni identitet



Bitdefender (2022): What is digital identity theft, *https://www.bitdefender.com/cyberpedia/what-is-digital-identity-theft/, pristupljeno 12.6.2022*

Bitna razlika između fizičke i digitalne krađe identiteta je upravo ta da ogromna količina dostupnih informacija i raznih izvora podataka, koje napadači mogu pronaći putem Interneta, olakšava samu krađu i lažno predstavljanje (Bitdefender, 2022). Uzevši u obzir činjenicu da se mnoge internetske interakcije i transakcije odvijaju anonimnim putem (odnosno ne „licem u lice“), i da je sve veći broj njih automatiziran, nije čudno što internetske prevare ove vrste često ostaju nezamijećene duži vremenski period, a sami krivci često nikada ne budu pronađeni. Javljaju se i neki novi oblici krađa identiteta kao što su oponašanje putem društvenih medija, koje označava kloniranje identiteta i njegovo korištenje za prevare kontakata, iznuđivanja za ponovnim pristupom korisničkom računu i prijetnje drugim korisnicima (Bitdefender, 2022). Sama umreženost otvara priliku za dodatnu zaradu pa kriminalci, koji su na neovlašten način prikupili podatke, mogu iste prodati putem aukcija na teže dostupnim dijelovima Interneta (tzv. *dark web*) i tako zaraditi velike novčane iznose. Naime, brojevi socijalnog osiguranja prodaju se za 1 USD, brojevi kreditnih kartica za oko 110 USD, a putovnice Sjedinjenih Američkih Država postižu cijenu od čak 2.000 USD (Norton, 2022). Sama tehnologija, odnosno njena dostupnost, cjenovna pristupačnost i lakoća ovladavanja njome, čine krađu identiteta mogućom za pojedince koji se u materijalnim uvjetima nisu upuštali u kriminalne aktivnosti ovog tipa (Idwatchdog, 2022).

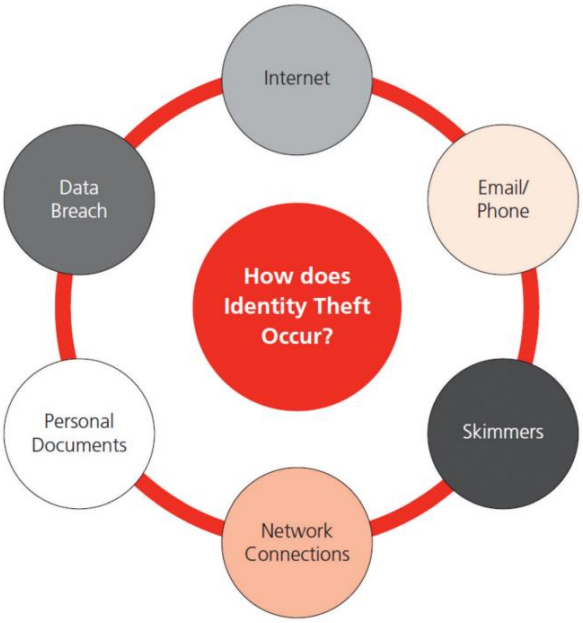
Osnovne oblike digitalnih krađa identiteta moguće je na temelju zajedničkih karakteristika podijeliti u nekoliko skupina. Prema portalu Idwatchdog to su:

- Prevare putem Interneta i mrežnih uređaja – u ovim vrstama prevara domišljato se koristi temeljna, javno dostupna internetska i računalna infrastruktura kako bi se naštetilo korisnicima iste. Dva osnovna oblika krađe identiteta su lažne web stranice i javno dostupne Wi-Fi mreže, odnosno USB portovi koji se koriste kao kanali napada na korisnike.
- Prevare putem e-maila ili telefona – karakterizira ih kontaktiranje žrtava preko najkorištenijih komunikacijskih kanala današnjice, e-mail poruka i tekstualnih mobilnih poruka (SMS), ali i telefonskih poziva. Vrste su *phishing*, *smishing* i *vishing*.
- Prevare od strane poznanika – ove prevare podrazumijevaju iskorištavanje već dobro poznatih informacija o žrtvi od strane njoj bliskih osoba. Uključuju prevare od strane člana obitelji ili prijatelja i prevare eksploatacije povjerenja.
- Povrede maliciozne uporabe podataka – odnose se na namjerno ili nenamjerno otkrivanje podataka kao rezultata kriminalnih aktivnosti ili nepažnje prilikom rukovanja podacima.

Ovdje se ubraja i kupoprodaja tako prikupljenih podataka na ilegalnim internetskim tržištima.

- Fizička krađa podataka – povezanost fizičkog i digitalnog identiteta, odnosno mogućnost lažnog predstavljanja na Internetu koje proizlazi iz posjedovanja neke informacije iz fizičkog svijeta, također ima negativne učinke. Ova skupina obuhvaća najveći broj prevara, iz čega je vidljiva međuovisnost materijalnog i virtualnog. U ove prevare ubrajaju se *skimming* te fizičke krađe imovine kao što su krađa samog novčanika, pošte, kreditne kartice ili osobnih dokumenata, ali i tzv. „*dumpster diving*“, odnosno pretraživanje otpada potencijalnih žrtava s ciljem dobivanja bitnih i povjerljivih informacija (Idwatchdog, 2022).

Slika 3. Skupine metoda krađe identiteta



HSBC Bank (2022): Your Money Counts – Identity theft, *https://www.us.hsbc.com/content/dam/hsbc/us/docs/pdf/ID_Theft_Workbook_revApril2019.pdf, pristupljeno 13.6.2022*

3. KIBERNETIČKI KRIMINAL

3.1 Definiranje kibernetičkog kriminala

Kako bi se lakše definirao pojam kibernetičkog kriminala i shvatila njegova ozbiljnost, važno je promotriti evoluciju računalne tehnologije, širinu načina njena korištenja i konačno, utjecaja koji ona ima na život modernog čovjeka.

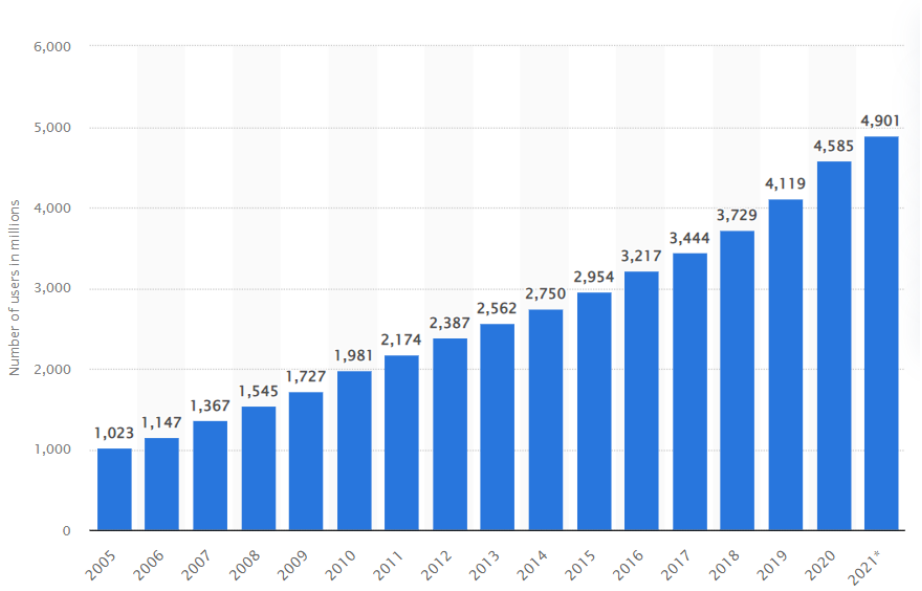
3.1.1 Digitalne tehnologije i digitalna transformacija

Potreba za sustavom koji će u većoj ili manjoj mjeri služiti za jednostavnije ili složenije obrade podataka, kao i pohranjivati neke od tih podataka, seže daleko u ljudsku povijest. Već se u trećem tisućljeću pr. Kr. u Maloj Aziji javljaju jednostavne naprave za rješavanje navedenih problema, koje današnji oblik poprimaju 1946. godine izumom ENIAC-a, prvog modernog elektroničkog računala. Današnja elektronička računala četvrte generacije programabilni su strojevi namijenjeni obradama podataka u najširem smislu. Shematski ih je moguće prikazati kao sustav koji se sastoji od 5 temeljnih dijelova: centralne procesorske jedinice, memorijske jedinice, ulazno-izlazne jedinice i sabirnica. Funkcioniraju na temelju instrukcija, odnosno naredbi putem kojih se vrši komunikacija i obrada podataka između navedenih računalnih jedinica. Uzevši u obzir širinu primjene računala, ona postaju temeljni dio svakodnevnih interakcija i transakcija 21. stoljeća (Pivar, J. i Vlahović, N., 2020).

Istovremeno, razvija se i sustav koji bi omogućio međusobno povezivanje računala, njihovu komunikaciju i ostale oblike interakcije (kao što je prijenos sadržaja). Američka vojska početkom 1960-ih godina nastoji razviti tehnologiju koja bi daljinsku obradu podataka učinila mogućom. U svom naumu uspijeva 1969. godine kada uspostavlja vezu između dva američka sveučilišta te tako nastaje ARPANET (skraćenica od *Advanced Research Projects Agency Network*), a sam događaj smatra se izumom Interneta. Inicijalnoj vezi postupno se pridružuju i ostale akademske ustanove, čineći tako sverastuću mrežu povezanih sustava. Razvijaju se i internetski protokoli, odnosno pravila prijenosa sadržaja Internetom. Također, nastaju razni mrežni uređaju koji zajedno s protokolima stvaraju temeljnu infrastrukturu za nastanak „mreže nad mrežama“. S vremenom raste i kapacitet, brzina i pouzdanost prilikom prijenosa sadržaja

u mreži, čime Internet postaje jednim od najvažnijih civilizacijskih dostignuća modernog doba, ali i najznačajnijim medijem u proteklih nekoliko desetljeća (Leiner et al., 1997).

Slika 4. Porast korisnika Interneta promatran na globalnoj razini



Statista (2022): Number of Internet users worldwide from 2005 to 2021,*https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/, pristupljeno 16.6.2022.*

Masovna integracija računala i Interneta u sve sfere društvenog, gospodarskog, političkog i kulturološkog života čine opisana dostignuća najmoćnijim kanalima donošenja promjena, ali i sredstvima čije inovativno korištenje može donijeti određeni napredak i konkurentsku prednost. Navedeno se postiže ispravnim korištenjem digitalnih tehnologija. Ovaj pojam označava samu okosnicu nove, tehnološki utemeljene (digitalne) ekonomije, a odnosi se na skup koji sačinjavaju informacijske tehnologije, računalne znanosti te komunikacijske i povezive tehnologije (Spremić, 2017). Same digitalne tehnologije na temelju intenziteta primjene moguće je podijeliti u dvije velike skupine. To su primarne digitalne tehnologije (mobilne tehnologije, društvene mreže, računalstvo u oblacima, veliki podaci i njihova analitika, senzori i Internet stvari) i sekundarne digitalne tehnologije (3D pisači, robotika, dronovi, virtualna i proširena stvarnost i kognitivne tehnologije) (Spremić, 2017).

Neke od najstarijih djelatnosti iz temelja su promijenjene intenzivnim korištenjem digitalnih tehnologija. Ovaj fenomen poznat je pod nazivom digitalna transformacija.

“Digitalna transformacija poslovanja odnosi se na stalnu primjenu digitalnih tehnologija usmjerenu osmišljavanju inovativnih poslovnih strategija i disruptivnih poslovnih modela, primjeni progresivnih koncepcija poslovanja, novih načina vođenja i upravljanja (digitalni lideri), kako bi se kupcima ponudili bolji proizvodi, usluge i osobito iskustva njihova korištenja. Pri tome se intenzivno koriste digitalne tehnologije kako bi se stvorila nova vrijednost za kupce, omogućilo nenadmašno iskustvo upotrebe poslovnog modela, što bi trebalo rezultirati boljim poslovnim prihodima i općenito boljim rezultatima poslovanja“ (Spremić, 2017, str. 40).

Postizanje digitalne transformacije u poslovanju nikako nije lako jer ovisi o čitavom nizu faktora. Razumijevanje digitalnih tehnologija i ovladavanje njima samo je jedan od uvjeta. Potrebna su velika ulaganja u digitalne kompetencije zaposlenika na svim razinama, a posebice na upravljačkim pozicijama (viši menadžment, tzv. C-pozicije). Sukladno tome, digitalna transformacija mora biti strateška inicijativa menadžmenta, odnosno vođena „od vrha“. Nužno je kreirati i fleksibilnu IT infrastrukturu. Često je potrebna i promjena orijentacije organizacijske kulture u onu usmjerenu eksperimentiranju, preuzimanju rizika i inovaciji (Spremić, 2017). Usvajanje ovih praksi i obrazaca ponašanja vodi do postupnog razvoja ka zrelom IT upravljanju, odnosno zrelom digitalnom poslovnom modelu. Savastano et al. (2022) u svojem radu dokazuju kako je zrelost digitalnog poslovnog modela u direktnoj korelaciji s održivošću uspjeha poduzeća, posebice u dinamičnim i nesigurnim okolnostima današnjice.

Moguće je zaključiti kako je digitalna transformacija u pozadini većine najkorištenijih proizvoda i usluga današnjice. Promatrani fenomen kreativnim i inovativnim pojedincima i organizacijama spremnima na rizik nudi čitav niz dotad neiskorištenih prilika. Digitalne tehnologije i njihovo strateško korištenje uistinu dovode do revolucionarnih izuma koji iz temelja mijenjaju tradicionalna tržišta i industrije. Uslugama kao što je komunikacija (e-mail, WhatsApp, Viber, Messenger), prijevoz (Uber, Bolt, Flixbus), trgovina (Amazon, Alibaba i ostale online trgovine), plaćanje (Google Wallet, Apple Pay), rezervacija smještaja (Booking, Air b'n'b), prijenos multimedijskog sadržaja (YouTube, Netflix), naručivanje hrane (Glovo, Wolt) i mnogima drugima moguće je pristupiti na zahtjev u bilo kojem trenutku, s bilo koje lokacije (Spremić, 2017). Tehnologija uistinu postaje osnovnim sredstvom korištenim za zadovoljenje želja i potreba svake osobe na svijetu, a život bez nje praktički je nezamisliv.

3.1.2 Pojmovno razgraničenje kibernetičkog kriminala

Iz prethodno opisanih primjera vidljivo je da je moderna civilizacija u velikoj mjeri postala ovisna o digitalnim tehnologijama. Iako digitalna transformacija donosi iznimne prednosti kao što su brža, jeftinija, kvalitetnija i pouzdanija konzumacija digitalnih dobara, sa sobom donosi i određene nedostatke. Oni se vezuju uz rastuće pouzdavanje u tehnologiju, odnosno isključivo oslanjanje na moderna tehnološka dostignuća. Saznavanje lokacije određene adrese i planiranje rute putovanja nepojmljivo je bez rješenja kao što je Google Maps. Rezervacija smještaja pretežito se odvija preko digitalnih platformi. Praćenje vremenske prognoze putem bilo kojeg kanala osim mobilnih aplikacija stvar je prošlosti. Konačno, cjelokupna komunikacija isključivo se odnosi na digitalne načine komuniciranja. Jasno je da digitalna revolucija sa sobom donosi neograničene prednosti i prilike, stoga je važno primijetiti kako se pojedinci njome ne služe isključivo u altruistične, odnosno legalne svrhe. Sveopća migracija materijalnog svijeta u digitalnu sferu malo koje društvene aspekte ostavlja netaknutima, a kriminal nije jedan od rijetkih izuzetaka. Ovisnost o tehnologijama stvara put za nelegalno djelovanje u kibernetičkoj domeni koje je poznato pod nazivom kibernetički kriminal.

"Svaka kriminalna aktivnost koja uključuje računalo bilo kao instrument, metu ili sredstvo za nastavak daljnjih zločina spada u opseg kibernetičkog kriminala. Opća definicija kibernetičkog kriminala može biti "protupravna djela u kojima je računalo ili alat ili meta ili oboje" (Chawki et al., 2015, str 1).

Računalna tehnologija u kriminalnim radnjama može imati četiri glavne uloge, a to su redom:

- uloga objekta – odnosi se na nanošenje fizičke štete ili uništenje računala i računalne infrastrukture, bila ona namjerna ili nenamjerna,
- uloga subjekta – podrazumijeva računalnu tehnologiju koja čini okruženje, odnosno medij za počinjenje kriminalnih aktivnosti, kao u slučaju računalnih virusa,
- uloga alata - računala i računalna infrastruktura omogućuju kriminalcima planiranje, počinjenje i upravljanje kriminalnim aktivnostima te
- uloga simbola - uključuje prijetnje korištenja računala i računalne tehnologija za počinjenje određenih šteta (Chawki et al., 2015).

