Univerza v Mariboru
Fakulteta za varnostne vede

Domen Zorko

UPORABA SMISHINGA V BANČNIŠTVU

Diplomsko delo
visokošolskega študijskega programa Informacijska varnost

Ljubljana, december 2023

Univerza v Mariboru

Fakulteta za varnostne vede

UPORABA SMISHINGA V BANČNIŠTVU

Diplomsko delo

Študent: Domen Zorko

Študijski program: Visokošolski študijski program Informacijska varnost

Mentor: izr. prof. dr. Blaž Markelj

ZAHVALA

Zahvaljujem se mentorju izr. prof. dr. Blažu Marklju za pomoč, napotke, usmerjanje ter potrpežljivost med pisanjem diplomskega dela.

Prav tako se zahvaljujem tudi svoji družini in prijateljem, ki so mi med pisanjem nudili podporo.

Rad bi se zahvalil tudi vsem, ki so sodelovali z odgovarjanjem na raziskovalna anketna vprašanja.

UPORABA SMISHINGA V BANČNIŠTVU

Ključne besede: smishing, bančništvo, socialni inženiring

UDK: 004.056.53(043.2)

Povzetek

Smishing si kot oblika kibernetskega napada deli s phishingom skupne značilnosti, vendar se razlikuje po tem, da se izvaja preko SMS-sporočil. Napadalci, ki se odločijo uporabljati metodo smishinga, uporabljajo strategije napadov socialnega inženiringa, s ciljem, da uporabniku pošljejo sporočilo, ki vzbuja občutek nujnosti in strahu, v upanju, da povzročijo dovolj stresa, da žrtev uboga napadalca takoj in brez pomisleka. Glavni namen napadalcev je večinoma pridobitev osebnih podatkov, poverilnic, finančnih podatkov ter vodenje žrtev na zlonamerne spletne strani. Pri smishing napadih kriminalci pogosto uporabljajo SMS-spoofing, ki je ključni dejavnik pri uspešnosti smishinga še posebej v kontekstu mobilnega bančništva, ki ga dandanes uporablja večina posameznikov, ki ima v lasti mobilno naprava. Zaradi visokega števila uporabnikov in možnosti kraje denarja so mobilne banke privlačna tarča za kibernetski kriminal. Napadalci se zavedajo dejstva, da banka s svojimi tehničnimi sredstvi ni zmožna povsem odpraviti človeških napak. Zaradi tega je preprečitev smishing napadov velik izziv, ki zahteva celovit pristop. Ta pristop mora vključevati več elementov obrambe, kot so izobraževanje uporabnikov o obstoju in nevarnostih smishinga, implementacija tehničnih sredstev za prepoznavanje ter blokiranje smishing sporočil ter sodelovanje med bankami in varnostnimi strokovnjaki. Izobraževanje uporabnikov je najpomembnejše, saj lahko samo uporabnik, ki je bil poučen o odkrivanju smishinga, zanesljivo prepozna neobičajne načine komunikacije. Preprečevanje smishinga je razvijajoč problem, ki bo zahteval neprestano učenje in prilagajanje novih ukrepov.

THE USE OF SMISHING IN BANKING

Keywords: Smishing, banking, social engineering

UDC: 004.056.53(043.2)

Abstract

Smishing is a type of cyber attack that shares common characteristics with phishing in terms of attack methods. The main difference is that it is sent from an SMS message. In smishing, attackers use social engineering attack strategies by sending a message to the user that aims to instill a sense of urgency and fear in the user, causing them to obey the attacker immediately and without hesitations due to stress. The goal of attackers is ususally to obtain personal data, credentials, financial data and lead victims to malicious websites. In smishing attacks, criminals ofter use SMS spoofing, which is one of the key factors in the success of smishing, especially in the context of mobile banking, which is used by the majority of people these days. Due to the number of users and the possibility of stealing money, mobile banks are a particularly attractive target for attackers. Attackers are aware of the fact that a bank cannot overcome human error entirely with just technical means, so the prevention of smishing requires a comprehensive approach that includes a combination of user education, technical solutions and cooperation with banks and security experts.

KAZALO VSEBINE

KAZALO TABEL

KAZALO GRAFOV

UPORABLJENI SIMBOLI IN KRATICE

Smishing – SMS-ribarjenje

Phishing – ribarjenje

SMS – short message service ali sistem kratkih sporočil

Scareware – strašilna programska oprema

Baiting – zvabljanje žrtev v izvajanje zlonamernih dejanj, kot sta odpiranje zlonamernih povezav ali prenos zlonamernih datotek

Pretexting – uporaba lažne identitete v namene pridobitve zaupnih informacij od žrtve

spear phishing – usmerjena oblika ribarjenja, kjer napadalci pridobivajo občutljive informacije od specifičnih posameznikov ali organizacij

whaling – usmerjenja oblika ribarjenja, kjer napadalci ciljajo na osebe na visokih položajih za namene izvajanja goljufij

1 UVOD

V zadnjih 20 letih internet vsako leto pridobiva na svoji pomembnosti pri vlogi v globalni komunikaciji in se vedno bolj integrira v vsakdanja življenja ljudi do te mere, da so pametne naprave že skoraj integriran del ljudi. Inovacije, hitrost delovanja in nizki stroški so povečali dostopnost, uporabo in zmogljivost interneta. Zaradi teh dejavnikov ima danes internet več kot 3 milijarde uporabnikov. Ta množica uporabnikov vsako leto prinaša na milijarde evrov dobička na svetovnem trgu (Patterson & Nurse, 2022)

Internet je postal nepogrešljiv del vsakdanjega življenja. Uporablja se za nakupovanje, elektronsko pošto, izobraževanje ter komunikacijo. Družbena omrežja, kot sta Twitter in Facebook, so poleg ljudi izkoriščene tudi s strani raznih novinarskih podjetij za hitro širjenje novic.