Razvijaju se mnoge vrste kibernetičkog kriminala, a kao najčešće skupine kriminalnih aktivnosti navode se prevara putem elektroničke pošte i Interneta, prevara identiteta (gdje se osobni podaci kradu i koriste), krađa podataka o financijskom ili kartičnom plaćanju, krađa i prodaja korporativnih podataka, kibernetičko iznuđivanje (zahtijevanje novca kako bi se spriječio budući napad), *ransomware* napadi (vrsta kibernetičke iznude nakon što je napad počinjen) i kibernetička špijunaža (gdje hakeri pristupaju državnim podacima ili podacima tvrtke) (Kaspersky, 2022). Spremić (2017) navodi kako se glavne prijetnje na Internetu, ovisno o objektu napada, dijele u 3 temeljne skupine. To su kibernetički kriminal (na razini pojedinca ili organiziranih skupina), kibernetička industrijska špijunaža (na korporativnoj i institucionalnoj razini) i kibernetičko ratovanje (na državnoj razini). Također, kada je riječ o kibernetičkom kriminalu, najčešća je podjela u dvije skupine, odnosno skupinu kriminalnih aktivnosti u kojima su računala i računalna infrastruktura meta napada te kriminalnih aktivnosti u kojima su računala i računalna infrastruktura sredstvom napada (Chawki et al., 2015).

Čimbenici koji kibernetičku, odnosno računalnu domenu čine primamljivom za počinjenje kriminala su mnogostruki. Internet nudi veliku mogućnost anonimnosti, koju je u stvarnom svijetu znatno teže postići. U prilog ide i činjenica da velik dio počinitelja kriminalnih djelovanja ovog tipa nikad nije uhvaćen i procesuiran, niti je snosio posljedice. Znanja i vještine potrebne za uspješno djelovanje dostupniji su i lakše usvojivi. Također, ostvarivo je daljinsko počinjenje kriminalnog djelovanja bez velike potrebe za izlaganje riziku. Glavni motivi za počinjenje kibernetičkog kriminala najčešće su financijska korist, osveta, potreba za dokazivanjem sposobnosti i moći, ili ostvarenje nekih interesnih i ideoloških ciljeva. Same posljedice također mogu bit značajnije nego u stvarnosti, a mogu poprimiti oblik financijske štete, ukaljanog ugleda, narušavanja povjerenja u osobu ili organizaciju, štete na kvaliteti i otežan nastavak poslovanja, potrebe za prekidom samog poslovanja, ali u nedavnim incidentima čak i ugroze samog ljudskog života te smrti.

3.2 Evolucija kibernetičkog kriminala

Iako proboji i maliciozno korištenje informacijsko-komunikacijske tehnologije sežu u prvu polovicu 19. stoljeća, sama pojava i razvoj kibernetičkog kriminala veže se uz najranije računalne viruse. Zbog već spomenute anonimnosti koja otežava vođenje evidencije kada je riječ o kibernetičkom kriminalu, teško je sa sigurnošću ustanoviti koji je uistinu prvi računalni virus. RABBITS virus generalno je prihvaćen kao začetnik računalnih virusa. Anonimna osoba

ga je 1969. godine instalirala na računalo u računalnom centru Sveučilišta u Washingtonu. Program je kreirao vlastite kopije do trenutka preopterećenja sustava i prestanka rada računala (Herjavec Group, 2021). Neizostavan je događaj iz 1988. godine kada je zabilježena pojava prvog Internetskog, odnosno računalnog „crva“. Riječ je o malicioznim programima koji repliciraju sami sebe te se internetskom infrastrukturom šire na druga računala. Kreirao ga je Robert Morris na MIT-u (*Massachusetts Institute of Technology*) bez shvaćanja rizika svojeg izuma. Greška u kodu crva je ubrzo uzrokovala uskraćivanje usluga na više od dvije tisuće računala, uzrokujući štetu koja se procjenjuje između 100.000 i 10.000.000 USD. Morris tako postaje prva osoba osuđena za kršenje akta o računalnoj prijevari i zlouporabi, što ga čini drugom osobom osuđenom za kibernetički kriminal (prvi je bio Ian Murphy 1981. godine). 1980-ih i 1990-ih jača interes za korištenje računala i Interneta u stjecanju nelegalnih koristi, a promatrani trend se nastavlja sve do danas, čineći kibernetičke rizike i napade jednima od najozbiljnijih suvremenih prijetnji (Herjavec Group, 2021).

Važno je skrenuti pažnju na činjenicu da se većina temeljnih obilježja kibernetičkog kriminala mijenja s vremenom. Sofisticiranost napada znatno je porasla, a današnji napadi izvedeni su od strane strpljivih pojedinaca koji do najsitnijih detalja planiraju i ostvaruju svoje nakane. U samim počecima napadi su se većinom fokusirali na eksploataciju računalnih sustava i mreža s računalom kao krajnjim ciljem. Danas je spomenuta infrastruktura samo alat koji omogućuje pristup novom krajnjem cilju, ljudima (Spremić, 2017). To je moguće zaključiti i iz promatranih statistika, prema kojima su najzastupljeniji oblici kibernetičkog kriminala krađa identiteta, zlonamjerni računalni kod, *phishing*, hakiranje, lažno predstavljanje, društveni inženjering i sl., tj. upravo oni napadi usmjereni na čovjeka. Kriminalci su uvidjeli da je najnepouzdaniji dio svakog sustava čovjek, odnosno njegova nepažnja ili nedostatak znanja za ispravno djelovanje. Stoga pravovremeno, kvalitetno i kontinuirano upoznavanje ljudi s kibernetičkim rizicima postaje svojevrsnim imperativom (Spremić, 2017).
Rezultat spomenutih trendova neki su od najskupljih i najistaknutijih incidenata modernog doba. Financijske štete često se procjenjuju u desecima i stotinama milijuna američkih dolara, a posljedice često znaju biti kobne za sam nastavak poslovanja promatrane organizacije ili institucije.

Stuxnet je naziv malicioznog računalnog virusa kojim je 2010. godine bila zahvaćena iranska nuklearna elektrana. Meta napada bili su elektromagnetski sklopovi unutar same elektrane. Napadači su iskoristili slabosti korištenog Windows operativnog sustava, pretražili mrežu u

potrazi za onim računalima koja kontroliraju opremu u elektrani te poslali naredbe o uništenju iste opreme. Smatra se kako je Stuxnet ušao u nuklearnu elektranu putem USB ulaza. Napad je uzrokovao otkazivanje centrifuga unutar elektrane s potencijalnim kobnim posljedicama. Spajanjem računala na Internet zahvaćeno je preko 30.000 IP adresa. Uzrokovao je štetu u iznosu od 1.000.000 USD, a samračunalni kod toliko je sofisticiran da se Stuxnet smatra prvim digitalnim oružjem (Malwarebytes, 2022).

Još jedan od naprednih napada je WannaCry *ransomware*. Također omogućen Windowsovim softverom, proširio se na 230.000 računala u 150 zemalja. Ovaj je zlonamjerni računalni kod nakon zaraze onemogućio korisnicima pristup korištenju računala te pritom tražio otkupninu u iznosu od 300 do 600 USD. Zahtijevana isplata trebala je biti u obliku Bitcoina jer je transakcije kriptovalutama teže pratiti putem Interneta. Mehanizam WannaCry napada funkcionirao je na temelju crva, slično kao i Stuxnet. Troškovi oporavka ovog napada iznosili su približno 4 milijarde USD, čineći ga jednim od najskupljih kibernetičkih incidenata do sada (Malwarebytes, 2022).

Iz navedenih primjera očito je da kriminalne aktivnosti i prijetnje u digitalnom okruženju poprimaju sasvim drugu dimenziju. Aktivnosti kriminalaca sve su kompleksnije i malicioznije te iziskuju sve veće troškove sanacije. Mogućnost utjecaja na sve velike segmente društva, kao i šanse za ostvarenjem kobnih posljedica sve su vjerojatnije. Kritična infrastruktura, sustav neophodan za neometano odvijanje života stanovnika neke države ili područja, zbog svoje važnosti postaje sve češćom metom napada. Konačno, zapažen je rastući trend pojave kriminalnih organizacija, odnosno udruženja koji počinjenjem kriminalnih kibernetičkih aktivnosti žele promovirati svoje ciljeve. Svi spomenuti čimbenici iziskuju nužnost za ovladavanjem znanja i vještina koja će rezultirati odgovornim i svjesnim ponašanjem u digitalnom okruženju.

3.3 Mjere i načini zaštite od kibernetičkog kriminala

S obzirom na to da je sam nastup napada počinjenih korištenjem računalne infrastrukture postao isključivo pitanje vremena, javlja se potreba za uspostavljanjem mehanizama obrana od ove vrste prijetnji. Sve češće se spominje i implementira metodologija kibernetičke sigurnosti kao krovnog sustava metoda obrana i minimizacije kibernetičkih rizika.

„Pojam kibernetičke sigurnost se odnosi na holistički model ovladavanja, upravljanja i osiguravanja funkcioniranja suvremenoga informatičkog okruženja koji uključuje tehnološke, organizacijske, društvene i ostale aspekte, u odnosu na klasične procedure informacijske sigurnosti koje su mahom tehnološki usmjerene“ (Spremić, 2017, str 53).

U samoj definiciji važno je obratiti pozornost na dvije temeljne odrednice. Prvo, riječ je o slojevitom holističkom pristupu koji implicira napore na svim razinama u ovladavanju i upravljanju rizicima, a na organizacijskoj razini označava sudjelovanje svih dionika organizacije (s vodstvom, odnosno menadžmentom na čelu) u kreiranju cjelovite strategije obrane i zaštite (Spremić, 2017). Na njega se nadovezuje druga bitna odrednica, a ona upućuje na svojevrsnu evoluciju u filozofiji prevencije šteta izazvanim ovim vrstama ugroza. Naime, sami kreatori modela i strategija kibernetičke sigurnosti svjesni su odmaka od isključivo tehnološkog aspekta kada je riječ o ovim napadima. Na sve većoj važnosti dobiva uloga pojedinca, odnosno zajednice u razumijevanju i pravilnom usvajanju organizacijske filozofije i kulture u podizanju razine svijesti kada je riječ o rizicima iz ove skupine (Spremić, 2017). Iz navedenog je moguće formirati dva slična, ali u suštini različita pojma, a to su informacijska sigurnost i već pojašnjena kibernetička sigurnost. Informacijska sigurnost primarno se bavi aspektom upravljanja tehnološkim rizicima, dok kibernetička sigurnost metodologiju proširuje uvođenjem ljudskog aspekta u cjelokupno shvaćanje rizika. Može se reći kako je informacijska sigurnost potpojam kibernetičke sigurnosti. Tako definirani koncepti postaju temeljem za obranu od sofisticiranih, kompleksnih napada i incidenata s kojima su društva suočena na svim razinama, od individualne do državne (Spremić, 2017).

Sam razvoj metoda i načina zaštite pratio je odmak od aspekta informacijsko-komunikacijskih tehnologija na onaj društveni. Riječ je o kontrolama, odnosno zaštitnim mjerama i mehanizmima čijim se ispravnim korištenjem vjerojatnosti od nastupa neželjenih događaja mogu znatno umanjiti. Kontrolama se nastoje očuvati i postići tri temeljna parametra (principa) na kojima počiva informacijska sigurnost:

- Povjerljivost – odnosi se na raspoloživost pojedinih informacija i informacijskih sustava samo i isključivo osobama koje su za to ovlaštene. Postiže se kontrolama ograničavanja pristupa putem ograničavanja ovlasti unutar sustava, kao što su identifikacija i autorizacija.
- Cjelovitost (integritet) – označava ispravnost i cjelovitost informacija tijekom cijelog njenog postojanja, odnosno naglašava njenu zaštitu od manipulacije i neovlaštenog

pristupa. Osigurava se kontrolnim mjerama zaštite podataka u prijenosu i mirovanju (kao što su sigurnosni internetski protokoli, kriptiranje podataka, zaštita pristupa dijelovima sustava).

- Dostupnost (raspoloživost) – označava pristup informacijama i sustavima za to ovlaštenim osobama na način i prema potrebama te osobe. Kontrole vezane uz zahtjev dostupnosti su kontrole za dostupnošću informacijskih resursa te kontrole održavanja kontinuiteta poslovanja i oporavka od katastrofe (Spremić, 2017).

Na principe informacijske sigurnosti nadovezuju se i zahtjevi informacijskih sustava. To je u prvom redu zahtjev sigurnosti koji se odnosi na održavanje kontinuiteta odvijanja funkcija informacijskog sustava, odnosno sprječavanje događaja kao što su prirodne katastrofe i ljudsko djelovanje, koji rezultiraju narušavanjem temeljnih funkcija i otežavaju nastavak željenog rada sustava. Slijedi zahtjev raspoloživosti (dostupnosti) koji je idejno sličan zahtjevu povjerljivosti kada je riječ o informacijskoj sigurnosti te dodatno naglašava pravilnu autorizaciju i administriranje sustavom. Konačno, zahtjev tajnosti zasniva se na dostupnosti pojedinih, tajnih informacija organizacije i pojedinca te ističe diferenciranje privatnih i povjerljivih podataka (Spremić, 2017).

S druge strane, organizacijske kontrole pretežito se sastoje od edukacija i podizanja svijesti zaposlenika o rizicima iz promatrane domene. Navedeno se većinski postiže donošenjem internih akata, odnosno pravilnika i standarda (normi) koji propisuju ispravno i odgovorno postupanje. Na najvišoj razini upravljanja riječ je o odgovarajućem delegiranju odgovornosti te formiranju sigurnosnih strategija upravljanja rizicima (Spremić, 2017).

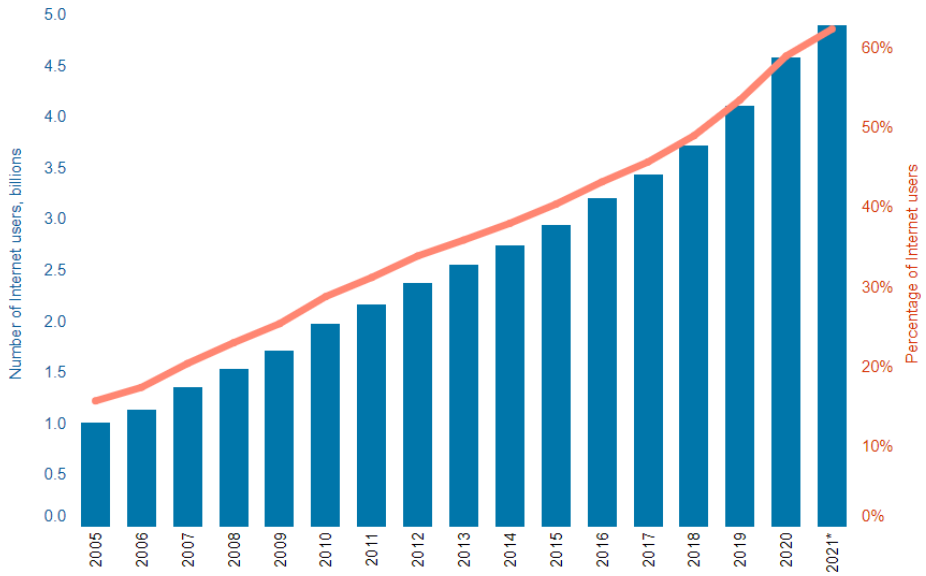
3.4 Povezanost pojave pandemije i kibernetičkog kriminala

Kao što to biva i u stvarnosti, kriminalci u virtualnoj sferi koriste svaku priliku koja im se pruži kako bi eksploatirali aktualne nedostatke i ostvarili svoje naume. Jedna od najvećih prekretnica proteklih desetljeća upravo je pojava i širenje virusa SARS-CoV-2, uzročnika bolesti COVID-19 (koronavirusa), koja je u protekle dvije godine zavladala svijetom.

Sama zaraza ovim dotad nepoznatim virusom započela je u prosincu 2019. godine u kineskom gradu Wuhanu. Prvi slučajevi govorili su o teškim slučajevima upale pluća za koje se činilo kako korijene vuku iz zajedničkog mjesta, goleme wuhanske tržnice na kojoj se trgovalo živim životinjama. Kineski ogranak svjetske zdravstvene organizacije zaprimio je vijesti o rastućem broju slučajeva zaraze, no kineske vlasti oštro su demantirale i cenzurirale sve informacije o ovoj bolesti. Zaraza se postupno počela širiti Kinom, ali i ostatkom svijeta, uz istovremenu neizvjesnost Svjetske zdravstvene organizacije oko proglašenja globalne zaraze, odnosno pandemije. Konačno, u ožujku 2020. godine WHO proglašava pandemiju, a s obzirom na eksponencijalni porast slučajeva zaraze, ali i smrti, gotovo sve države svijeta istovremeno proglašavaju izvanredno stanje. Kako bi se spriječilo daljnje širenje bolesti, zabranjene su sve vrste javnih okupljanja, rad gotovo svih ustanova maksimalno je ograničen ili u potpunosti prekinut te je izrazito preporučeno ili zakonom određeno smanjenje kretanja izvan mjesta prebivanja. Do današnjeg dana, COVID-19 bilježi periode jačih i slabijih intenziteta na koje se znanstvenici često referiraju nazivom „valovi“, koji pokazuju ciklički karakter ovisan o razdoblju godine te još uvijek ne pokazuju znakove stajanja. Zabilježeno je preko 540 milijuna slučajeva zaraze, a sama bolest odnijela je preko 6 milijuna života (European Council, 2022).

Opisana pandemija rezultirala je drastičnim promjenama u gotovo svim aspektima društva današnjice. Neki od njih su gospodarske prirode kao npr. ekonomska kriza i pojava dosad neviđenih tržišnih fenomena, rastući pritisci na zdravstveni sustav, propadanje nekih od najstabilnijih organizacija i poslovnih modela, masovni prekidi radnih odnosa, ali i društvene promjene kao što su kulturološki, sociološki i psihološki odmaci od dotadašnjih društvenih interakcija, stavova i navika ljudi. Iako tragičan, fenomen širenja virusa donio je i neke pozitivne promjene. Naime, potreba za smanjenjem fizičkog kontakta dodatno je potakla migraciju u virtualnu dimenziju podržanu digitalnim tehnologijama. Mnoge organizacije, suočene s egzistencijalnim pitanjem, započinju proces „prisilne“ digitalne transformacije te ubrzo uviđaju kako im digitalne tehnologije nude širok spektar mogućnosti i dovode do konkurentskih prednosti.