Družbena omrežja so poleg komunikacij in obveščanja postala ključna tudi za podjetja, ki preko njih s pomočjo promocij dosežejo ogromno število ljudi, ki je bilo včasih nepredstavljivo (Siddiqui & Singh, 2016).

Vsak nov razvoj pa s sabo prinese tudi ljudi in organizacije, ki poskušajo izkoristiti tehnologijo za kriminalna dejanja. Tveganja, ki izhajajo iz kriminalnih dejanj, ki nastanejo iz finančnih in političnih motivov so vsako leto večja in naprednejša (Scott et al., 2021), čeprav je bilo leta 2022 investiranih skoraj 170 milijard dolarjev v varnostne investicije in obvladovanje tveganj (Gartner, 2022). Kljub vsem tem investicijam je britanska vlada leta 2022 v raziskavi ugotovila, da je kar 72 % od 1200 podjetij in organizacij doživelo neko vrsto incidenta s področja kibernetske varnosti (Patterson & Nurse, 2022).

Dejstvo je, da se bodo današnje organizacije morale sprijazniti, da so varnostni incidenti skoraj neizogibni. Po podatkih world economic foruma 95 % incidentov kibernetske varnosti nastane zaradi človeške napake, zaradi česar bodo morala podjetja investirati v izobraževanja in učenje iz napak (World Economic Forum, 2022).

Tako kot pri večini kibernetskih napadov je tudi pri smishingu cilj napada kraja občutljivih informacij in denarja. Smishing je izraz, ki je sestavljen iz besed »SMS« in »phishing« ter se nanaša na zlonamerne aktivnosti, ki se izvajajo prek SMS-sporočil. Delež populacije se je že naučil prepoznavati phishing poskuse, ki se dogajajo na e-pošti. Smishing tako predstavlja novo grožnjo, ki je ljudje ne pričakujejo in na to niso pozorni. Napadalci imajo tako več možnosti za uspeh pridobivanja osebnih podatkov in finančnih podatkov. (Yeboah-Boateng Ezer Osei & Mateko Amanor).

Po podatkih SI-CERT je bilo leta 2022 pri nas kar 1432 phishing incidentov, pod katere spada tudi smishing, ki je v strmem porastu. Opažen je trend, da napadalci preko SMS-sporočil pod pretvezo preverjanja podatkov ali potrjevanja transakcij želijo pridobiti avtentikacijske podatke za dostop do žrtvine elektronske banke (SI-CERT, 2023a).

1.1 Namen in cilji

Namen diplomskega dela je raziskati smishing, saj je ta vrsta kibernetskega kriminala v porastu zaradi vedno večje uporabe mobilnega bančništva. Napadalci izkoriščajo to porast za oškodovanje uporabnikov, ker se večina ljudi ne zaveda, da je tak napad sploh izvedljiv. Identificiral se bo tudi vzorec napadov in njihove posledice za uporabnike in banke.

Cilj diplomskega dela je analizirati ključne vidike in tveganje, ki ga predstavlja smishing, ter s pomočjo ankete ugotoviti, koliko ljudi v Sloveniji je ozaveščenih o tovrstnih napadih.

1.2 Raziskovalna vprašanja in hipoteze

Raziskovalna vprašanja zaključnega dela:

- Kako se uporabniki odzivajo na prejemanje smishing sporočil in kako pogosto poročajo o njih?
- Kolikšno je število izvedenih prevar v zadnjih letih (v primeru, da so banke pripravljene deliti te informacije)?
- Kakšni so trenutni varnostni postopki, da se minimizira možnost uspešnih smishing napadov na uporabnike?

Hipoteze zaključnega dela:

- H1: Veliko število uporabnikov mobilnega bančništva se je že srečalo s poskusi spletnih prevar.
- H2: Ozaveščenost ljudi o obstoju smishinga je nizka.
- H3: Smishing je postal eden izmed najpogostejših metod za napade v bančništvu.
- H4: Psihološki vidiki prevar in manipulacije igrajo pomembno vlogo pri uspešnosti smishing napadov.

2 MOBILNA OMREŽJA IN TEHNOLOGIJA POŠILJANJA SMS-SPOROČIL

Prva generacija mobilnih omrežij je bila predstavljena konec 70. let prejšnjega stoletja, v uporabo pa je prešla v začetku 80. let. Temeljila je na podlagi analognega omrežja. Generacije bomo v nadaljevanju označevali s kratico G. (PCMAG, n. d.)

V 90. letih smo doživeli razvoj 2G in 2,5G. 2G se je osredotočala le na brezžično komunikacijo (GSM), ki naj bi nadomestila analogne PSTN- in ISDN-telefone, medtem ko je 2,5G že omogočala minimalni prenos podatkov (GPRS, EDGE, IS-95B), merjenih v kilobitih na sekundo. (PCMAG, n.d.)