Slika 5. Ukupni i postotni porast svjetskog stanovništva koje se koristi Internetom u prvoj godini pandemije



ITU (2022), Internet use, *https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/, pristupljeno 19.6.2022*.

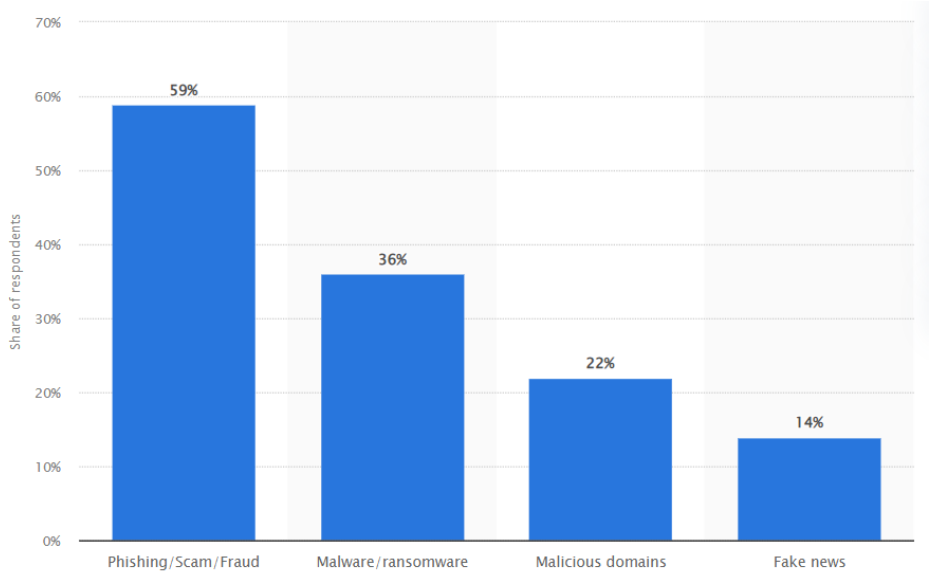
Tijekom pandemije Internet postaje glavnim sredstvom koje omogućuje interakciju s drugim članovima društva, a za mnoge jedini kanal za rad, učenje i pristup osnovnim javno dostupnim uslugama. Porast globalnog stanovništva koje se koristi Internetom iznosio je 10.2%, što ga s prethodnih 4.1 milijarde ljudi (54% svjetskog stanovništva) povisuje na sadašnjih 4.9 milijarde (63% svjetskog stanovništva) i označava najveći postotni porast broja korisnika Interneta promatran u jednom desetljeću (ITU, 2022).

Procjenjuje se kako je COVID-19 znatno skratio vrijeme potrebno za provođenje kvalitetne digitalne transformacije. Gotovo svi poslodavci započeli su sa znatno izdašnijim ulaganjima u digitalne inicijative, kanale i resurse, a napore u kreiranju u digitalne strategije sada vide kao imperativ u održivom poslovnom uspjehu u budućnosti. Globalno izvanredno stanje mnogima postaje prilika za nove poslovne pothvate, ali i revitalizaciju posrnulog poslovanja (LaBerge et al., 2020).

Iako poželjna i pozitivna, seoba svih interakcija i transakcija u novu, virtualnu dimenziju sa sobom nosi već spomenute rizike. Isključiva prisutnost u internetskom svijetu implicira golemu izloženost tehnološkim prijetnjama, tj. kibernetičkim rizicima. Ovaj pomak nije prošao neopaženo od strane kibernetičkih kriminalaca. Oni sveopće inicijalno stanje panike i nesigurnosti koriste za dodatna nanošenja šteta i ostvarivanje koristi kroz nelegalne aktivnosti.

Interpol prijetnje svrstava u 5 velikih skupina: maliciozne domene, online prevare i *phishing*, maliciozne programe namijenjene prikupljanju podataka, disruptivne programe namijenjene onemogućavanju pružanja usluga i masovno dezinformiranje javnosti. Interpolovi stručnjaci naglašavaju kako ubrzana digitalna transformacija, iako prijeko potrebna, nije temeljito provedena, odnosno zapaženi su veliki nedostaci u kreiranju politika i strategija digitalne obrane. Također, predviđaju budući porast svih navedenih oblika kriminala te zagovaraju kreiranje globalnog sustava zaštite i obrane od kibernetičkih prijetnji koji je već u razvoju (Interpol, 2020). Europska policijska akademija (CEPOL) skreće pozornost na sve veće korištenje malicioznih programa (*malwarea*) namijenjenog mobilnim telefonima, gdje sam razvoj obrambenih programa ne prati učestalost korištenja ovih uređaja, kao ni uznapredovale računalne viruse iz ove domene. Navode i značajan porast u online prevarama vezanima uz (pre)prodaju medicinskih pomagala povezanih s koronavirusom, kao što su oprema za testiranje, zaštitne maske, samo cjepivo i sl. (Coman i Mihai, 2022). Microsoft prati kibernetičke incidente povezane s pandemijom COVID-19 od njenih samih početaka. Bilježe velik inicijalni porast u incidentima, a glavnim motivom za porast broja uspješnih napada smatraju znatiželju i nesigurnost pojedinaca te njihovu želju za informiranjem (Microsoft, 2020). Ono oko čega se slažu sve navedene institucije i organizacije je činjenica da je došlo do znatnog porasta u aktivnostima uključenima u kibernetički kriminal te se predviđa kako će se ovaj trend dodatno produbiti u budućnosti.

Slika 6. Postotni porast najzastupljenijih kibernetičkih prijetnji u 2020. godini



Statista (2022), Key cyberthreats related to the COVID-19 pandemic in 2020, by threat type, *https://www.statista.com/statistics/1257198/main-covid-19-cyberthreats/, pristupljeno 20.6.2022.*

Ono oko čega se stručnjaci unutar navedenih institucija, ali i sama znanstvena zajednica također slažu je činjenica da su napadi usmjereni na krađu digitalnog identiteta jedan od najzastupljenijih pandemijskih rizika. Ovisno o obuhvatu istraživanja, gotovo uvijek se nalaze u tri najzastupljenije prijetnje usmjerene pojedincima i organizacijama. Potreba za konstantnim online prisustvom, kao i potvrđivanjem vlastitog identiteta u virtualnim transakcijama kao što su rad na daljinu, obrazovanje na daljinu, online trgovina i sl., daju kriminalcima mnoštvo prilika za dobivanje identifikacijskih informacija putem kojih se kasnije mogu lažno predstavljati. Također, oblici kibernetičkog kriminala koji se odnose na krađe identiteta kao što su *phishing*, društveni inženjering i drugi oblici, često služe kao alat koji osim krađe identiteta dovodi do velikih šteta na razini široj od samog pojedinca (npr. putem *ransomwarea* i *malwarea*). Istovremeno, Onfido, tehnološka tvrtka koja se bavi verifikacijom identiteta, provela je istraživanje nad 400.000 korisnika u kojem istražuje je li došlo do promjena u stavovima prema digitalnom identitetu u protekle dvije godine. Rezultati govore kako 60% ispitanika na dnevnoj bazi dijeli informacije vezane uz svoj digitalni identitet češće nego prije pandemije, dok je samo 13% njih uvjereno kako neće doći do povreda istog (Onfido, 2022). Navedeno upućuje na pad u povjerenju vezanom uz dijeljenje privatnih identifikacijskih informacija, kao i za novim, pouzdanijim rješenjem za upravljanje vlastitim digitalnim identitetom.

Lallie et al. (2021) u svojem iscrpnom pregledu incidenata u tromjesečnom razdoblju između ožujka i svibnja 2020. godine analiziraju globalnu scenu kibernetičkih prijetnji i njezin utjecaj na Ujedinjeno Kraljevstvo. Istraživanje se sastojalo od dubinskog uvida u statistiku internetskih pretraga koje uključuju kombinacije riječi iz domene koronavirusa i kriminalnih aktivnosti omogućenih kibernetičkim putem. Rezultati istraživanja jasno ukazuju kako je daleko najzastupljeniji oblik napada bio upravo *phishing*, koji se na globalnoj razini spominje u postotku od 37% svih izvršenih napada, a u samom Ujedinjenom Kraljevstvu zaslužan je za 86% ukupnih počinjenih napada. Autori u zaključku navode kako je ljudska nepažnja, koja je često glavni okidač uspješnih napada krađe identiteta, potaknuta osjećajem neizvjesnosti i potrebom za što bržim pronalaskom informacija. Predviđaju smanjenje udjela napada krađe identiteta u ukupnim kibernetičkim napadima, no svejedno ih ocjenjuju izrazito ozbiljnom prijetnjom.

4. PHISHING

4.1 Teorijski okvir phishinga

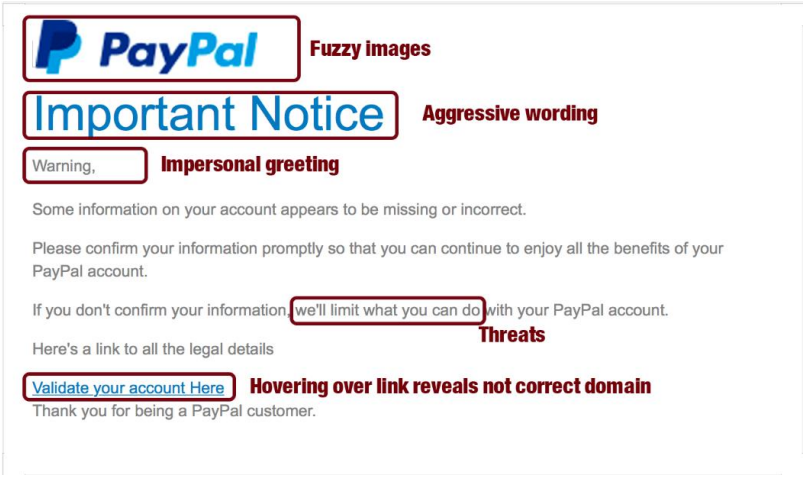
Phishing je najzastupljenija vrsta digitalne prevare počinjene kroz lažno predstavljanje (oponašanje) od strane počinitelja, tijekom kojeg se nastoji obmanuti metu napada na način da ona vjeruje kako je u interakciji s legitimnom osobom ili institucijom (CERT, 2022). Krajnji cilj *phishinga* može poprimiti dva oblika, a to sue krađa povjerljivih identifikacijskih podataka mete ili distribuiranje zlođudnog računalnog koda na računalo i računalni sustav. U prvom slučaju, napadači žele pristupiti korisničkim podacima mete kao što su identifikacijski podaci (korisničko ime i lozinka) kako bi dobili pristup nekom sustavu, ili broj kreditne kartice koji kasnije koriste pri počinjenju financijskih transakcija i nanošenju novčane štete. Sama distribucija malicioznih programa najčešće služi kao način otvaranja „kanala“ putem kojeg kriminalci kasnije mogu pristupati računalnom sustavu, ali i kao alat ucjene koja se ostvaruje onemogućavanjem funkcija i pristupa sustavu. *Phishing* napadi najčešće se pokušavaju ostvariti putem e-mail poruka (96% slučajeva) u kojima se primatelja navodi da unese određene identifikacijske podatke ili klikom na određeni link pristupi nekoj internetskoj stranici (CERT, 2022).

Pretpostavlja se da su prvi *phishing* napadi nastali oko 1995. godine, ali široj javnosti su postali poznati tek desetak godina kasnije. Samo ime upućuje na postavljanje „mamaca“ putem lažnih e-mail poruka i web stranica (eng. *fishing* = pecanje), a zamjena slova *f* slovima *ph* referira se na prve hakere koje se nazivalo *phreakovima*. Sami izraz prvi put se spominje početkom 1996. godine, a prvi napadi sastojali su se od krađa korisničkih lozinki koje su se potom koristile za kreiranje zahtjeva za izdavanje kreditnih kartica. Kriminalci potom počinju kreirati elektroničke poruke koje od primatelja traže da potvrde svoje korisničke podatke ili podatke o naplati, a ova praksa nastavlja se sve do danas. Početkom 2000-ih kriminalci kreću s napadima na online sustave plaćanja kao što su eBay i PayPal, a incidenti su samo u 2004. godini zahvatili oko 1.2 milijuna ljudi u SAD-u i uzrokovali štetu u ukupnom iznosu od gotovo jedne milijarde dolara (Phishing.org, 2022). Iako temeljna metodologija napada ostaje ista, *phishing* napadi kontinuirano evoluiraju. Danas su najzastupljenija online prijetnja čije otkrivanje postaje sve teže, a nanesene štete sve dramatičnije te često nadilaze sam financijski aspekt. Mnoge

organizacije, čija djelatnost obuhvaća kibernetičke rizike i kibernetičku sigurnost, kao glavne oblike *phishinga* navode *phishing* putem e-maila, *spear phishing*, *whaling* te *smishing* i *vishing*. E-mail *phishing* najzastupljeniji je oblik *phishinga*, a podrazumijeva registraciju lažne internetske domene koja imitira legitimnu. Ovaj oblik može poprimiti nekoliko podvrsta, odnosno metoda prevare, koje uključuju zahtjeve za unosom korisničkih podataka, lažne linkove i lažna web mjesta (CERT, 2022). *Spear phishing* također podrazumijeva elektroničku poštu, no za razliku od ostalih napada, kriminalci već imaju određene informacije o samoj meti, tako da je sami napad ciljano usmjeren ka pojedincu ili skupini unutar neke organizacije te ga je znatno teže otkriti. Whalingom se nazivaju *spear phishing* napadi usmjereni na same izvršne osobe unutar neke organizacije. Želi se iskoristiti njihova preokupiranost poslom kako bi se napadači domogli velikih financijskih iznosa. *Smishing* i *vishing* karakteristični su po tome što glavno sredstvo napada nije e-mail, već SMS poruke i telefonski pozivi (IT governance, 2022).

Nekoliko je klasičnih indikatora putem kojih je moguće prepoznati pokušaj *phishinga*. Prvo, gotovo uvijek su poslani s javne e-mail domene, gdje samo ime domene zna biti krivo napisano. Pozdrav, odnosno adresiranje osobe kojoj je poruka namijenjena skoro uvijek je općenito, generalizirano. Sama poruka može sadržavati previše gramatičkih pogrešaka i zatipaka, a stil pisanja odstupa od konteksta poruke. Konačno, sama poruka implicira stanje hitnosti i od primatelja zahtijeva žurno djelovanje, inače posljedice mogu biti kobne. Ukoliko poruka sadrži link (URL), prelaskom kursora preko njega prikazuje se ime lažne domene (IT governance, 2022).

Slika 7. Prikaz phishing *e-maila*



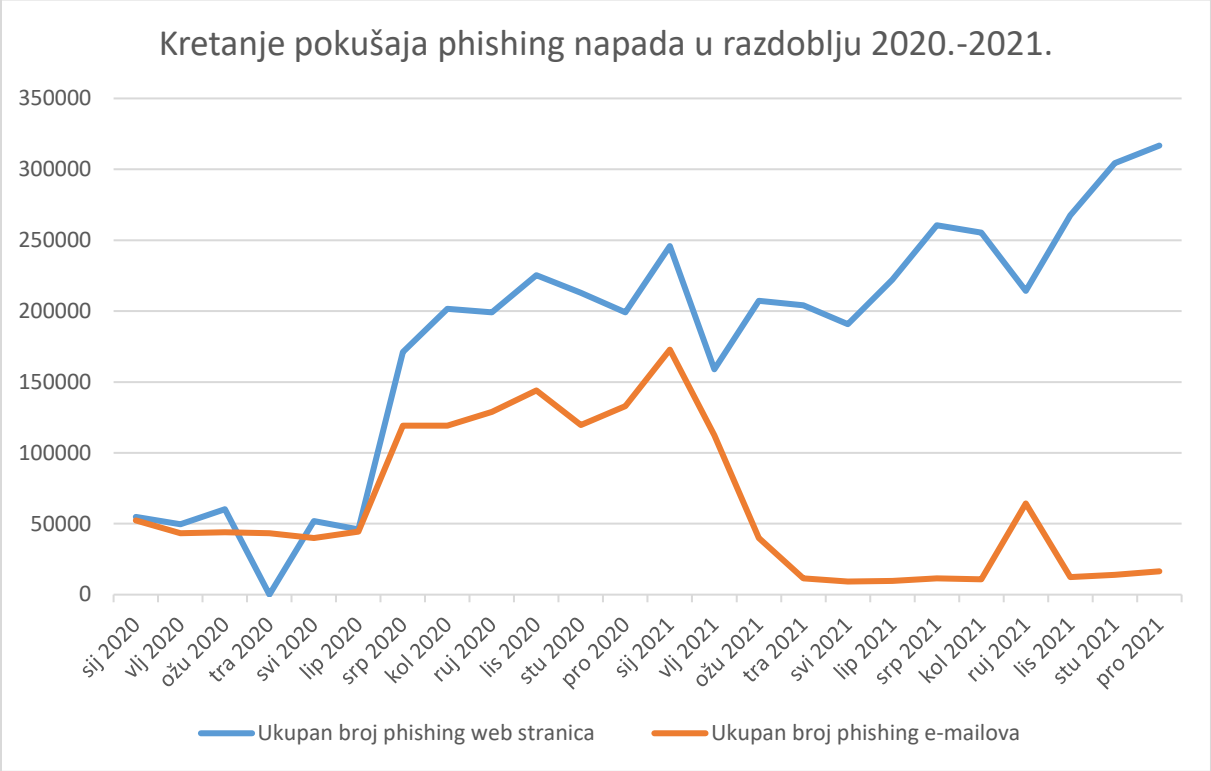
AWAREGO (2022), 6 ways to recognize phishing emails and how to avoid being scammed, *https://awarego.com/recognize-phishing-emails-avoid-being-scammed/, pristupljeno 23.6.2022.*

4.2 Obilježja phishing napada u uvjetima pandemije

Razdoblja velikih kriza, nesigurnosti i tenzija prikladno su plodno tlo za počinjenje bilo koje vrste kriminala. Događaji kao što su intenzivna politička previranja i svrgavanja s vlasti, ratovi, tržišne nestabilnosti, ali i teroristički napadi i epidemiološke krize većeg razmjera, sve češće poprimaju digitalni karakter i sele se u virtualnu sferu. Sukladno tome, kriminalne aktivnosti počinjene u informatičkom okruženju postaju neizostavan i neželjen rezultat ovih i sličnih događaja. Nedavna pandemija svakako nije činila iznimku. Sveopća migracija u online okolinu s pokušajem ograničavanja širenja zaraze učinila je svjetsko stanovništvo izrazito ranjivim na sve oblike kibernetičkog kriminala.

Vrsta incidenta koju je svakako važno naglasiti je upravo *phishing*, posebice napadi počinjeni u samim počecima pandemije. Naime, zapažen je dotad nezabilježeni porast u prijavljenim i počinjenim incidentima ovog tipa. *Phisheri* su pokušali iskoristiti ljudski strah od zaraze virusom i hitnost u traženju informacija oko same bolesti i zaštitne opreme. Izazvali su ono što se naziva „infodemijom“, odnosno lažnim širenjem informacija koja je plodno tlo za iskorištavanje slabosti (Frontierin). Dolazi do porasta broja e-mailova s tematikom virusa te sukladno tome, broja *phishing* stranica na koje će primatelj e-maila doći klikom na URL poruke. APWG (*Anti-Phishing Working Group*) u svojim kvartalnim izvještajima prati statistiku pokušaja *phishing* napada unazad 15 godina. Korištenjem podataka iznesenih u izvještajima dobiven je grafikon koji se nalazi na *slici 8*. Pokušaji napada putem lažnih web stranica (domena) na koje se nastoji usmjeriti korisnika u kontinuiranom je porastu uz manje oscilacije. S druge strane, pokušaji napada putem lažnih e-mailova pokazuju tendenciju rasta sve do siječnja 2021. godine, kada kreće razdoblje pada. Navedeno upućuje na strategiju napuštanja samih e-mailova i ulaganje dodatnih napora lažne web stranice kao glavni vektor napada. APWG također navodi kako kriminalci uviđaju da sama taktika zahtjeva za odavanjem povjerljivih podataka više nije uspješna kao prije, a ljude postaje lakše zavarati imitiranjem same web lokacije. *Phishing* e-mailovi tako postaju sve sofisticiraniji i poprimaju formu prethodno spomenutih *spear phishing* i *whaling* napada. Ova kombinacija čini *phishing* napade izuzetno moćnim napadima usmjerenima krađi identiteta i distribuciji zlućudnog koda, što dovodi do veće vjerojatnosti uspjeha samih napada (APWG, 2022).

Slika 8. Kretanje pokušaja *phishing* napada u razdoblju 2020.-2021.



Izvor: djelo autora

Provedenu analizu potvrđuju i druge organizacije i internetske zajednice usmjerene na praćenje i prevenciju *phishinga* i kibernetičkog kriminala općenito. F5 tako navodi porast od 220% u ukupnim incidentima povezanima uz *phishing* u odnosu na uobičajeni godišnji prosjek (F5, 2022). Globalno je preko 80% organizacija zamijetilo porast u pokušajima *phishing* napada od početka pandemije (Ironscales, 2021). Opisane trendove navele su čak i institucije kao što su američki FBI i europska ENISA na alarmiranje javnosti o ovoj rastućoj prijetnji.

Akdemir i Yenal (2021) odlučili su provesti temeljito empirijsko istraživanje *phishing* incidenata. Kao temeljnu motivaciju navode zabrinjavajuće statistike kao što je 18 milijuna zabilježenih *phishing* i *malware* napada u travnju 2020. Napade kategoriziraju u 9 vrsta, i to su redom: poruke koje nude informacije koje će pomoći u suzbijanju zaraze, poruke u kojima se nudi financijska pomoć, poruke u kojima se nudi usluga, poruke u kojima se nudi lijek, poruke u kojima se navodi prijetnja, poruke u kojima se izvještava o isteku korisničkog računa, poruke u kojima se traži pomoć ili usluga te poruke koje nude edukacijske programe. Najveći broj krivotvorenih načina kontaktiranja (23%) odnosio se na oponašanje nekog državnog tijela. Zaključuju kako će se trend napada putem krađe identiteta nastaviti tijekom cijele pandemije.

Još jedan promatrani trend je porast napada na kritičnu infrastrukturu. Kritičnom infrastrukturom smatra se „odabrani skup sektora čija se imovina, sustavi i mreže, bilo fizičke ili virtualne, smatraju toliko vitalnim da bi njihovo onesposobljavanje ili uništenje imalo iscrpljujući učinak na sigurnost, nacionalnu ekonomsku sigurnost, nacionalno javno zdravlje ili sigurnost, ili bilo koju njihovu kombinaciju“ (CISA, 2022). Sektori koji su postali najciljanijom metom tijekom pandemije koronavirusa su zdravstveni, transportni i energetski sektor (Ardagna et al., 2021). Na posebnom udaru je zdravstveni sektor, gdje kriminalci iskorištavaju djelatnike čija je koncentracija i moć opažanja zbog izuzetnih napora ionako umanjena. APWG izvještava o godišnjem porastu od 35% u napadima na zdravstveni sektor, dok neki drugi izvori iznose gotovo četiri puta veće brojke. Analiza incidenata ukazuje na to da kriminalci dolaze do identifikacijskih podataka zdravstvenih djelatnika te ih koriste za dobivanje pristupa mreži, koju potom onesposobljavaju za rad putem DoS (*Denial of Services*), no češće i *ransomware* napada. Tako inficirana infrastruktura dodatno otežava aktivnosti preopterećenog zdravstvenog sustava čiji su kapaciteti tijekom cijele pandemije iskorišteni do maksimuma. Kriminalci se nadaju kako će ova činjenica dodatno zastrašiti donositelje odluka i potaknuti ih na isplaćivanje zahtijevanih iznosa.

Uzevši u obzir spomenute činjenice, može se zaključiti kako su obilježja *phishing* napada tokom trenutne pandemije sljedeća:

- *Phishing* napadi osnova su za širenje dezinformacija, panike i lažnih vijesti u samim počecima pandemije
- Dolazi do znatnog porasta u kibernetičkim napadima iz domene *phishinga*
- *Phishing* napadi u početku bilježe porast u svim svojim oblicima
- S vremenom broj napada putem lažnih e-mailova pada, dok je broj napada putem lažnih web mjesta i dalje u porastu
- Promjenama u strategiji samih napada povećava se njihova sofisticiranost i uspješnost
- Zamijećen je i porast napada na kritičnu infrastrukturu, posebice zdravstveni, energetski i transportni sektor.

ENISA (*European Union Agency for Cybersecurity*) navodi još jedan novitet, a to je uvođenje PhaaS (*Phishing*-as-a-Service) napada. Riječ je o napadima koji slijede SaaS (Software-as-a-Service) poslovni model, odnosno plaćanje nekoj osobi kako bi razvila cjelokupnu *phishing* kampanju, od samog lažnog e-maila ili web lokacije do integracije i distribucije malicioznog koda (Ardagna et al., 2021).

4.3 Analiza odabrane studije slučaja

Kako bi se u potpunosti shvatila ozbiljnost i doseg *phishing* napada tijekom same pandemije, prvo će ukratko biti predstavljena nekolicina najpoznatijih *phishing* napada u proteklih deset godina, nakon čega slijedi temeljita analiza odabrane studije slučaja tijekom same pandemije.

Kao što je već spomenuto, *phishing* napadi prisutni su u online sferi dugi niz godina. Sama krađa identiteta izazvana ovim putem izuzetno je ozbiljan prekršaj koji može uzrokovati dugoročne financijske, emotivne i mnoge druge posljedice. Jedan od financijski najštetnijih incidenata uzrokovanih p*hishingom* je onaj povezan s krađom 100 milijuna dolara u kojem su oštećeni Facebook i Google. Evaldas Rimasauskas smatra se predvodnikom skupine koja je između 2013. i 2015. godine slanjem *phishing* e-mailova ovim tehnološkim divovima otela velike novčane iznose. Naime, kriminalna skupina osnovala je fiktivnu tvrtku koja je nalikovala pravoj, Quanta Computers, koja je stvarni partner Facebooka i Googlea. Počinitelji su slali relativno dobro oponašane e-mailove zaposlenicima zaduženima za višemilijunske transakcije, na koje su zaposlenici nasjeli i izvršili isplatu sredstava. Skupina je uložila iznimne napore kako bi oponašanje identiteta prošlo nezamijećeno, no 2015. godine ipak biva otkrivena, a njen prethodnik uhapšen i osuđen zbog krađe (Cnbc, 2019).

Medijski najeksponiraniji *phishing* incident povezan je s američkom medijskom kućom Sony Pictures Entertainment, podružnicom japanskog Sonyja. Naime, napad je počinila kriminalna organizacija koja se povezuje sa Sjevernom Korejom, a temeljnom motivacijom se smatra osveta za produkciju i distribuciju filma *The Interview*, komedije koja na satiričan način prikazuje Sjevernu Koreju i njenog poglavara Kim Jong-Una. Smatra se kako su napadači odmah po najavi započinjanja snimanja filma krenuli sa slanjem *phishing* e-mailova zaposlenicima kompanije. Putem njih su postupno dobivali kontrolu nad SPE-ovom mrežom i podacima. Izvršili su niz napada kojima su dobili pristup povjerljivim podacima i naštetili sustavu. 14. studenog 2014. godine napadači određenim novinarima šalju golemu količinu informacija o samoj kompaniji i njenim zaposlenicima. Uslijedio je niz prijetnji i ucjena kojima se sam film nastojao spriječiti od prikazivanja, no SEP ih je odlučio zanemariti. Američki predsjednik i sigurnosne agencije oštro su osudile ovaj napad, a počinitelji ispunjavaju prijetnje i javno objavljuju informacije u proljeće 2015. godine. Napad je znatno naštetio poslovanju SPE-a (Horton i Desimone, 2018).

Za razliku od *phishing* napada prije same pandemije, tijekom nje znatno je porastao interes za napade na kritičnu infrastrukturu. Zdravstveni sektor tradicionalno je bio jedna od omiljenih meta kiberkriminalaca, no u posljednje dvije godine trend iskorištavanja preopterećenosti bolničkog i zdravstvenog sustava gotovo postaje standardom. Odabrana studija slučaja promatra napad počinjen na bolnički centar Sveučilišta u Kaliforniji, u San Diegu. Počinjen u proljeće 2021. godine, ovaj napad znatno je financijski oštetio bolnicu te rezultirao kompromitiranjem povjerljivih informacija pacijenata i zaposlenika te postao reprezentativnim primjerom krađe identiteta uslijed aktualne pandemije.

Sigurnosni tim bolničkog centra Sveučilišta u Kaliforniji tijekom ožujka 2021. godine zamijetio je sumnjive aktivnosti na svojoj mreži, no bilo im je potrebno gotovo mjesec dana kako bi s pouzdanošću ustanovili da je došlo do sigurnosnih proboja njihove mrežne infrastrukture. Nije točno ustanovljeno kada je napad počeo niti koliko su kriminalci bili prisutni unutar same mreže, ali sam incident je prijavljen FBI-u i vanjskim ekspertima kako bi se otkrili pravi razmjeri počinjene štete. Ustanovljeno je kako je inicijalni vektor napada *phishing* e-mail putem kojeg su počinitelji obmanuli jednog od zaposlenika i dobili pristup bolničkom informacijskom sustavu. Napadači su tako dobili pristup podacima kao što su puno ime, adresa, datum rođenja, e-mail adresa, broj telefaksa, informacije o zahtjevima (datumima i cijenama) zdravstvenih usluga, laboratorijski rezultati, medicinska dijagnoza i stanja, brojevi medicinske dokumentacije i drugi medicinski identifikatori, informacije o receptima i liječenju, medicinske informacije, broj socijalnog osiguranja, državni identifikacijski broj, broj kreditnih kartica ili financijskih računa, broj studentske iskaznice te korisničko ime i lozinka gotovo svih pacijenata, osoblja i studenata liječničkog centra (Healthcare IT news, 2021). Centar je odmah priznao odgovornost te obavijestio sve potencijalne žrtve o kompromitaciji i mogućnosti zlouporabe njihovih podataka. Najveći rizik predstavlja krađa podataka o medicinskoj povijesti jer se ovim putem na ilegalan način mogu dobiti lijekovi i pokrenuti zahtjevi za medicinskim zahvatima. Također, moguće je i otvaranje korisničkih kreditnih računa i počinjenje financijske štete. Krađa broja socijalnog osiguranja u SAD-u također otvara šanse za ostvarivanje financijskih koristi kao što su vladine financijske olakšice i sl.

Trenutačno je u tijeku sudski proces u kojem je Bolnički centar tužen za povredu korisničkih podataka kroz nemarno ponašanje. Također se navode nemar, kršenje ugovora i kršenje državnih zakona o privatnosti podataka i medicinskoj povjerljivosti. Uviđajem je utvrđeno kako su kriminalci imali pristup sustavu gotovo 5 mjeseci, a „procurili“ su podaci gotovo 500.000 osoba. Centar je, kao kompenzaciju, ponudio svim oštećenima godinu dana besplatnih

medicinskih usluga i kreditnog praćenja putem svojeg osiguravajućeg društva. Financijski iznos počinjene štete još uvijek nije u potpunosti utvrđen (The San Diego Union-Tribune, 2021).

Iz studije slučaja moguće je donijeti nekoliko sigurnosnih preporuka glede same zaštite od *phishing*a. Preporuke tako uključuju:

- Razvoj, implementaciju i kontinuirano prakticiranje strategije kibernetičke sigurnosti
- Edukaciju i osposobljavanje zaposlenika o rizicima i načinima prepoznavanja *phishinga*
- Upućivanje na obraćanje pozornosti i kritičko promišljanje kad je riječ o sumnjivom sadržaju koji je prezentiran, posebice onom koji se odnosi na odavanje povjerljivih informacija
- Ažuriranje postojećih i donošenje novih informacijskih sigurnosnih kontrola
- Kontinuirano ulaganje u hardverske i softverske elemente mrežne infrastrukture
- Praćenje trendova kada je riječ o informatičkim sigurnosnim mjerama, ali i incidentima
- Korištenje antivirusnih i zaštitnih programa

Važno je spomenuti kako iako primarna, kritična infrastruktura nije jedina meta napada digitalne krađe identiteta. Neki od značajnijih napada zabilježenih tijekom pandemije su masovne prevare putem zahtjeva za autorizacijom korisničkih računa Microsoft Office 365 paketa kojima su većinom ciljani viši menadžeri pojedinih organizacija, ali i napadi usmjereni na krađu povjerljivih podataka onih korisnika koji su zbog zatvaranja kino dvorana dugo očekivane filmove željeli pogledati putem ilegalnih streaming servisa (IT governance, 2022). Zajednička karakteristika ovih napada je činjenica da se iskorištava isključiva ovisnost društva o tehnologiji pri obavljanju kako poslovnih, tako i ležernih aktivnosti u vrijeme pandemije. Posebna pozornost se skreće na slučaj kampanje darivanja PlayStation 5 igraće konzole. U ovom slučaju iskorištena je činjenica da na globalnoj razini nedostaje silicija potrebnog za ugradnju u mikročipove koji su danas dio svakog elektroničkog uređaja, što dovodi do nestašica mnogih uređaja na tržištu. Počinitelji su u ovom slučaju pokušavali imitirati farmaceutsku kompaniju India Pharma koja u stvarnosti nije provodila nikakav nagradni natječaj. Putem lažnih elektroničkih poruka primatelja se usmjerava na podjednako lažnu Amazonovu stranicu, gdje se na njega odbrojavanjem vremena u kojem je konzola dostupna vrši pritisak ne bi li upisao podatke svoje kreditne kartice te adresu, poštanski broj, e-mail i broj telefona

(Kaspersky, 2022). S obzirom na dokolicu i dosadu uzrokovanu izolacijom, kao i veću online prisutnost nego u normalnim uvjetima, pretpostavlja se kako je ovoj lažnoj akciji darivanja pristupilo više ljudi nego što bi to inače bio slučaj, no Kaspersky još nije objavio konkretnu brojku pojedinaca koji su na prevaru stvarno i nasjeli.