V prelomu tisočletja je bil predstavljen 3G, ki je že omogočal višje prenose podatkov (1 Mbit/s). Večina 3G-omrežij je po svetu dandanes že ukinjenih, da se frekvence lahko porabijo za druge namene. (Kakkar, 2016)

4G je hitrosti prenosa podatkov le še nadgradila, podpira pa tudi različne IP-protokole, zaradi česar prihaja do neke vrste združevanja mobilnih in fiksnih storitev. (Kakkar, 2016)

Zaenkrat zadnja generacija, imenovana 5G, je bila svetu prvič predstavljena leta 2018 in se je šele nedavno začela uporabljati v večjem obsegu. 5G omogoča do sedaj najvišje hitrosti prenosa podatkov – do 1Gbit/s. 5G poleg velikih hitrosti omogoča tudi večje kapacitete na baznih postajah, kar pomenih, da je hkrati lahko povezanih več uporabnikov, hitrost pa pri tem ne trpi v tolikšni meri, kot pri 4G. (Bhalla Vardhan Anand & Bhalla Ratana Mudit, 2010)

2.1 Trenutna raba mobilnih omrežij in njihova varnost

Najpopularnejši omrežji sta ta trenutek 4G in 5G, od starejših generacij pa je po večini v uporabi le še 2G, saj deluje kot nek “backup” v primeru, da pride do kakšne okvare. Kar se tiče varnosti, je najmanj zaščiten 2G, saj ponuja slabo enkripcijo med bazno postajo in napravo, kar lahko privede do prestrezanja sporočil in klicev. (Rupprecht et al., 2018)

Novejše generacije (4G in 5G) so v primerjavi s starejšimi bolje zaščitene, kar se tiče same enkripcije podatkov, ki potujejo med baznimi postajami ali pa med bazno postajo in napravo. Ker pa delujejo med drugim tudi na IP-protokolih, jim grozijo ranljivosti, kot so DDoS-napadi, IP-spoofing … (Rupprecht et al., 2018)

2.2 Tehnologija pošiljanja SMS-sporočil

SMS-sporočila so bila predstavljena skupaj z 2G-omrežjem. Protokol oziroma tehnologija, ki omogoča pošiljanje teh kratkih sporočil, pa sprva ni bila namenjena temu, zaradi česar je kot taka tudi omejena. Omejitev enega sporočila je nekje 140 bitov, kar zadošča za 160 latinskih znakov ali številk, za nelatinske pisave pa 70. (Taylor & Vincent, 2005)

Pošiljanje SMS-sporočil temelji na SMPP-protokolu (short message peer to peer), ki omogoča komunikacijo naprave z baznimi postajami operaterjev. SMPP se uporablja tako za prejemanje kot pošiljanje sporočil. Gre za TCP/IP-protokol, ki omogoča hitro pošiljanje in dostavljanje sporočil. Primer: Ko vtipkamo in pošljemo sporočilo, le-ta potuje prek radijskih valov najprej do nadzornega centra, ki nato sporočilo usmeri proti ustrezni bazni postaji, da je lahko dostavljeno. (SMS-Magic, 2020)

2.3 Ranljivosti

SMS-sporočil dandanes ne uporabljamo več le za komunikacijo drug z drugim, temveč prek SMS-sporočil prejemamo tudi enkratna gesla za prijave v račune, potrjevanje prijav Ta mehanizem je bil uveden predvsem zaradi raznih phishing prevar in vdorov v račune. Uporabnik prejme kodo prek enkratnega SMS-sporočila, to vrsto zaščite računov pa imenujemo dvofaktorska avtentikacija. Za to vrsto dvofaktorske avtentikacije se največkrat organizacije odločijo, ker je najcenejša, ni pa najbolj varna. (Mulliner Collin et al., 2014)

Vrste napadov, ki pretijo na poslana SMS-sporočila, so:

- Fizični dostop do telefona: če napadalec dobi fizični dostop do telefona, lahko zlahka pride do enkratnih gesel, ki jih oseba prejme prek SMS-sporočila. Sam fizični dostop do telefona ni enostaven, zato ta metoda ni najbolj popularna
- SIM Swap prevara: gre za neke vrste socialni inženiring, kjer je cilj pridobiti SIM-kartico žrtve na način, da operater izda novo (nadomestno). S tem, ko napadalec pridobi SIM-kartico, bo namesto žrtve prejel vse klice in sporočila (med drugim tudi SMS-sporočila z gesli). To je resna grožnja predvsem za mobilno bančništvo.
- Brezžično prestrezanje: že zgoraj je bilo omenjeno, da se sistemi za preverjanje pristnosti sporočila nanašajo zgolj na varnost mobilnih omrežij. Problem nastane predvsem za sporočila, ki so poslana prek GSM- in 3G- tehnologije – obe tehnologiji nudita šibke algoritme enkripcije in imata pomanjkanje na področju medsebojne avtentikacije med baznimi postajami in napravami. Ravno zaradi pomanjkanja medsebojne avtentikacije prihaja do lažnih napadov in prestrezanja na baznih postajah (man in the middle napadi).
- Trojanski konji na mobilnih napravah: zlonamerna programska oprema (predvsem trojanski konji) so posebej zasnovani za prestrezanje SMS-sporočil, ki lahko vsebujejo enkratna gesla za avtentikacijo. To programsko opremo v veliki večini primerov nenamenoma namesti uporabnik sam s kliki na sumljive spletne

strani in mesta, ki nato vodijo do prenosa škodljivih datotek na napravo. (Mulliner et al., 2014)