5. DRUŠTVENI INŽENJERING

5.1 Teorijski okvir društvenog inženjeringa

Društveni inženjering najsofisticiranija je tradicionalna metoda digitalne krađe identiteta. Može ga se okarakterizirati kao sofisticiraniju, usko ciljanu vrstu *phishinga* koja gotovo graniči sa *spear phishingom*. Društveni inženjering u potpunosti je umjeren na psihološki segment kibernetičke sigurnosti, odnosno na ljudsku tendenciju povjerljivosti drugima. Ova visokorazvijena kriminalna aktivnost podrazumijeva iniciranje komunikacije s pojedincem putem informacija koje su kriminalcu već otprije poznate, a rezultat su detaljnog istraživanja mete napada. Na ovaj način znatno se poboljšava vjerojatnost uspjeha samog napada, a manipulacija osobom dovodi se na potpuno novu razinu. Za razliku od ostalih napada krađe identiteta koje je donekle moguće spriječiti tehničkim sigurnosnim mjerama, napadi društvenog inženjeringa zbog same činjenice da ciljaju ljudsku narav mogu biti detektirani, ali izrazito ih je teško ili gotovo nemoguće spriječiti. Tijekom samog napada pokušava se manipulirati žrtvom kako bi sama otkrila što više povjerljivih podataka pomoću kojih kriminalci mogu dobiti pristup nekom sustavu ili počiniti nezakonite financijske radnje. Napadi društvenog inženjeringa trenutno čine najkompleksniju masovnu kibernetičku prijetnju za koju stručnjaci još uvijek nemaju dovoljno efikasno rješenje (Salahdine i Kaabouch, 2019).

Sami tijek napada sastoji se od četiri koraka. Prvi korak naziva se istraživanje, odnosno prikupljanje informacija. U današnje vrijeme već spomenutog digitalnog otiska, sve je lakše putem internetskih izvora prikupiti razne podatke o osobama, bili oni poslovne ili privatne, javne ili povjerljive prirode. Počinitelji na temelju određenog kriterija odabiru žrtvu te prikupljaju što više dostupnih podataka o njoj kako bi joj pristupili sa što većom dozom lažne prisnosti. Slijedi faza pristupanja i uspostavljanja odnosa sa žrtvom čiji je krajnji cilj uspostava odnosa povjerenja. Ovaj korak moguće je provesti uživo, bez uporabe tehnoloških rješenja (zbog čega se društveni inženjering smatra znatno starijom prevarom od izuma samih računala) ili računalnim putem, kroz e-mail ili neke druge digitalne kanale. Treća faza je tzv. faza igre u kojoj se koristi prethodno uspostavljen odnos kako bi se pridobile povjerljive informacije žrtve.

U posljednjoj fazi, fazi izlaska, napadač nestaje bez traga nakon što je dobio potrebne informacije (Salahdine i Kaabouch, 2019).

S obzirom na to da je psihološko i emotivno manipuliranje osobom kako bi ona otkrila svoje povjerljive podatke moguće i bez uporabe informacijsko-komunikacijske tehnologije, smatra se kako „vještina“ društvenog inženjeringa korijene vuče daleko u ljudsku povijest. No, društveni inženjering počinjen modernim putem kakav se podrazumijeva i danas, započinje sredinom 1990-ih, u isto vrijeme kada i *phishing*. Upravo zbog zajedničkog podrijetla mnogi autori smatraju *phishing* samo jednim od pojavnih oblika suvremenog društvenog inženjeringa. Dolazi do razvoja ove vrste kriminala, tako da društveni inženjering danas poprima sve već navedene forme *phishinga*, uz neke dodatne pojavne oblike. Riječ je o *pretextingu* i obrnutom društvenom inženjeringu. U *pretexting* napadima počinitelj oponaša zaposlenika organizacije s kojom je žrtva već u kontaktu i ima uspostavljen odnos povjerenja. Ovaj oblik napada podrazumijeva prethodno prikupljanje informacija o pojedincu kojim započinje faza prikupljanja informacija. Obrnuti društveni inženjering uključuje interakciju u kojoj kriminalac uvjerava metu da ima određenih problema te prezentira određeno rješenje. Pojedinac potom samoinicijativno stupa u interakciju s napadačem i biva uvučen u uspostavljanje odnosa povjerenja (CompTIA, 2022). Razvija se kompleksna klasifikacija napada društvenog inženjeringa koja je prikazana na *slici 9*. Riječ je o svim oblicima napada (bili oni fizički ili virtualni) koji podrazumijevaju dobivanje povjerljivih informacija o pojedincima nelegalnim putem.

Slika 9. Pojavni oblici suvremenog društvenog inženjeringa

MDPI (2019), Social engineering attacks: a survey, *https://www.mdpi.com/1999-5903/11/4/89*, *pristupljeno 26.6.2022.*

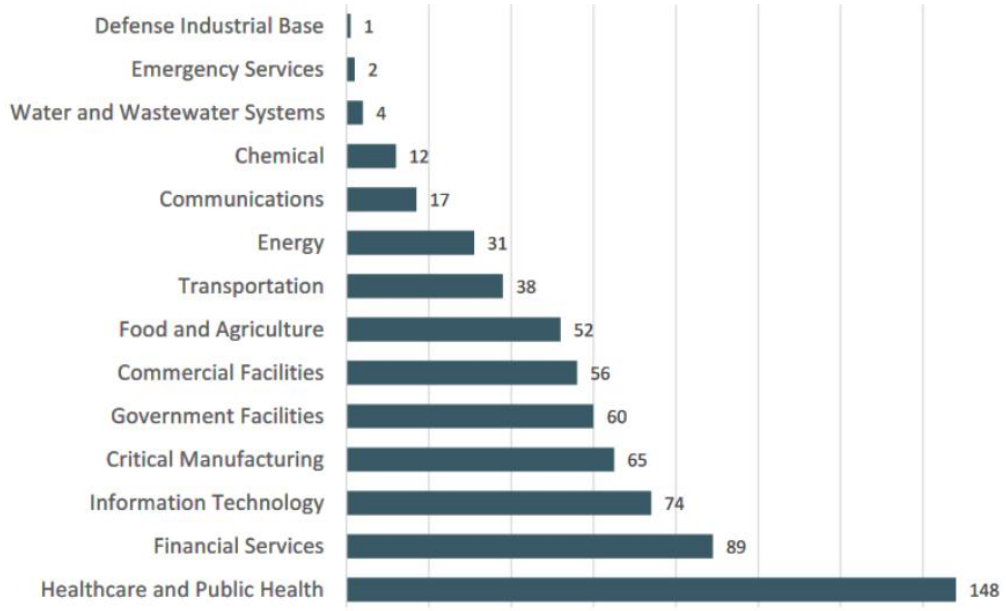
5.2 Obilježja napada društvenog inženjeringa u uvjetima pandemije

COVID-19 dodatno produbljuje status društvenog inženjeringa kao najsofisticiranije kibernetičke prijetnje počinjene putem ljudskog faktora. Iako je neupitno da je došlo do porasta u broju ovog tipa napada, sama činjenica da je napade društvenog inženjeringa tradicionalno teško pratiti znatno otežava određivanje apsolutnog broja samih napada. Kontaktiranje s kriminalcima postaje toliko sofisticirano da ga je izuzetno teško detektirati, posebice ako o njemu ne postoji nikakav zapis. FBI aproksimira ovaj porast na 70% u prvoj godini pandemije, a ukupne gubitke procjenjuje na 1.8 milijardi dolara u promatranom razdoblju (Security Intelligence, 2021). Navedeno potvrđuje i Firewall Times s procjenama porasta od 74% u 2021. godini. S druge strane, Kaspersky navodi štetu počinjenu u 2020. godini prema navedenim oblicima društvenog inženjeringa, a to su *phishing*, *vishing*, *smishing*, *pharming*, krađa identiteta, prevare povjerenja i financijske prevare te kompromitacije poslovnih e-mailova. Navode kako je u 2020. ukupan broj ovih prevara zahvatio 345.406 pojedinaca i uzrokovao ukupnu štetu od gotovo 3 milijarde dolara. Također, uzevši u obzir prethodno promatrani trend porasta napada *phishinga*, koji je samo jedan od oblika društvenog inženjeringa, moguće je zaključiti da je došlo do porasta incidenata. Glavna razlika je činjenica da kriminalci, primarno zbog fizičkog distanciranja i izoliranja, napuštaju fizičke oblike društvenog inženjeringa, no zauzvrat masovno iskorištavaju one počinjene digitalnim putem. Pretpostavlja se kako je u 2021. godini čak 93-98% incidenata u većoj ili manjoj mjeri povezano s društvenim inženjeringom (Firewall Times, 2022).

Važno je izdvojiti dvije metode napada koje su se svojom učestalošću istakle na sceni kibernetičkog kriminala. Riječ je o kompromitaciji poslovnih e-mailova (*Business E-mail Compromise*, BEC) i *ransomware* napadima omogućenima putem društvenog inženjeringa. Obje metode kao krajnji cilj imaju ostvarivanje financijskih koristi putem kompromitacije segmenata računalne infrastrukture. BEC napadi su vrsta sofisticirane prijetnje tijekom koje napadači nastoje dobiti pristup e-mail računima visokopozicioniranih zaposlenika i zaposlenika zaduženih za odobravanje znatnih financijskih transakcija unutar organizacije (Venkatesha i Reddy, 2021). FBI izvještava kako je samo u 2021. godini prijavljeno 19.954 BEC-ova koji su rezultirali gubicima od 2.4 milijarde dolara. Prevare su za vrijeme trajanja pandemije dosegle sofisticiranu razinu koja je uključivala kompromitaciju e-maila osobe autorizirane za

odobravanje financijskih transakcija, nakon koje bi osobi koja te transakcije stvarno i provodi uslijedio poziv na virtualni sastanak. Na samom početku sastanka počinitelji bi postavili ranije preuzetu sliku osobe koja je inicirala sastanak, a sam nedostatak pomicanja pravdali bi lošom internetskom vezom. Potom bi odobrili prijenos sredstava osobi zaduženoj za njihovo obavljanje. Čim bi prijenos sredstava bio gotov, ona bi se odmah konvertirala u kriptovalute i proslijedila u digitalne novčanike kriminalaca. Drugi promatrani trend je distribucija *ransomwarea* putem društvenog inženjeringa. Kriminalci kontaktiraju pojedince i manipuliraju njima potičući ih na preuzimanje datoteka koje sadržavaju zloćudni kod koji potom zahvaća računalni sustav unutar kojeg se računalo na koje je preuzet paket nalazi. *Ransomware* potom kriptira podatke, čime onemogućuje daljnji rad sustava, te traži odštetu kako bi omogućio ponovni pristup. Kriminalci koji koriste ovaj oblik računalne ucjene uzdaju se u potrebu za što skorijim nastavkom odvijanja poslovanja koja bi potaknula žrtvu na isplatu tražene otkupnine. *Ransomwareom* se tradicionalno ciljaju i privatni i javni sektor. 80% organizacija sektora kritične infrastrukture doživjelo je *ransomware* napade u 2021. godini (Claroty, 2022), a samo u SAD-u je zabilježeno 649 ovakvih napada (Bleeping Computer, 2022). Hiji i Alam (2021) zapažaju kako su incidenti primarno vezani uz zdravstveni sektor, odnosno same medicinske ustanove i organizacije, ali ciljani su i ostali sektori kao što su energetski i telekomunikacijski.

Slika 10. Statistika *ransomware* napada na kritičnu infrastrukturu u SAD-u u 2021. godini



Bleeping Computer (2022), FBI: Ransomware hit 649 critical infrastructure orgs in 2021, *https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-649-critical-infrastructure-orgs-in-2021/*, pristupljeno 27.6.2022.

Na prikazanoj grafici očito je kako je daleko najciljaniji sektor upravo onaj zdravstveni, koji je u 2021. godini bio metom 22.8% sveukupnih napada ovog tipa.

Obilježja napada društvenog inženjeringa u uvjetima pandemije COVID-19 su sljedeća:

- Došlo je do porasta brojeva napada društvenog inženjeringa na globalnoj razini
- Iako je točan broj nemoguće odrediti, procjenjuje se kako se učestalost napada društvenog inženjeringa povećava po stopi od 70% godišnje
- Napadi društvenog inženjeringa postaju sve sofisticiraniji
- Dva najzastupljenija vektora napada društvenog inženjeringa tokom pandemije su napadi kompromitacije poslovnih e-mailova i napadi distribucije *ransomwarea* kroz društveni inženjering
- Prvi vektor napada povezuje se uz privatni sektor, dok je drugi vezan uz napade na kritičnu infrastrukturu, odnosno javni sektor
- Dolazi do porasta napada na institucije kritične infrastrukture kojima se želi doći do što većih ilegalnih financijskih koristi

5.3 Analiza odabrane studije slučaja

Promatrana studija slučaja odnosi se na *ransomware* incident omogućen putem društvenog inženjeringa kojim je u svibnju 2021. godine napadnut Colonial Pipeline, najveći američki naftovod. *Ransomware* je onemogućio pojedine dijelove sustava i učinio ga nedostupnim na razdoblje od tjedan dana. Ovaj događaj imao je toliki neželjeni efekt na cjelokupnu istočnu obalu SAD-a da ga je američki predsjednik proglasio izvanrednim stanjem. Istovremeno je riječ o najvećem kibernetičkom napadu na kritičnu infrastrukturu SAD-a u povijesti.

Colonial Pipeline najduži je američki naftovod koji se proteže od Meksičkog zaljeva do Istočne obale SAD-a. S radom je započeo 1926. godine, a danas se sastoji od gotovo 9000 kilometara cijevi te tako čini najveću mrežu opskrbe naftom u državi. Od vitalne je važnosti jer zadovoljava potrebe velikog dijela države za gorivom za automobile i zrakoplove, ali i za grijanje, zbog čega ga se opravdano svrstava u kritičnu infrastrukturu.

Napad započinje 6. svibnja 2021. kada kriminalci upadaju u sustav i vrše inicijalnu krađu podataka. Hakerska grupa je unutar dva sata ukrala više od 100 gigabajta povjerljivih podataka. 7. svibnja počinitelji nastavljaju s napadom na samu mrežu tijekom koje zadobivaju kontrolu nad funkcijama sustava kao što su računovodstvo i sustav naplate, pa Colonial Pipeline tek tada postaje svjestan napada. Kriminalci potom traže otkupninu u iznosu od 75 bitcoina, što je prema tadašnjim tržišnim vrijednostima bilo ekvivalentno iznosu od 4.4 milijuna dolara. Obzirom da služba za informacijsku sigurnost ne uspijeva suzbiti napad i vratiti kontrolu nad sustavom, angažira sigurnosnu tvrtku Mandiant s ciljem prekida napada i istraživanja cjelokupnog incidenta.

Temeljitim uviđajem utvrđeno je da su kriminalci pristup sustavu dobili upravo pomoću društvenog inženjeringa. Pretpostavlja se kako su otkrili lozinku VPN-a jednog od zaposlenika i putem ovladavanja VPN-om kao poveznicom s poslovnom mrežom kompanije zadobili kontrolu nad cijelim sustavom Colonial Pipelinea. Glavnim krivcem smatra se hakerska skupina DarkSide za koju se pretpostavlja kako potječe iz Rusije ili ostatka istočne Europe, a poznata je po svojim izrazito sofisticiranim *ransomware* napadima s velikom razinom uspješnosti. Mandiant u početku svoje intervencije ne uspijeva zadobiti kontrolu nad sustavom, zbog čega se Uprava Colonial Pipelinea odlučuje na plaćanje otkupnine. Kriminalci otkrivaju ključ za dekriptiranje, pa IT služba ponovo dobiva pristup sustavu, a uobičajeno poslovanje uspostavlja se 12. svibnja.

Posljedice koje je opisani incident ostavio na poduzeće i na američko društvo su značajne. Colonial Pipeline biva tužen te je u srpnju 2021. godine Uprava izvedena pred Kongres kako bi se održalo saslušanje o cijeloj situaciji. Ovaj događaj imao je negativne posljedice koje nadilaze granice same kompanije. Tijekom nedostupnosti usluga naftovoda došlo je do nedostatka zrakoplovnih goriva što je rezultiralo otkazivanjem mnogih letova u istočnom dijelu SAD-a. Ta informacija izazvala je paniku u javnosti, što je uzrokovalo ogromne gužve i na benzinskim crpkama u saveznim državama Floridi, Georgiji, Alabami, Virginiji te Sjevernoj i Južnoj Karolini. Panično kupovanje goriva postalo je toliko intenzivno da je ubrzo dovelo do znatnog poskupljenja cijene goriva na tom dijelu tržišta, a dodatno je produbilo već postojeće deficite zaliha. Što se tiče samog Colonial Pipelinea, Ministarstvo pravosuđa u suradnji sa sigurnosnima agencijama uspjelo je vratiti 65 od ukupnih 75 bitcoina otuđenih kroz ucjenu (TechTarget, 2022).

Opisani kibernetički incident upućuje na izuzetnu sofisticiranost, ali i teškoću otklanjanja samih problema jednom kad je napad počinjen. S obzirom na rastuću uspješnost napada kada je riječ

o ostvarivanju financijskih koristi, stručnjaci su uvjereni kako će ciljanje visokopozicioniranih ili ovlaštenih osoba nastaviti trend rasta, kako u javnom, tako i u realnom sektoru. Rastuća izloženost digitalnim načinima komunikacije postupno čini ljude podložnijima manipulaciji, zbog čega je potreba za novim, efektivnijim mehanizmima obrane sve veća.