3 MOBILNO BANČNIŠTVO

Z vzponom interneta v poznih 90. letih prejšnjega stoletja je dobilo mobilno bančništvo svoje začetke. Na začetku je samo peščica bank na svetu zagotavljala storitve preko spletnih mest, ki so bile za današnje standarde zelo osnovne. Te osnovne storitve so obsegale samo pregled stanja računa in iskanje bankomatov, ki so bili v bližini uporabnika. V tistem času te storitve niso bile zanesljive in prijazne za uporabnike, kar je pomenilo, da so pričakovali, da bo bančništvo na daljavo omejeno samo na osebne računalnike. Kar ni čudno, ker nihče ni pričakoval, da so današnji pametni telefoni sploh možnost. (Cleveland, 2016)

Pametni telefoni, ki so v zadnjih letih postali integriran del ljudi, so bili takrat nepredstavljivi. Njihov obstoj je bil ključen za rast mobilnega bančništva, vendar se je mobilno bančništvo ves čas razvoja spopadalo z ovirami. Največji izzivi takrat so bili slaba dostopnost, funkcionalnost, počasno osveževanje zaslona in malo funkcij za današnje standarde. Poleg slabe uporabniške izkušnje so bili v tistem času stroški, ki so povezani z gostovanjem in storitvami spletnih mest dovolj visoki, da se veliko bankam ni zdelo vredno implementirati mobilnega bančništva. Zaradi tega so fizične poslovalnice za veliko večino ljudi ostale edin način uporabe bank. Leta 2007 so se pojavili prvi pametni telefoni, ki so bili dostopni širšemu trgu. Ta napredek v kapaciteti so banke hitro izkoristile z uporabniku prijaznejšimi aplikacijami, ki so strankam omogočale dostop do svojih računov, prenos sredstev in plačilo računov. Ta nova priročnost je ljudi vodila v trend sprejemanja mobilnega bančništva do današnje mere, ko skoraj ni človeka, da ne uporablja te tehnologije.(Sorbet, 2022)

Največje prednosti mobilnih bank so:

1. Stalna dostopnost – mobilni telefon je prenosljiv in vedno pri uporabniku, kar omogoča uporabo in nadzor kadarkoli pod pogojem, da ima internetno povezavo. Ta dejavnik je zelo pomemben pri potovanjih.
2. Usmerjenost lokacije – pametni telefon lahko GPS prepozna in tako personalizira storitve na podlagi lokacijskih storitev. GPS lahko prepozna uporabnikovo lokacijo in mu preko funkcije »najbližji bankomat« pokaže lokacije vseh bankomatov uporabnikove banke, skupaj z informacijami o oddaljenosti, lokaciji in storitvah.
3. Priročnost – ljudje niso omejeni na delovni čas ali lokacije bank za dostop do elektronskih dejavnosti. To omogoča, da lahko na primer ljudje, ki nekje čakajo v vrsti, opravijo kakšen nakup ali plačilo preko mobilne banke in si tako olajšajo delo. (Rahmani et al., 2012)

Z vzponom mobilnega bančništva se je vzpenjal tudi kibernetski kriminal, ki je pa postavil vprašanje, ali so mobilne banke vredne zaupanja. Zaradi tega je redno testiranje bančnih aplikacij pomembno, saj odkriva ranljivosti ter poleg zaupanja ljudi prihrani tudi čas in stroške. Zaradi razvijajoče grožnje kibernetskih napadov so skozi leta banke razvile razne varnostne mere, ki ščitijo osebne podatke in poverilnice uporabnikov:

- certifikati za varne povezave (SSL), ki šifrirajo podatke, ki so poslani med mobilno aplikacijo in strežniki banke,
- večfaktorsko preverjanje identitete,
- biometrika,
- ojačanje varnosti aplikacije, kot je varovanje kode z namenom preprečitve zlonamernih dejavnosti,
- redni varnostni pregledi in posodobitve, da se prilagajajo sproti, preden se zgodi uspešen napad,
- obvestila ob uporabi, ki uporabnike obvestijo transakcijah in prijavah na njihovem bančnem računu preko obvestil. (Kazuaki, 2023)

Nova tehnologija, ki se s kripto trga postopoma implementira tudi v mobilno bančništvo, je blockchain. Izraz izvira iz kriptovalute bitcoin, ki temelji na decentraliziranem sistemu, kjer so transakcije preverjene preko kompleksnih matematičnih operacij, ki se imenujejo dokaz delovanja (proof of work). Te operacije zagotavljajo natančnost transakcij in preprečujejo kibernetski kriminal. Ko je seznam transakcij, ki so združene v transakcijski blok (block), uspešno preverjen se doda v verigo (chain) blokov, ki sestavlja neki skupek blokov in se imenuje knjiga (ledger). Decentralizirana tehnologija blockchain temelji na soglasju pri veriženju blokov med člani omrežja, zaradi česar je varna in zanesljiva. (Ammouss, 2016)

Čeprav je bila ustvarjena za kripto trg, blockchain tehnologija ponuja mobilnemu bančništvu naslednje prednosti:

1. Nespremenljivost podatkov – ko se podatki zabeležijo v verigo blokov, jih ni več mogoče spreminjati ali brisati. To zagotavlja integriteto finančnih transakcij, ki je odporna proti zunanjim manipulacijam.
2. Transparentnost – transakcije, ki so zabeležene v veriženju blokov, so vidne vsem udeležencem v omrežju. Ta transparentnost veča zaupanje med uporabniki, ker lahko neodvisno preverijo informacije v njihovem veriženju blokov.
3. Kriptografska varnost – vsaka transakcija je šifrirana in povezana s prejšnjo, kar jo naredi zelo zanesljivo glede varnosti. Uporaba javnih in zasebnih ključev omogoča, da lahko do transakcij dostopajo samo pooblaščeni uporabniki. (Carrington, 2022)