Kada je riječ o napadima društvenog inženjeringa, sigurnosne preporuke koje bi minimizirale šanse za uspješno počinjenje napada su sljedeće:

- Kritičko promišljanje u online komunikaciji i interakciji s drugim pojedincima putem digitalnih kanala, posebice ako se zamijeti kako posjeduju informacije koje ne bi smjeli (što indicira da su do njih možda došli nelegalnim putem)
- Verificiranje osobe s kojom se virtualnim putem raspravlja o povjerljivim temama s ciljem utvrđivanja njihovog pravog identiteta
- Nepovjerljivost kada je riječ o otkrivanju povjerljivih informacija izvan kanala kojima se one inače dijele
- Prakticiranje politike čistog stola, odnosno ostavljanje elektroničkih uređaja i ostalih medija koji sadržavaju povjerljive podatke isključivo pod autoriziranim nadzorom
- Prakticiranje filozofije, ali i formalne organizacijske politike putem koje se određuju pojedinci i skupovi pojedinaca koji trebaju imati (zajednički) pristup određenim povjerljivim informacijama

Jedan od napada društvenog inženjeringa koji je odjeknuo u javnosti tijekom prve godine pandemije povezan je s društvenom mrežom Twitter. Naime, kriminalci su hakirali 130 računa visokoprofiliranih korisnika ove platforme koji su većinom bili medijski eksponirane osobe. Jednom kad su zadobili kontrolu nad korisničkim računima, krenuli su s masovnim objavljivanjem dobrotvorne akcije. Prevara se sastojala od zahtjeva za slanje bitcoina u dobrotvorne svrhe, odnosno fonda za financijsku pomoć najoštećenijima od strane pandemije. Ovdje kriminalci nastoje emocionalno manipulirati i iskoristiti empatiju korisnika Twittera u pomoći najugroženijima. Tvrdilo se kako bi donatori naknadno dobili dupli iznos bitcoina kao zahvalu za svoje uplate. Potaknuti lažnom inicijativom slavnih, mnogi su nasjeli na prevaru i donirali ukupni iznos od 12.83 bitcoina što je u to vrijeme bilo jednako ekvivalentu od gotovo 150,000 američkih dolara. Analizom napada utvrđeno je kako je napad pomno usmjeren na malu grupu zaposlenika koja je bila autorizirana koristiti alate za upravljanje korisničkim računima. Kada je dobiven pristup korisničkom računu samo jednog zaposlenika, infiltrirana je

i cjelokupna mreža. Promatrani napad ukazuje na činjenicu kako društvene mreže mogu biti moćan medij u počinjenju prevara krađe identiteta (HKCERT, 2020).

6. DEEPFAKE TEHNOLOGIJA

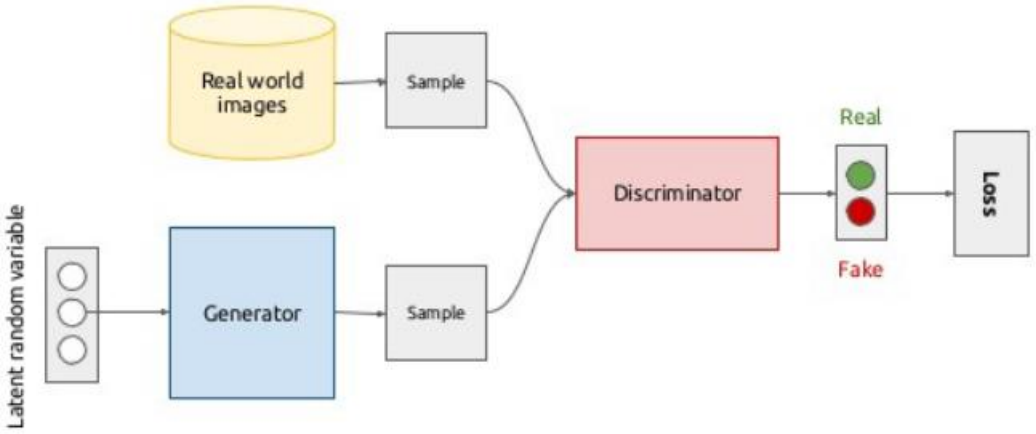
6.1 Teorijski okvir deepfake tehnologije

Deepfake je naziv za sintetički multimedijski sadržaj temeljen na umjetnoj inteligenciji koji ima širok spektar primjena, a glavna karakteristika mu je hiperrealistična simulacija. Tehnologija je toliko uznapredovala da je često nazivaju „photoshopom u pokretu“. Pojam *deepfake* prvi put se spominje 2017. godine na internetskom forumu Reddit i kombinacija je riječi „*deep learning*“ (duboko učenje, područje unutar znanosti umjetne inteligencije) i „*fake*“ (lažnjak, varka) što savršeno opisuje prirodu ove tehnologije. Riječ je o izrazito sofisticiranoj softverskoj tvorevini koja je u svojoj suštini lažna, odnosno prikazuje ono što se u stvarnosti (još uvijek) nije dogodilo. Iako *deepfake* zbog dosadašnjih slučajeva korištenja ima većinski negativnu konotaciju, stručnjaci zagovaraju njegovu uporabu u korisne svrhe (Somers, 2019).

Tehnologija na kojoj počiva ova vrsta varki je umjetna inteligencija. Riječ je o znanosti pomoću koje se nastoje stvoriti inteligentni strojevi, odnosno računalni programi koji imaju kognitivne sposobnosti racionalnog ponašanja, prosuđivanja i djelovanja na način da oponašaju ljude i njihove intelektualne sposobnosti. Umjetna inteligencija ima izrazito širok spektar primjene, zbog čega ju se danas smatra univerzalnim rješenjem problema i esencijalnim dijelom svih digitalnih proizvoda i usluga. Razvila su se mnoga područja umjetne inteligencije kao što su strojno učenje, obrada prirodnog jezika, govor, ekspertni sistemi, robotika i vizualna područja. *Deepfake* se temelji na dubokom učenju koje spada u metode strojnog učenja. Riječ je o kreiranju neuronskih mreža putem kojih se želi imitirati funkcioniranje ljudskog mozga, odnosno stvoriti računalni program koji je sposoban „učiti“ na temelju golemih setova podataka. Učenje se naziva dubokim jer se temelji na prolasku podataka kroz „slojeve“ neuronskih mreža putem kojih se optimizira sam rad programa (IBM, 2022). Tehnologija *deepfakea* funkcionira na temelju GAN (*Generative Adverserial Network*) sustava. Riječ je o dva sustava umjetne inteligencije, točnije dvije neuronske mreže koje se međusobno natječu, tj. sudjeluju u „igri“ gdje je dobitak jedne mreže ujedno gubitak druge. Prva mreža naziva se generatorom i ona pokušava pretvoriti ulazne podatke u smislenu sliku željenog objekta. Tako dobivena slika dodaje se u skup slika koje se potom predstavljaju drugoj mreži, diskriminatoru,

koji pokušava pronaći razliku između ostalih, pravih slika i sintetički generirane slike. Ovaj proces se ponavlja dok god je „lažna“ slika neopažena od strane identifikatora. Identifikator u početku s izrazitom lakoćom nalazi razlike između pravih i falsificiranih slika, no vremenom to postaje sve teže. Smatra se kako je minimalan broj iteracija potrebnih za uspješno kreiranje lažne slike 150.000 (The Guardian, 2020).

Slika 11. Koncept GAN sustava



Medium.com (2019): GANs – A brief introduction to Generative Adverserial Networks,*https://medium.com/@saibharath897/generative-adversarial-networks-gans-560c5c988128*, pristupljeno 30.6.2022.

Iako djeluje kompleksno, izrada *deefakea* prosječne kvalitete nipošto nije komplicirana, čemu uvelike doprinosi brzi razvoj internetske zajednice koja se identificira kao entuzijasti ove vrste digitalne manipulacije. Na Internetu je dostupno mnoštvo besplatnih materijala pomoću kojih se mogu načiniti više ili manje uvjerljive varke, a javlja se i sve veći broj mobilnih aplikacija koje podržavaju kreiranje istih. Važno je naglasiti kako će za izradu uvjerljivijeg *deepfakea* sposobnog zavarati veći broj ljudi ipak biti potrebno računalo jače procesorske moći i grafičkih sposobnosti od većine modernih osobnih računala. Danas tako u kreiranju *deepfakeova* sudjeluje čitav niz raznih interesnih stana, od onih koji ga koriste u pozitivne, legalne svrhe kao što su akademska i industrijska uporaba, istraživanje i razvoj do onih koji ga koriste u manje poželjne, ilegalne svrhe kao što su osvete, ucjene, širenje lažnih informacija, krađa identiteta i ostale vrste kriminalnih aktivnosti. *Deepfake* se tako često navodi kao izrazito moćna, ali u

suštini neutralna tehnologija čija uporaba može poprimiti različite oblike i razmjere, a zapravo ovisi o samim korisnicima i njihovim krajnjim ciljevima (The Guardian, 2020).

6.2 Potencijal i rizici korištenja deepfake tehnologije

Širok spektar korištenja *deepfake* tehnologije čine ju, kao i samu umjetnu inteligenciju, jednom od najviše obećavajućih naprednih tehnoloških rješenja. Iako se ova tehnologija može koristiti u mnoge pozitivne svrhe, nekolicina malicioznih oblika primjene daju joj većinski negativnu konotaciju. U nastavku slijedi pregled prvo pozitivnih, a zatim i negativnih primjera korištenja *deepfake* tehnologije.

Trenutno najzastupljeniji pozitivan način primjene odnosi se na industriju zabave, primarno na filmsku umjetnost. Naime, realističnost ove tehnologije čini ju neizostavnim rješenjem u slučajevima kada stanje nekog od glumaca otežava snimanje ili kad su potrebni specijalni efekti koje dotadašnjim mogućnostima nije moguće postići. Vjerojatno najpoznatiji primjer je slučaj filmskog serijala *Brzi i žestoki*. Naime, jedan od glavnih glumaca franšize, Paul Walker, tragično je preminuo uslijed snimanja sedmog filmskog nastavka. *Deepfake* tehnologija pomogla je da ga se putem prethodno korištenih snimki na filmskom platnu „oživi“ što je omogućilo završetak snimanja filma (The Hollywood Reporter, 2015). Osim slikovnih, *deepfake* omogućava i kreiranje audio imitacija glasa. Tako je glumcu Valu Kilmeru, koji je od posljedica karcinoma grla izgubio sposobnost govora, na ekranu ona vraćena, što mu je omogućilo repriziranje uloge u filmu *Top Gun:Maverick* (BGR, 2022).

Moguće je korištenje i u edukativne svrhe, gdje postoji potencijal za korištenje inovativnih načina podučavanja koji bi zahtijevali interaktivno sudjelovanje učenika te tako tradicionalnom školstvu dali sasvim novu dimenziju. Samo neki od primjera su rekreiranje poznatih ličnosti 20. stoljeća u predmetima kao što je povijest, koji učenicima često znaju biti nezanimljivi. *Deepfakeove* je moguće koristiti na višim akademskim razinama, kao što su fakulteti. Ovdje se navodi primjena u obrazovanju liječnika putem simulacija slučajeva iz stvarnog svijeta (Towards Data Science, 2020). Znanstvenici također istražuju potencijal GAN-ova u detekciji anomalija u rendgenskim snimkama, a smatra se kako bi *deepfakeovi* znatno pridonijeli procesu otkrivanja novih kemijskih spojeva i molekula, što bi rezultiralo napretkom u istraživanju i razvoju materijalnih i medicinskih znanosti. Konačno, navodi se slučaj upotrebe u modnoj

industriji i marketingu, gdje je moguće kreiranje modela koji nisu stvarni ljudi, već sintetičke kreacije, što bi smanjilo troškove modnih revija i marketinških kampanja (Westerlund, 2019).

Westerlund (2019) prijetnje dijeli u četiri kategorije, a to su širenje lažnih vijesti putem obmanjivanja novinara koji potom ne mogu razlučiti istinite od lažnih informacija, prijetnja nacionalnoj sigurnosti putem širenja propagande i miješanjem u izbore, smanjenje kredibiliteta nadležnih ustanova putem obmanjivanja društva te porast kibernetičkih prijetnji usmjerenih na društva i organizacije. Može se zaključiti kako je *deepfake* dosad najsofisticiranija metoda krađe identiteta jer je njenim manipuliranjem multimedijom (slikom, videom i zvukom) moguće istovremeno zavarati golem broj ljudi. Entuzijasti umjetne inteligencije, ali i kibernetičke sigurnosti, na ovaj se način imitacije često referiraju kao na novu etapu u razvoju društvenog inženjeringa. Prevare počinjene ovim putem do sad su najveći financijski uspjeh polučile putem telefonskog kontaktiranja visokorangiranih pojedinaca unutar organizacija. Također, lažni sadržaj toliko je sofisticiran da nerijetko može oponašati izgled osobe do te mjere da zaobiđe biometrijske mjere autentifikacije, što mnoga poduzeća koja se bave verifikacijom identiteta dovodi u nepovoljan položaj (Channel Asia, 2021).

Povijest korištenja *deepfakea* za maliciozne imitacije zapravo započinje 2016. godine, kad je ova tehnologija još bila u povojima. Američki komičar i voditelj Jimmy Fallon satirično se osvrnuo na tadašnje američke predsjedničke izbore. Iako je skeč bio jednostavan do te razine da se jasno vidjela razlika između predsjedničkog kandidata Donalda Trumpa i Jimmyja Fallona, internetska zajednica promptno je reagirala i kreirala izuzetno uvjerljiv *deepfake*. Ovo se smatra prvom javnom demonstracijom zastrašujućeg potencijala *deepfakea*. Uslijedio je čitav niz imitacija medijski eksponiranih osoba čije izjave i djela imaju jak odjek u javnosti. Redom su imitirani čelnik Microsofta Bill Gates, prvi čovjek Facebooka Mark Zuckerberg, američke političarke Nancy Pelosi i mnogih drugih. Svaki primjer podrazumijevao je korištenje u većoj ili manjoj mjeri kontroverznog sadržaja koji bi, shvaćen bez konteksta, mogao imati znatne posljedice na identitet osobe i organizacije koju predstavljaju. Prvi „pravi“ primjer pokušaja maliciozne uporabe tehnologije odvio se tijekom predsjedničkih izbora u Gabonu 2019. godine. Trenutni predsjednik i predsjednički kandidat Ali Bongo bio je na liječenju u Saudijskoj Arabiji zbog čega je duže vrijeme izbivao iz zemlje te su započele glasine kako je tamo i preminuo. Vlada, u cilju smirivanja situacije, objavljuje video bez zvuka u kojem predsjednik djeluje sasvim zdravo. No, nekoliko dana kasnije izbija vojni puč koji dodatno potpiruje iovako nestabilnu političku situaciju u Gabonu. Bongov protukandidat Ben

Moubamba optužuje vladu za pokušaj manipuliranja izborima krivotvorenjem videa predsjednika putem *deepfake* tehnologije, no Bongo se u međuvremenu oporavlja i preuzima vlast (The Guardian, 2019).

Tehnološko imitiranje političara osobito je popularno za vrijeme kriznih vremena, o čemu svjedoče dva nedavna incidenta. U travnju 2020. godine politička aktivistička grupa pod imenom Extinction Rebellion (XR) na Facebooku je objavila video koji predstavlja tadašnju belgijsku premijerku Sophie Wilmes. Originalna snimka odnosila se na njezin govor vezan uz pandemiju COVID-19, no aktivisti su kreirali alternativni govor u kojem premijerka povezuje epidemiološke krize u proteklih 20 godina (Ebolu, SARS, Svinjsku gripu) i ostale moderne medicinske anomalije s ljudskom eksploatacijom i uništavanjem prirode (Medium.com, 2022). Također, u lipnju 2022. godine iskorištava se aktualni ukrajinsko-ruski sukob kako bi se po prvi put koristila *deepfake* tehnologija u jednom videopozivu. Naime, gradonačelnici nekolicine europskih prijestolnica, Beča, Madrida i Berlina kontaktirani su radi održavanja video sjednice s kijevskim gradonačelnikom Vitalyjem Kličkom. Poziv je održan na platformi za održavanje videopoziva, Webexu, u petak 24. lipnja 2022. Prvih 15 minuta gradonačelnici su uistinu bili uvjereni kako je riječ o razgovoru s pravim kijevskim gradonačelnikom, što potvrđuju i prisutni članovi njihovih kabineta. No, nakon što je Kličko započeo s optuživanjem ukrajinskih izbjeglica za iskorištavanje programa socijalne pomoći u zapadnoeuropskim državama i zagovaranjem njihove deportacije u Ukrajinu kako bi sudjelovali u sukobima, ostali sudionici postali su sumnjičavi. Kada je došlo do prekida veze, ured gradonačelnika Berlina odmah je kontaktirao ured gradonačelnika Kijeva. Ustanovljeno je kako osoba koja je sudjelovala u pozivu nije bio kijevski gradonačelnik, odnosno da je riječ o izuzetno uvjerljivoj varci počinjenoj putem *deepfakea* (The Guardian, 2022).

6.3 Analiza odabrane studije slučaja

Medijski najeksponiraniji i prvi prijavljeni slučaj korištenja *deepfake* tehnologije u prave kriminalne svrhe zabilježen je 2019. godine. Incident se sastojao od korištenja telefonskog poziva putem kojeg se jednog od vrhovnih ljudi neimenovane britanske energetske kompanije izmanipuliralo na plaćanje sredstava počiniteljima. Ovaj napad ujedno se smatra i prvim slučajem korištenja tehnologije umjetne inteligencije u kriminalne svrhe.