4 VRSTE NAPADOV SOCIALNEGA INŽENIRINGA

Napadi socialnega inženiringa so najhitreje rastoča vrsta napada v današnjih omrežjih in so velika grožnja kibernetski varnosti uporabnikov. Za socialni inženiring bi lahko rekli, da je to kibernetski napad, ki se namesto na tehnične sisteme usmeri na ljudi. Zaradi tega lahko rečemo, da tako vrsto kibernetskega napada lahko izvaja vsak, ker tehnična sredstva niso potrebna. Pogostost kibernetskih napadov se veča, kar v praksi pomeni, da se je leta 2017 zgodil en kibernetski napad na 39 sekund. Ocenjeno je, da bodo do leta 2025 te vrste napadov nabrale do 10,5 milijarde evrov škode. Problem je tudi v tem, da je 95 % kibernetskih napadov socialnega inženiringa povezanih s človeškimi napakami, kar pomeni, da smo ljudje sami najšibkejši člen v obrambi proti kibernetskemu kriminalu. (Washo Hetro, 2021)

Bistvo socialnega inženirstva je pri prepričanju uporabnikov, da ogrozijo svoje informacijske sisteme. Namesto tehničnih napadov na sisteme se napadalci raje osredotočajo na ljudi, ki imajo dostop do informacij in z njimi manipulirajo. Izziv pri borbi proti takim napadom je to, da so tehnični zaščitni ukrepi večinoma neučinkoviti proti takim vrstam napadov. Poleg tega so ljudje velikokrat preveč samozavestni v svoje sposobnosti prepoznavanja takih napadov, kar omogoča napadalcem uspešno manipulacijo. (Krombholz et al., 2015)

V Sloveniji je bilo v letu 2022 beleženih 4123 kibernetskih incidentov, pri čemer je ocenjeno, da jih je bilo od teh 4123 incidentov kar 70 % napadov socialnega inženiringa.

SI-CERT je podal tudi lestvico najvišjih in povprečnih oškodovanj v kibernetskih napadih, na kateri za leto 2022 vsa mesta zasedajo napadi socialnega inženiringa. (SI-CERT, 2023a) V zadnjih dveh letih je bilo ribarjenje v svetu kibernetske varnosti med prevarami socialnega inženiringa že drugo leto zapored na prvem mestu. Ta vrsta napadov zdaj predstavlja kar 30 % vseh incidentov v kibernetskem prostoru. Statistični podatki SI-CERT nam kažejo, da je število napadov ribarjenja dramatično naraslo z 9 % v letu 2018,

16 % v letu 2019 in 25 % v letu 2020, in zdaj predstavlja levji delež 30 % vseh incidentov. Ta rast poudarja dejstvo, da so ljudje preveč samozavestni v svoje sposobnosti odkrivanja groženj.(SI-CERT, 2022)

Tabela 4.1: Znesek oškodovanja pri vrstah napada

Znesek oškodovanja	Vrsta napada
3.000.000 €	Socialni inženiring (Phishing napad z vrivanjem v poslovno komunikacijo. Napad je uspel, ampak je bil prenos denarja ustavljen s strani banke in Urada RS za preprečevanje pranja denarja)
400.000 €	Socialni inženiring (izsiljevanje z lažnimi grožnjami o pregonu)
58.000 €	Socialni inženiring (Povprečno oškodovanje v nigerijski prevari)
31.000 €	Socialni inženiring (Povprečno oškodovanje v ljubezenski prevari)
19.000 €	Socialni inženiring (Povprečno oškodovanje zaradi lažne tehnične pomoči Microsofta)
3.400 €	Socialni inženiring (Povprečno oškodovanje pri phishing zlorabi kreditne kartice)
780 €	Socialni inženiring (Povprečno oškodovanje pri spletnem nakupovanju)

Čeprav so si razne vrste napadov socialnega inženiringa različne, jih še vedno povezuje neki skupni vzorec. Ta skupni vzorec ima štiri stopnje (Salahdine & Kaabouch, 2019):

1. zbiranje informacij in raziskava tarče,
2. vzpostavljanje odnosa z žrtvijo preko direktnega stika ali e-pošte,
3. izkoriščanje vzpostavljenega odnosa in razpoložljivih informacij za izvedbo napada,
4. uspešen napad in umik.

Napadalec pri zbiranju informacij raziskuje tarčo tako, da zbira informacije iz različnih virov in načinov, kot so dumpster diving, javni dokumenti, spletne strani, socialna omrežja in stiki v živo. Raziskava tarče je zelo pomembna, ko je napad usmerjen v enega samega uporabnika. (Koyun & Al Janabi, 2017)

V fazi vzpostavljanja odnosa z žrtvijo bo napadalec z direktnimi stiki ali preko e-pošte poskušal s pomočjo manipulacije pridobiti zaupanje žrtve. Ko je zaupanje pridobljeno, bo napadalec izkoristil žrtev za razkritje kritičnih informacij, kot so npr. poverilnice ali podatki bančne kartice.

V zadnjem koraku bo napadalec uporabil podatke, ki jih je pridobil z manipulacijo, da bo dosegel svoj cilj, npr. dostop do bančnega računa žrtve (Ghafir et al., 2016)

4.1 Scareware

Scareware deluje na tak način, da prestraši uporabnika, ki potem zaradi strahu pred virusi namesti ali kupi programsko opremo, ki je škodljiva. Najpogosteje deluje tako, da dobi uporabnik pop-up oglas, da ima na računalniku škodljivo programsko opremo, ki se je lahko reši samo, če klikne na hiperpovezavo in naloži datoteko. Napadalci radi uporabljajo imena in logotipe znanih računalniških podjetij, kot so Google, ker s tem dajo uporabniku vtis, da je opozorilo na grožnjo legitimno. Če napadalec uspešno izvede napad, ponavadi dobi možnosti za (IBM, n. d. a):

- krajo identitete, ker uporabnik vpiše svoje podatke kreditne kartice,
- denarna korist, ker uporabnik kupi lažne protivirusne programe,
- uporabniku preda trojanskega konja, ki zbira občutljive informacije.

4.2 Baiting

"Baiting" oziroma vabljenje je vrsta napada socialnega inženiringa, ki se zanaša na človeško radovednost. Najpogosteje se uporablja tako, da napadalec nastavi vabo, ki je v tem primeru USB-ključek na nekem vidnem mestu. Ko žrtev opazi USB-ključek, ki ima po možnosti tako ime, da pritegne pozornost, se ne more upreti, da ga ne odnese domov ali v službo, kjer ga vstavi v računalnik. Če je USB vstavljen v računalnik, se zlonamerna programska oprema samodejno namesti v sistem in da napadalcu možnost, da ukrade osebne in finančne podatke. (Jones, 2022)

4.3 Pretexting

Pretexting je tehnika socialnega inženiringa, s katero napadalec manipulira z žrtvami, da razkrijejo občutljive informacije. Pretexting je izmišljen scenarij, ki si ga izmislijo napadalci z namenom kraje osebnih podatkov žrtve.

Med pretexting napadi se lahko napadalec pretvarja, da je uslužbenec ponudnika internetnih storitev in uporabi to lažno identiteto zaupanja, da dobi dostop do žrtvinega računalnika.

Ker pretexting napadi ne uporabljajo manipulacije s strahom, si mora napadalec izmisliti dobro zgodbo, da vzpostavi lažen občutek zaupanja, kot tudi odgovore na možna vprašanja s strani žrtve. (Imperva, n. d.)

4.4 Phishing

Phishing ali ribarjenje je prevara socialnega inženiringa, pri kateri napadalci od uporabnika poskušajo dobiti pomembne informacije, kot so gesla, osebne podatke ali bančne podatke, z uporabljanjem lažnih spletnih strani in elektronske pošte, pri kateri se pretvarjajo, da so legitimna podjetja. Phishing se najpogosteje izvaja preko e-pošte, kjer napadalec pripne zlonamerne povezave, ki preusmerijo žrtve na lažne spletne strani, kjer napadalci pridobivajo njihove zaupne podatke. (Siti Hawa Apandi et al., 2020)

Ribarjenje je po podatkih SI-CERT najpogostejši tip socialnega inženiringa in je v strmem porastu. Do leta 2018 so phishing prevare predstavljale samo 9,21 % primerov, vendar so v treh letih primeri eksplodirali na skoraj vsak tretji primer, kar pomeni, da je delež napadov leta 2021 predstavljal 29,90 % vseh kibernetskih prevar. Leta 2022 je pa phishing dosegel kar 40 % vseh napadov. Phishing se najpogosteje izvaja preko elektronske pošte ali lažnih spletnih strani, vendar so napadalci odkrili, da ljudje niso tako pozorni na phishing napade preko SMS-sporočil (smishing), zato je tudi ta vrsta phishinga v porastu. (SI-CERT, 2023)

4.5 Spear phishing

Spear phishing je vrsta phishing napada, ki je usmerjena na specifično osebo ali organizacijo. Napadi se ponavadi izvajajo preko zlonamerne elektronske pošte. Cilj napadalcev je namestitev zlonamerne programske opreme ter pridobivanje občutljivih informacij. (Kaspersky, n. d.)

Napadalci si vzamejo čas, da raziščejo njihove tarče tako, da ima sporočilo vtis, kot da je bilo poslano od nekoga, ki mu tarča zaupa. Če žrtev klikne na zlonamerno povezavo ali prilogo, lahko napadalec prevzame njihovo identiteto in je v omrežju neopažen. Glavna razlika med phishingom in spear phishingom je, da so phishing sporočila bolj splošna in lažje prepoznavna, ker se osredotočajo na ogromno število poslanih sporočil, medtem

ko so spear phishing sporočila specializirana za določeno osebo ali organizacijo, kar jim daje večjo možnost uspeha. (Lenaerts-Bergmans Bart, 2023)

Zaradi velike količine javno dostopnih informacij, ki jih ljudje objavljamo na socialnih omrežjih, kot sta Facebook in Linkedln, se napadalcem olajša delo. Po poročilu Omdie lahko napadalci ustvarijo prepričljivo spear phishing sporočilo že po samo 100 minutah splošnega iskanja na Googlu. (IBM, n. d.)