U ožujku 2019. godine kriminalci su putem telefonskog poziva kontaktirali izvršnog direktora britanske energetske kompanije. Glas u slušalici predstavio se kao izvršni direktor njemačke tvrtke majke koji mu je naložio da isplati sredstva na bankovni račun mađarske kompanije dobavljača. Zahtjev je implicirao žurnost u izvršenju plaćanja i naveo rok od jednog sata unutar kojeg sredstva moraju biti prenesena. Obmanuti direktor tijekom izvještaja rekao je kako nije bilo sumnje da je glas u telefonu pripadao njegovom šefu jer je njemački naglasak i boja glasa savršeno odgovarala svim njihovim prethodnim susretima. To ga je ponukalo da doista naloži prijenos sredstava te je iznos od 223.000 eura transferiran na navedeni račun. Uslijedila su još dva telefonska poziva u kojima su počinitelji naveli kako plaćanje nije uspješno te kako mole ponovni pokušaj transfera. Također, izvršni direktor je do tada primijetio kako je poziv upućen s telefonskog broja registriranog u Austriji. Napad je odmah potom prijavio, no sredstva su već bila prenesena na bankovni račun u Meksiku i raspodijeljena na druge udaljene lokacije (The Wall Street Journal, 2019).

Početkom 2020. hongkonška banka biva metom sličnog napada. Menadžer banke zaprima poziv osobe čiji je glas bez poteškoća prepoznao, a pripadao je direktoru iz UAE-a s kojim je komunicirao već mnogo puta. Tvrdio je kako njegova tvrtka priprema preuzimanje jedne druge tvrtke te mu je potrebno odobriti sredstva u iznosu od 35 milijuna dolara. Transfer je pripremljen, a menadžer banke čak je zaprimio e-mailove uključenih strana koji jasno navode detalje transakcije. S obzirom na to da ni u jednom trenutku nije posumnjao u legitimitet ovog zahtjeva, započeo je s prijenosom novčanih sredstava na račun. Nakon što je napad naknadno otkriven, UAE započinje istragu kako bi utvrdio uvjete napada i vratio otuđena sredstva kojima su oštećene institucije unutar države. Vlasti su u pomoć pozvale američke istražitelje za koje se smatra da imaju najviše iskustva u postupanju s ovakvim slučajevima, a istraga ovog incidenta još uvijek traje (Forbes, 2021).

Prethodno predstavljene studije slučaja daju naslutiti kako je *deepfake* izrazito moćna tehnologija koja u pogrešnim rukama poprima ulogu visoko sofisticiranog digitalnog oružja protiv kojeg još uvijek nisu razvijeni dovoljno efikasni sustavi obrane. Kao što je navedeno, ljudski element u borbi protiv ovih tehnologija izrazito je neefikasan, no svejedno se preporuča temeljita edukacija, odnosno osvješćivanje o ovom tipu prijetnji. Stručnjaci kao rješenje primarno vide kompleksna tehnološka dostignuća koja će biti upotpunjena zakonskim i regulatornim zahtjevima. Westerlund (2019) navodi iduće preporuke u borbi protiv *deepfake* tehnologije:

- Formiranje legislativnog i regulatornog okvira za kontrolu *deepfake* tehnologije
- Suradnja najvećih tehnoloških kompanija (divova) u borbi protiv *deepfakeova*
- Uvođenje korporativnih politika, kodeksa ponašanja i etičkih normi unutar društvenih mreža i političkih kampanji
- Edukacija i trening zaposlenika
- Podizanje svijesti javnosti
- Aktivni razvoj i kontinuirano korištenje naprednih tehnologija u borbi protiv *deepfakeova*.

7. METODE ZAŠTITE PROTIV KRAĐE IDENTITETA

Kao što je u radu već predstavljeno, kriminalne aktivnosti povezane s krađom digitalnog identiteta postaju sve ozbiljniji problem. Postupno ulaze u sve sfere ljudskog života, od krađa identiteta i oštećenja osobe na individualnoj razini do počinjenja velikih šteta na razini poduzeća, pa čak i kritične infrastrukture i javnog mnijenja, odnosno države. Stoga je potrebna pomno osmišljena strategija borbi protiv ove vrste kriminala. Stručnjaci zagovaraju detaljno razrađene sigurnosne mjere koje se sastoje od kombinacije rješenja koja utječu na ljudski i tehnološki aspekt krađe digitalnog identiteta. Arbanas et al. (2021) dokazuju kako je pri kreiranju strategije informacijske sigurnosti nužno promatrati ne samo tehnološke, već i sociološke i organizacijske komponente. Također, predstavljaju konceptualni okvir za ocjenjivanje i poboljšanje kulture informacijske sigurnosti unutar organizacije, koji se sastoji od 3 glavne komponente, organizacijskih mjera, sociooloških faktora i tehnoloških mjera. Ovaj zaključak podudara se s ranije promatranim pojmom kibernetičke sigurnosti koje naglasak stavlja na holističko postupanje sa sofisticiranim i kompleksnim rizicima, kakvima su krađe digitalnog identiteta u zadnje vrijeme i postale.

7.1 Metode zaštite s organizacijskog aspekta

Stručnjaci iz područja informacijske sigurnosti slažu se oko činjenice da efikasna, odgovorna i zrela strategija kibernetičke sigurnosti treba počivati upravo na organizacijskom aspektu. Nerijetko navode sintagmu „najslabije karike“ kojom označavaju manjkavost ljudskog elementa u informacijskom sustavu (Gardner, 2014). Ovo je posebice vidljivo u incidentima u kojima je digitalna krađa identiteta bila osnovnim ciljem ili pomoćnom metodom pri ostvarenju nauma kriminalaca. Iskorištavanje ljudi i manipuliranje njihovim emocijama i psihom poprilično je perfidan način kriminalnog djelovanja, zbog čega mu je potrebno pristupati s velikom razinom opreza.

Gotovo svi prijedlozi borbe protiv digitalnih krađa identiteta započinju s edukacijom i podizanjem svijesti o ovoj vrsti rizika među ljudima. Gardner (2014.) navodi kako je program informacijske edukacije i treninga zaposlenika temelj svake zrele organizacijske sigurnosne strategije. Alkhalil et al. (2021) u iscrpnom pregledu novih trendova u digitalnoj krađi identiteta svoje sigurnosne preporuke započinju upravo ovim prijedlogom, iako naglašavaju kako ljudske mjere nikada ne pružaju potpunu zaštitu. Kao rješenje ljudskog aspekta navode podizanje

svijesti o sigurnosnoj zaštiti (eng. *security awareness training*) kroz zajedničku ili individualnu edukaciju zaposlenika putem seminara i tečajeva, kontinuirano provođenje probnih napada krađe identiteta kako bi se ustvrdilo jesu li usvojena znanja uistinu korisna te edukacija ljudi putem scenarija kompjuterskih igrica (tzv. gamifikacije). Iznose činjenicu kako interaktivna edukacija o online krađama identiteta može povećati efikasnost treninga za čak 60%. No, autori svejedno navode kako je, promatrajući nedavne napade ove vrste, bilo koja vrsta osvješćivanja i edukacija nedovoljna te savjetuju upotpunjavanje strategije obrane naprednim tehnološkim rješenjima. Back i Guarette (2021) u svojem radu nastoje ispitati efikasnost tradicionalnih edukacija vezanih uz *phishing* napade. Provode istraživanje u kojem promatranu populaciju (N=2000) dijele u dvije grupe s jednakim brojem ljudi, gdje jedna grupa pohađa tečaj informacijske sigurnosti, a druga ne. Potom, svi promatrani subjekti u razdoblju od deset dana zaprimaju jedan testni *phishing* e-mail. Rezultati ukazuju da je razlika između pojedinaca koji su pohađali i onih koji nisu pohađali tečaj neznatna kada je riječ o otvaranju e-mail i otvaranju lažnog URL-a. Autori zaključuju kako je trenutna razina edukacije protiv digitalnih krađa identiteta nedovoljno efikasna i odviše općenita. Prepoznaju važnost podizanja svijesti ljudi digitalnoj krađi identiteta, no kritiziraju trenutne metode i predlažu neke nove. Prijedlozi autora sastoje se od kreiranja online platforme na izradi koje bi sudjelovali stručnjaci iz različitih područja, a nudila bi mogućnost personalizirane, specificiranije edukacije ovisno o pozadini i iskustvu polaznika. Slično kao i Gardner, zagovaraju neki vrstu gamificiranog pristupa osvješćivanju ljudi jer smatraju da su dosadašnje metode nedovoljno uspješne.

Uzevši u obzir promatrane radove, kao organizacijske metode zaštite od digitalnih krađa identiteta mogu se navesti:

- Podizanje svijesti ljudi (zaposlenika) putem edukacija i treninga
- Donošenje organizacijskih pravilnika i procedura pri dijeljenju povjerljivih podataka elektroničkim putem
- Napuštanje tradicionalnih, odviše općenitih oblika edukacije i orijentiranje prema specifičnim, prilagođenim edukacijama
- Uvođenje interaktivnih edukacija sličnima računalnim igricama, odnosno gamifikacija samih programa edukacija i podizanja svijesti

7.2 Metode zaštite s tehnološkog aspekta

Kada je riječ o tehnološkim mjerama zaštite, stručnjaci zagovaraju napredna tehnološka rješenja koja bi mogla parirati podjednako sofisticiranim prijetnjama. Prijedlozi se dijele u dvije skupine rješenja, jednu zasnovanu na umjetnoj inteligenciji i drugu utemeljenu na *blockchain* tehnologiji.

Umjetna inteligencija i potencijal njenog korištenja zahvatile su gotovo svaku industriju i djelatnost današnjice, a kibernetička sigurnost svakako nije iznimka. Dostignuća na području kibernetičke sigurnosti kada je riječ o krađi identiteta većinom se odnose na kreiranje i ugradnju što efikasnijeg filtera u komunikacijske kanale, koji bi potom bio sposoban prepoznati kada je riječ o komunikaciji namijenjenoj krađi podataka primatelja. U obzir bi se uzimali kontekst i sadržaj poruke, ali i pretraga poruka za bilo kakvim anomalijama, upozorenjima i odstupanjima od uobičajenih načina komuniciranja (Gatefy, 2021). Basit et al. (2020) navode kako su aktualna tehnološka rješenja u obliku filtera poruka djelotvorna u samo 20% slučajeva, što implicira potrebu za preciznijim načinima detekcije. Tehnološke protumjere zasnovane na umjetnoj inteligenciji autori dijele u dvije glavne skupine. Riječ je o tehnikama dubokog učenja i tehnikama strojnog učenja, koje bi krađu digitalnog identiteta putem *phishinga* trebale svesti na minimum. Metode zasnivane na dubokom učenju funkcionirale bi na način da je neuronskoj mreži predstavljen set ulaznih podataka, a neuroni u mreži moraju zaključiti je li riječ *phishing* porukama ili legitimnoj korespondenciji. Eksperimentalno je utvrđeno kako ovaj način klasifikacije e-mailova, ukoliko je mreža opskrbljena s dovoljno velikim setom podataka, pokazuje razinu preciznosti od 97.61%. U daljnjim istraživanjima nastojat će se provesti uspješna klasifikacija isključivo na temelju URL-a koji se nalazi u poruci. Metode strojnog učenja funkcioniraju na sličan način, no ovdje je unaprijed potrebno modelu navesti koje su to karakteristike lažnog, a koje ispravnog e-maila, na temelju čega on donosi odluke o legitimitetu poruke. Ovim načinom postignuta je točnost klasifikacije od 93.5%, a nastoji se kreirati model koji će ispravnu odluku donijeti na minimalnom broju poznatih obilježja. Zaključuju kako bi ova dva načina detekcije pshihinga mogla pravovremeno identificirati, prijaviti i blokirati zloćudnu korespondenciju koja bi funkcionirala u 99% slučajeva. Jafar et al. (2022.) predlažu slično rješenje koje nazivaju GRU (*Gated Recurrent Unit*). Riječ je o izuzetno brzom i efikasnom klasifikatoru e-mailova čija ja najveća zabilježena točnost 98.30%. Model je specifičan po tome što sadržava tzv. vrata (filter) na svakoj razini neuronske mreže što znatno doprinosi brzini same detekcije malicioznih poruka. I hrvatski stručnjaci razvijaju alat koji će

doprinijeti detekciji *phishinga*. Naime, tvrtka Megatrend u suradnji s Ekonomskim i Filozofskim fakultetom Sveučilišta u Zagrebu nastoji razviti aplikaciju koja će biti u mogućnosti prepoznati *phishing* poruke na hrvatskom jeziku. Rješenje se zasniva na činjenici da je lakše postati žrtvom krađe digitalnog identiteta ukoliko je osoba kontaktirana na materinjem jeziku. Tehnologija se zasniva na treniranju dubokih neuronskih mreža, odnosno dubokom učenju. Naziva se PhisHRban, a trenutno je u fazi razvoja (HRT Magazin, 2022).

Druga skupina tehnoloških rješenja temelji se na *blockchain* tehnologiji. Ova tehnologija, razvijena 2009. godine, može se opisati kao distribuirani sustav (mreža), koji bilježi podatke o transakcijama u blokovima. Ovako kreirana baza podataka zasniva se na ravnopravnom uključenju svih dionika, a garantira transparentnost, integritet i nemogućnost krivotvorenja. Sustav je na popularnosti dobio predstavljanjem koncepta kriptovaluta (primarno Bitcoina), no načini uporabe ove tehnologije nadilaze aspekt financijskog sustava (BUG.hr, 2018). Trenutni, institucionalizirani i centralizirani sustavi digitalnog identiteta, smatraju se rizičnima i općenito manjkavima. Posebice su izloženi riziku hakiranja, jedne točke kvara, curenja podataka, zlćudnog manipuliranja podacima i internih napada (Yang i Li, 2020). Takemiya i Vanieiev (2018) predlažu sustav u kojem bi osoba imala kontrolu nad vlastitim informacijama i sama birala tko će joj (osoba ili institucija) imati pristup u digitalnoj sferi. Većina predloženih modela decentraliziranog sustava upravljanja digitalnim identitetom funkcionira na sličan način. Naime, korisnik platforme (sustava) za upravljanje identitetom upisuje svoje podatke koji se potom kriptiraju i digitalno potpisuju. Na ovaj način kreira se par ključeva, gdje se jedan (javni) ključ pohranjuje u lanac blokova (*blockchain*), dok drugi pripada isključivo korisniku da bi mogao potvrditi kako je upravo on vlasnik pohranjenih informacija. Korisnici dobivaju tzv. decentralizirani identifikator, odnosno pseudonim koji je potvrđen privatnim ključem. Taj identifikator moguće je prezentirati u širokom spektru interakcija s drugim osobama i institucijama unutar platforme. Pružatelj usluga prilikom interakcije s korisnikom od njega će zatražiti prezentaciju identifikatora. Kada korisnik prezentira identifikator, pružatelj usluge provjerava podudaraju li se javni ključ zabilježen u lancu koji potvrđuje potrebne informacije korisnika i privatni ključ potvrđen decentraliziranim identifikatorom. Ukoliko se ključevi podudaraju, korisnikov identitet je potvrđen, odnosno verifikacija njegovog (digitalnog) identiteta je uspješno provedena (Consensys, 2022).

8. ZAKLJUČAK

Krađa identiteta jedan je od najzloćudnijih oblika kriminalnih aktivnosti, koji na žrtvu ostavlja trajne posljedice. Eksponencijalnim razvojem digitalnih tehnologija i njegovom integracijom u našu svakodnevicu, gotovo svi aspekti ljudskog života postupno se sele u digitalnu dimenziju čineći tako virtualnu presliku stvarnosti. Aspekt koji također konvergira ka digitalnom je ljudski identitet, koji se može promatrati kao agregat digitalnih interakcija i transakcija osobe, koji ju jednoznačno određuje. Kako pozitivnih, digitalne tehnologije omogućuju digitalizaciju i negativnih segmenata ljudskog života. Digitalni kriminal, poznat pod pojmom kibernetičkog kriminala, također bilježi znatan porast s krađom digitalnog identiteta kao jednim od glavnih predstavnika ove vrste kriminala.

Istovremeno, nenadana pandemija bolesti COVID-19 uzrokovana virusom SARS-CoV-2 početkom 2020. godine potresla je svijet. Kao logična metoda ograničenja širenja zaraze nameće se socijalno distanciranje i izolacija, koja prisiljava ljude na sve veću prisutnost u digitalnom svijetu. Sve ljudske aktivnosti poprimaju virtualni karakter, što društvo u cjelini ostavlja izloženima raznim oblicima kibernetičkog kriminala. U svijetu u kojem su sve interakcije omogućene putem digitalnih kanala, krađa digitalnog identiteta postaje najozbiljnijaprijetnja svakom pojedincu i organizaciji.

Cilj ovog rada bio je analizirati kibernetičke prijetnje povezane s krađom identiteta u uvjetima pandemije COVID-19, odnosno unazad protekle dvije godine. Analiza se temeljila na četiri glavne hipoteze koje se nastojalo dokazati predstavljanjem statističkih podataka o kibernetičkom kriminalu ove vrste, kao i iscrpnom analizom studija slučaja.

Prva hipoteza nastoji dokazati kako je došlo do porasta kibernetičkih napada povezanih s krađom digitalnog identiteta. Ova pretpostavka potkrijepljena je statističkim i slikovnim pokazateljima prikupljenima od strane organizacija i institucija zaduženih za praćenje i analizu krađa digitalnog identiteta.

Druga hipoteza navodi kako je došlo do promjene meta napada krađe digitalnog identiteta. Ovdje se prvenstveno promatrao pomak od masovnih pokušaja krađe identiteta na individualnoj razini k naprednijim prijetnjama usmjerenim na specifične pojedince unutar organizacija i institucija koje se smatraju kritičnom infrastrukturom, s konačnim ciljem iskorištavanja atmosfere nesigurnosti, prekapacitiranosti i hitnosti u obmanjivanju javnosti radi ostvarenja

vlastitih koristi. Navedeno je također dokazano statistikom kibernetičkih napada prikupljenih od strane regulatornih tijela.