4.6 Whaling

Če je spear phishing podvrsta phishinga, je whaling podvrsta spear phishinga. Whaling napad uporablja enakih specializiranih sporočil kakor spear phishing, vendar pri whalingu napadalci specifično ciljajo na vodstvo v neki organizaciji z namenom, da razkrijejo finančne in druge zaupne informacije. Bistvo whaling napadov je dodatna specializacija na pomembnejše tarče z upanjem, da bo povzročena bistvena finančna ali informacijska škoda. (Lenaerts-Bergmans Bart, 2023)

5 KAJ JE SMISHING?

Smishing je vrsta kibernetskega napada, ki uporablja strategijo phishing napadov, ampak je poslan preko SMS-sporočila. Izraz smishing je sestavljen iz SMS in phishing. V smishing prevari napadalec pošlje lažno sporočilo določenemu številu prejemnikov, ki je lahko veliko ali pa usmerjeno na specifično osebo. V samem sporočilu uporabnike poskuša zavesti v razkritje občutljivih podatkov ali pa v storitev dejanja, ki mu škodi. (Din, 2022)

Smishing napadalci uporabijo večino trikov socialnega inženiringa na tak način, da pošljejo SMS-sporočila, ki imajo besedilo oblikovano na tak način, da v uporabniku vzbudi nujo in strah. Na ta način vabi uporabnika v to, da zaradi stresa ukrepa takoj in nepremišljeno in klikne na hiperpovezavo, ne da bi si vzel čas preveriti legitimnost sporočila. (Kaspersky, n. d.)

Cilj napadalcev je ponavadi pridobitev osebnih podatkov, poverilnic, finančnih podatkov in pa vodenje žrtev na zlonamerne spletne strani ali na prenos škodljive vsebine.

Pogosti primeri smishing sporočil so:

- Lažna varnostna obvestila: uporabnik dobi sporočilo, ki trdi, da je njegov bančni račun ogrožen ali zaklenjen in ga poskušajo zvabiti v to, da klikne na hiperpovezavo in razkrije svoje poverilnice in osebne podatke.
- Prevare z nagradami: sporočila, ki uporabniku sporočajo, da je prejemnik nagrade in da jo lahko prevzame, če posreduje svoje osebne podatke.
- Obvestila o dostavi: sporočila, ki se pretvarjajo, da so dostavna služba, pošljejo uporabniku hiperpovezavo, ki naj bi sledila paketu, če vpiše svoje podatke.
- Sporočila vladnih agencij: sporočila, ki vsebujejo hiperpovezavo pod pretvezo, da so vladne agencije, sporočijo uporabniku, da ima težave z davki. (Kaspersky, n. d.)

Pri smishingu kriminalci v svojih napadih pogosto uporabljajo SMS-spoofing, ki je eden izmed ključnih faktorjev pri uspešnosti SMISHINGA. Je zmožnost ponarejanja ID-ja pošiljatelja SMS, ki manipulira z imenom pošiljatelja v besedilnih sporočilih z namenom, da se predstavlja kot zaupanja vreden subjekt ali posameznik. Z razširjeno uporabo pametnih telefonov in VoIP je enostavno manipulirati identifikatorje klicateljev z nameščanjem ustreznih aplikacij na pametne telefone ali z uporabo storitev, ki ponujajo lažne identifikacije. Ker so telefonska omrežja razdeljena med različna podjetja in države, trenutno ni mehanizma za enostavno zaznavanje takšnih zavajajočih praks. To ranljivost so napadalci že izkoristili, na primer z manipulacijo identifikacije klicateljev v sili (npr. 112) ali za izvajanje goljufivih dejavnosti, kar je privedlo do resnih posledic. (Xu Wenyuan et al., 2014)

5.1 Kako napadalci pridobijo telefonsko številko

Pri smishingu imajo napadalci za pridobitev številk na voljo naslednje možnosti:

1. Družbeni mediji, spletni iskalniki in spletni imeniki:

V dobi digitalne povezanosti so telefonske številke pogosto javno objavljene na profilih družbenih medijev, spletnih straneh in v spletnih imenikih, pogosto brez vednosti ali privolitve lastnika. Napadalci to izkoriščajo s tehnikami, kot je spletno zbiranje podatkov (web scraping), s katerimi iz različnih spletnih platform zbirajo telefonske številke in druge osebne podatke, ki jih nato uporabljajo za izvajanje kibernetskih napadov. (Lemzy Alexa, 2022)

2. Tržnice na temnem spletu (Dark Web):

Temni splet je digitalno območje, nedostopno prek standardnih iskalnikov, ki vsebuje tržnice z nelegalnimi dobrinami in storitvami, vključno z bazami podatkov, ki vsebujejo milijone telefonskih številk. Na primer, aprila 2021 je bila na spletu objavljena zbirka podatkov, ki vsebuje informacije več kot 500 milijonov uporabnikov Facebooka (približno 20 % vseh naročnikov). Ključna vrednost teh podatkov je povezava telefonskih številk z identitetami. Vsak zapis v zbirki podatkov je vseboval telefonsko številko, veliko pa jih je vsebovalo tudi druge osebne podatke, kot so imena, datum rojstva, partnerski status itd. (Wadhwani Sumeet, 2021)

3. Generatorji številk in avtomatski klicatelji:

Napadalci pogosto uporabljajo avtomatske klicatelje in generatorje številk. To so napredne naprave, ki samodejno generirajo in kontaktirajo naključne telefonske številke, kar napadalcem omogoča, da dosežejo širšo populacijo brez ročnega posredovanja. Ko avtomatski klicatelj kontaktira z dejansko osebo, lahko napadalec uporabi različne manipulacijske tehnike, da posameznika na drugi strani prevara. (Robokiller, n. d. b)