Treća hipoteza pretpostavlja kako su napadi krađe digitalnog identiteta sofisticiraniji no ranije. Kao argument koriste se podaci koji ukazuju na to da je došlo do promjene u strategiji kibernetičkih kriminalaca, odnosno napuštaju se primitivne metode krađe identiteta kao što je jednostavni *phishing, i to* u korist sofisticiranijih metoda kao što su *spear phishing* i ostale napredne metode društvenog inženjeringa. Također se bilježi nastanak *deepfake* tehnologije, izrazito kompleksnog sintetičkog medija temeljenog na umjetnoj inteligenciji pomoću kojeg je moguće počiniti teške povrede krađe identiteta, što kriminalci uistinu i koriste u kriznim situacijama kao što je pandemija.

Konačno, četvrta hipoteza sastoji se od pretpostavke kako su trenutačne metode obrane od krađa identiteta nedovoljno efikasne te kako je potrebno razviti novu strategiju obrane. Osim iz predstavljenih studija slučaja, ovdje se referira i na istraživanje Back i Guarette iz 2021. kojim je dokazano da nema značajne razlike u uspješnosti prepoznavanja napada usmjerenih krađi identiteta između pojedinaca koji su obučeni za identifikaciju istih i onih koji to nisu. Predlažu se nove metode koje se temelje na kombinaciji ljudskih, ali i tehnoloških metoda za koje se smatra da bi mogle znatno minimizirati trenutne napredne prijetnje krađe digitalnog identiteta.

Uzevši u obzir navedeno, dolazi se do zaključka da su kibernetičke krađe digitalnog identiteta izrazito rizične prijetnje u stalnom porastu te da kriminalci nastoje iskoristiti svaku civilizacijsku krizu kao dodatnu podlogu za ostvarenje vlastitih koristi. Kriminalne aktivnosti ovog tipa konstantno napreduju, što implicira potrebu za holističkim metodama i strategijama obrane temeljenima na kombinaciji ljudskih i tehnoloških mjera zaštite, koje će u punom smislu odražavati koncept kibernetičke sigurnosti.

POPIS LITERATURE:

1. Akdemir, N., Yenal, S. (2021.): *How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails*, Newbury Park: SAGE
2. Alkhalil, Z., Hewage, C., Nawaf, L., Khan,. I. (2021.): *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*, Cham: Springer
3. APWG (2020.-2022.), Phishing activity trends reports, preuzeto 28. lipnja 2022. s https://apwg.org/trendsreports/
4. Arbanas, K., Spremić, M. i Zajdela Hrustek, N. (2021.*): Holistic framework for evaluating and improving information security culture*, Bingley: Emerald
5. Ardagna, C., Corbiaux, S., Sfakianakis, A., Douligeris, C., (2021.), *ENISA Threat Landscape 2021* [e-publikacija], preuzeto s https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
6. Back, R. i Guerette, R., T. (2021.): *Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks*, Newbury Park: SAGE
7. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., i Kifayat, K. (2020.): *A comprehensive survey of AI-enabled phishing attacks detection techniques*, Heidelberg: Springer Netherlands
8. Bertino, E., Paci, F., Shang, N. (2009.), Keynote 2: Digital Identity Protection - Concepts and Issues. (2009), u Guererro, J., E. (ur.), *2009 International Conference on Availability, Reliability and Security* (str. 19-28.), Fukoka: ARES
9. BGR (2022.), Val Klimer's Top Gun:Maverick Dialogue was All AI since he can no longer speak, preuzeto 30. lipnja 2022. s https://bgr.com/science/val-kilmers-top-gun-maverick-dialog-was-all-ai-since-he-can-no-longer-speak/
10. Bitdefender (2022.), What is digital identity theft? How to Spot, React and Report it, preuzeto 21. travnja 2022., s https://www.bitdefender.com/cyberpedia/what-is-digital-identity-theft/
11. Bitdefender (2022.), What is your digital footprint?, preuzeto 21. travnja 2022. s https://www.bitdefender.com/cyberpedia/what-is-digital-footprint/
12. Bleeping Computer (2022.), FBI: *Ransomware* hit 649 critical infrastructure orgs in 2021, preuzeto 29. linpja 2022. s https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-649-critical-infrastructure-orgs-in-2021/

13. Pivar, J., Vlahović. N. (2020.), Sklopovlje računala: Kronološki razvoj računala. U: Pejić Bach, M., Spremić, M. (ured)., Osnove Poslovne Informatike, Zagreb, Ekonomski fakultet Zagreb
14. Breckenridge, G. (2018.), A brief history of digital identity, preuzeto 20. travnja 2022. s https://medium.com/humanizing-the-singularity/a-brief-history-of-digital-identity-9d6a773bf9f5
15. BUG.hr (2018.), Što je u stvari *blockchain* i kako radi?, preuzeto 2. srpnja 2022.s https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011
16. CERT (2022.), Phishing, preuzeto 28. travnja 2022. s https://www.cert.hr/phishing/
17. Channel Asia (2021.), How Deepfakes enhance social engineering authentification threats, preuzeto 1. srpnja 2022. s https://www.channelasia.tech/article/692475/how-deepfakes-enhance-social-engineering-authentication-threats/
18. Chawki, M., Darwish, A., Khan, M., A., Tyagi, S. (2015.), Cybercrime: Introduction, Motivation and Methods, u: Kacprzyk, J. (ur.), *Cybercrime, Digital Forensics and Jurisdiction* (str. 3-23)., Cham: Springer
19. CISA (2022.), Critical infrastructure sectors, preuzeto 29. lipnja 2022. s https://www.cisa.gov/critical-infrastructure-sectors
20. Claroty (2022.), 80% of critical infrastructure organizations experienced *ransomware* attacks last year, preuzeto 29. lipnja 2022. s https://claroty.com/resource/80-of-critical-infrastructure-organizations-experienced-ransomware-attacks-last-year/
21. Cnbc (2019.), How this scammer used phishing emails to steal over $100 million from Google and Facebook, pristupljeno 8. svibnja 2022. s https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html
22. Coman, I., Mihai, I. (2022). The Impact of COVID-19. on Cybercrime and Cyberthreats, [e-publikacija], preuzeto s https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/489
23. CompTIA (2022.), What is social engineering?, The Human Element in the Technology Scam, preuzeto 29. lipnja 2022. s https://www.comptia.org/content/articles/what-is-social-engineering
24. Consensys (2022.), *Blockchain* in Digital Identity, preuzeto 3. svibnja 2022. s https://consensys.net/blockchain-use-cases/digital-identity/
25. European Council, Council of the European Union (2022.), Timeline – Council actions on COVID-19, preuzeto 24. travnja 2022. s

https://www.consilium.europa.eu/en/policies/coronavirus/timeline/

26. F5 (2022.), Phishing attacks soar during the pandemic, preuzeto 28. lipnja 2022. s https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal
27. FBI (2022.), Internet crime report, preuzeto 29. lipnja 2022. s https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
28. Firewall Times (2022.), Social engineering statistics, preuzeto 29. lipnja 2022. s https://firewalltimes.com/social-engineering-statistics/
29. Forbes (2021.), Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find, preuzeto 1. srpnja 2022. s https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=55656a777559
30. Gardner, B. (2014.), What is a Security Awareness Program?, u: Katsaropoulos, C (ur.), *Building an Information Security Awareness Program* (str. 1-8.), Elsevier: Amsterdam
31. Gatefy (2021.), How artificial intelligence and machine learning fight phishing, preuzeto 3. svibnja 2022. s https://gatefy.com/blog/how-ai-and-ml-fight-phishing/
32. Healthcare IT News (2021.), UC San Diego Health phishing attack exposes SSNs, financial info, preuzeto 8. svibnja 2022. s https://www.healthcareitnews.com/news/uc-san-diego-health-phishing-attack-exposes-ssns-financial-info
33. Herjavec Group (2021.), The history of cybercrime, preuzeto 25. lipnja 2022. s https://www.herjavecgroup.com/history-of-cybercrime/
34. Hiji, M. i Alam, G. (2021.): *A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions*, New York: IEEE
35. Hong Kong Computer Emergency Response Team Coordination Centre (2020.), Case Study on Bitcoin Scam Incident - A Combined Social Engineering and Privilege Escalation Attacks, preuzeto 28. travnja 2022. s https://www.hkcert.org/blog/case-study-on-bitcoin-scam-incident-a-combined-social-engineering-and-privilege-escalation-attacks
36. Horton, N., Desimone, A. (2018.), Sony's Nightmare before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace, preuzeto 7. svibnja 2022. s https://apps.dtic.mil/sti/citations/AD1046744
37. HRT Magazin (2022.), Naši informatičari razvijaju aplikaciju „PhisHRban“, aplikaciju koja će prepoznavati phishing poruke, preuzeto 2. srpnja 2022. shttps://magazin.hrt.hr/znanost-tehnologija/nasi-informaticari-razvijaju-phishrban-aplikaciju-koja-ce-prepoznavati-

phishing-poruke-7874792

38. IBM (2022.), What is Artificial Intelligence, preuzeto 30. lipnja 2022. s https://www.ibm.com/cloud/learn/what-is-artificial-intelligence
39. IBM (2022.), What is Deep Learning, preuzeto 30. lipnja 2022. s https://www.ibm.com/cloud/learn/deep-learning
40. Idwatchdog (2022.), 11 ways identity theft can happen, preuzeto 21. travnja 2022. s https://www.idwatchdog.com/11-ways-identity-theft-happens/
41. International Telecommunication Union (2022.), *Internet Use During the Pandemic* [podatkovni dokument], preuzeto s https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/
42. Interpol (2020.), COVID-19 cyberthreats, preuzeto 25. travnja 2022. s https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats
43. Interpol (2020.), Interpol reports show alarming rate of cyberattacks during COVID-19, preuzeto 25. travnja 2022. s https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
44. Ironscales (2021.), State of cybersecurity survey, preuzeto 29. lipnja 2022. s https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/
45. IT governance (2022.), 5 ways to detect a phishing e-mail, preuzeto 27. lipnja 2022. s https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
46. IT governance (2022.), The 5 most common types of phishing attack, preuzeo 27. lipnja 2022. s https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack
47. IT governance (2022.), 2021 review of phishing scams, preuzeto 28. travnja 2022. s https://www.itgovernance.eu/blog/en/2021-review-of-phishing-scams
48. Jafar, M., Al-Fawa'reh, M.,Barhoush, M. i Alshira'H, M.(2022.): *Enhanced Analysis Approach to Detect Phishing Attacks During COVID-19 Crisis*, Berlin: De Gruyter
49. Kaspersky (2022.), Social engineerign in 2021. preuzeto 29. lipnja 2022. s https://go.kaspersky.com/rs/802-IJN-240/images/NJ_Social_Engineering_KFP.pdf
50. Kaspersky (2022.), PlayStation 5 contest scam, preuzeto 28. travnja 2022. s https://www.kaspersky.co.uk/blog/scam-with-playstation-5-giveaway/22449/
51. Kaspersky (2022.), Whats is cybercrime, preuzeto 25. lipnja 2022. s https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

52. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., i Bellekens, X. (2021.*): Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*, Amsterdam: Elsevier
53. LeBerge, L., O'Toole C., Schneider, J., Smaje, K. (2020.), How COVID-19 has pushed companies over the technology tipping point—and transformed business forever, preuzeto 25. travnja 2022. s https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
54. Leiner, M.B., Cerf, V.G., Clark, D.D., Kahn, R.E., Kelinforck, L., Lynch, D.C., Postel, J., Roberts, L.G., Wolff, S. (1997.), A brief history of Internet, preuzeto 24. lipnja 2022. s https://www.internetsociety.org/internet/history-internet/brief-history-internet/
55. Majeed, M., M., F., Adisputera, A., Ridwan, M., (2020.): *Digital Identity*, Budimpešta: Budapest International Research and Critics University
56. Malwarebytes (2022.), Stuxnet, preuzeo 25. lipnja 2022. s https://www.malwarebytes.com/stuxnet
57. Malwarebytes (2022.), WannaCry, preuzeo 25. lipnja 2022. s https://www.malwarebytes.com/wannacry
58. Medium.com (2022.), Extinction Rebellion releases deepfake of Belgian Prime Ministe, preuzeto 2. srpnja 2022. s https://medium.com/sensity/tracer-newsletter-50-20-04-20-extinction-rebellion-release-deepfake-of-belgian-prime-minister-2b48d586b44
59. Microsoft (2020.), Exploiting a crisis: How cybercriminals behaved during the outbreak, preuzeto 25. travnja 2022. s https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
60. Nagy, P. i Koles, B. (2014.): *The digital transformation of human identity: Towards a conceptual model of virtual identity in virtual worlds*, Newbury Park: SAGE
61. Norton (2022.), Identity theft: What is it and how to avoid it, preuzeto 22. travnja 2022. s https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html
62. Onfido (2022.), How has Covid-19 changed our relationship with digital identity?, preuzeto 27. travnja 2022. s https://onfido.com/resources/blog/how-has-covid-19-changed-our-relationship-with-digital-identity
63. Phishing.org (2022.), Histroy of phishing, preuzeto 28. travnja 2022. s https://www.phishing.org/history-of-phishing

64. Salahdine, F., Kaabouch, N. (2019.): Social Engineering Attacks: A Survey., *Future Internet* [online], *11(4)*, 89 – 106., https://doi.org/10.3390/fi11040089
65. Savastano, M., Zentner, H., Spremić, M. i Cucari, N. (2021.), Assessing the relationship between digital transformation and sustainable business excellence in a turbulent scenario, *Total Quality Management & Business Excellence*, https://doi.org/10.1080/14783363.2022.2063717
66. Security Intelligence (2021.), Most digital attacks today involve social engineering, preuzeto 29. lipnja 2022. s https://securityintelligence.com/articles/most-digital-attacks-today-involve-social-engineering/
67. Somers, M. (2020.), Deepfakes, Explained, preuzeto 29. travnja 2022. s https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained
68. Spremić, M. (2017), *Sigurnost i Revizija Informacijskih Sustava u Okruženju Digitalne Ekonomije*, Zagreb: Ekonomski fakultet Zagreb
69. Spremić, M. (2017.), *Digitalna transformacija poslovanja*, Zagreb: Ekonomski fakultet Zagreb
70. Spremić, M. (2017.): *Governing Digital Technology – how Mature IT Governance can help in Digital Transformation?*, IARAS: Sofia
71. Takemiya, M., i Vanieiev, B. (2018). Sora Identity: Secure, Digital Identity on the *Blockchain.*, u: O'conner, L (ur.), *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* (str. 582-587.), Piscataway: The Institute of Electrical and Electronics Engineers, Inc.
72. Techopedia (2022.), What is digital identity, preuzeto 22, lipnja 2022. https://www.techopedia.com/definition/23915/digital-identity
73. TechTarget (2022.), Colonial Pipeline hack explained, preuzeto 30. lipnja 2022. s https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
74. The Guardian (2020.), What are deepfakes – and how can you spot them?, preuzeto 29. travnja s https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them
75. The Guardian (2022.), European politicians duped into deepfake video calls with mayor of Kyiv, preuzeto 2. srpnja 2022. s https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko

76. The Guardian (2019.), The rise of Deepfake and the threat to democracy, preuzeto 1. srpnja 2022. s https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy
77. The Hollywood Reporter (2015.), How Furious 7 brought late Paul Walker back to life, preuzeto 30. lipnja 2022. s https://www.hollywoodreporter.com/movies/movie-news/how-furious-7-brought-late-845763/
78. The San-Diego Union Trbune (2021.), UC San Diego Health sued over data breach that may have exposed records of 500,000 patients, preuzeto 8. svibnja 2022. s https://www.sandiegouniontribune.com/business/story/2021-09-23/sd-fi-ucsandiego-cyber-attack
79. The Wall Street Journal (2019.), Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, preuzeto 299. travnja 2022. s https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
80. Towards Data Science (2020.), Positive use cases of synthetics media (a.k.a. Deepfakes), preuzeto 30. lipnja 2022. s https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387
81. Venkatesha, S., Reddy, K. R., Chandavarkar, B. R. (2021.): *Social Engineering Attacks During the COVID-19 Pandemic*, Cham: Springer
82. Westerlund, M. (2019.), The Emergence of Deepfake Technology: A Review, preuzeto 29. travnja 2022. s https://timreview.ca/article/1282
83. Yang, X., Li, W.. (2020.): *A zero-knowledge-proof-based digital identity management scheme in blockchain*, Amsterdam: Elsevier

POPIS SLIKA

ŽIVOTOPIS

Domagoj Stančin rođen je 7. studenog 1996. godine u Zagrebu gdje završava osnovnoškolsko i srednjoškolsko obrazovanje. U ak. godini 2016./2017. upisuje Integrirani preddiplomski i diplomski studij poslovne ekonomije na Ekonomskom fakultetu Sveučilišta u Zagrebu. Tijekom studiranja sudjeluje u izvannastavnim aktivnostima kao što je članstvo u studentskoj udruzi Ekonomska klinika i Erasmus+ program studentske razmjene. 2020. godine zapošljava se u Microblinku kao analitičar podataka, gdje i danas radi na poziciji višeg eksperta. Područja interesa su mu digitalna transformacija, podatkovne znanosti i kibernetička sigurnost.