5.2 Kje je smishing uporabljen

Smishing je uporabljen v primerih, kjer si napadalec za žrtve specifično izbere uporabnike mobilnih telefonov. Najpogostejše tarče napada so(IBM, n. d. b):

- Finančne institucije: Napadalci se lažno predstavljajo kot banke in pošiljajo SMS-sporočila, v katerih pod pretvezo preverjanja podatkov ali potrjevanja transakcij želijo izvabiti poverilnice za dostop do uporabnikove elektronske banke. (SI-CERT, 2023)
- Dostavne službe: Uporabnik dobi SMS-sporočilo, kjer je hiperpovezava z obvestilom, da lahko preko nje sledi paketu. Vendar pa mora po kliku na povezavo za sledenje razkriti svoje osebne podatke. (IBM, n. d. b)

- E-trgovine: Napadalci pošiljajo sporočila pod pretvezo, da so popularna e-trgovina in ponujajo lažne promocije in nagrade v zameno za osebne podatke.
- Vladne agencije: Zgodijo se tudi primeri, ko se napadalci predstavljajo, da so Finančna uprava RS pod krinko vračila davka.
- Socialna omrežja: SMS-sporočila z namenom pridobitve poverilnic, ki so zamaskirana kot potrditvene kode za vpis na omrežje ali pa varnostna opozorila.
- Dobrodelne organizacije: Poizkus manipulacije ljudi s pretvezo, da so dobrodelna organizacija, ki pomaga ljudem v stiski.
- Kraja identitete: Smishing je lahko uporabljen kot sestavni del v načrtu kraje identitete. Namen napadalcev je v tem primeru zbrati čim več informacij.
- V sodelovanju s phishingom: Ta taktika se večinoma uporablja s podvrstama phishinga whalingom in spear phishingom. Napadalci v tem primeru povečajo možnost, da žrtev nasede na prevaro, ker je napadena na več straneh. (SI-CERT, 2023)

Preko teh metod so v letu 2022 v ZDA napadalci uspešno ukradli več kot 20 milijard dolarjev. Kar je 100 % povečanje v primerjavi z 2021. (Robokiller, 2022)

Smishing napadi pa niso omejeni na samo te primere in so zelo prilagodljivi za oportunistično izkoriščanje katere koli situacije v večini situacij kibernetskega socialnega inženiringa. Z razvojem tehnologije bodo napadalci našli nove načine za implementacijo smishinga. (IBM, n. d. b)

6 SMISHING V BANČNIŠTVU

V zadnjih letih se je skupaj z digitalizacijo razvilo tudi mobilno bančništvo, ki ga dandanes uporabljajo skoraj vsi ljudje. Popularnost je pridobilo še posebej zaradi priročnosti in dostopnosti uporabe. Vendar pa napredek prinaša tudi nova tveganja in nevarnosti za uporabnika. Te storitve so zaradi števila in ranljivosti uporabnikov zelo pogosta tarča napadalcev, ki si prizadevajo pridobiti dostop do finančnih sredstev uporabnikov. Napadalci izkoriščajo različne metode, da lahko izkoristijo zaupanje uporabnikov do bančnih platform, kot so aplikacije in spletne strani. Posledično se povečuje tveganje za krajo identitete, finančne izgube in zlorabo osebnih podatkov. (Alhuseen & Anwar, 2017)

Phishing prevare so v zadnjih nekaj letih v strmem porastu. Do leta 2018 so phishing prevare predstavljale samo 9,21 % primerov, vendar so v treh letih primeri povzpeli na vsaki tretji primer, kar pomeni, da je delež napadov leta 2021 predstavljal 29,90 % vseh kibernetskih prevar. Leta 2022 je pa phishing dosegel kar 40 % vseh napadov. Phishing se najpogosteje izvaja preko elektronske pošte ali lažnih spletnih strani, vendar so napadalci odkrili, da ljudje niso tako pozorni na phishing napade preko SMS-sporočil (smishing), zato je ta vrsta phishinga v porastu. (SI-CERT, 2023)

Smishing je v primerih rastoča verzija phishinga, ki spada med najstarejše internetne prevare. Tako kot pri vseh ostalih prevarah socialnega inženiringa hočejo napadalci pri smishingu pridobiti poverilnice in osebne podatke svojih žrtev (MiPi, 2023). Po podatkih SI-CERT opažajo trend, da so v zadnjih letih prevare na telefonih vedno bolj pogoste. Napadalci pri smishingu v bančništvu najpogosteje uporabijo krinko preverjanja podatkov ali potrjevanja transakcij s končno željo, da tako pridobijo avtentikacijske podatke za dostop do uporabnikove elektronske banke. (SI-CERT, 2023)

Sama smishing sporočila vsebujejo eno ali več naslednjih metod:

1. lažna varnostna obvestila,
2. lažna verifikacija računa,
3. napad, ki vključuje vishing,
4. prevare z lažno obljubo nagrade,
5. smishanje za kodo 2-stopenjske avtentikacije,
6. smishanje za osebne informacije,
7. zahteve za plačilo,
8. phishing hiperpovezave.

1. Lažna varnostna opozorila:

- V napadu z lažnimi varnostnimi opozorili napadalec pošlje SMS-sporočilo uporabnikom e-banke in trdi, da je iz bančne varnostne ekipe. V sporočilu stranki navaja, da je bila na njenem računu zaznana sumljiva aktivnost in da je račun ogrožen. Uporabniku razloži, da mora takoj ukrepati s klikom na hiperpovezavo. (Shweta et al., n. d.)
- Namen takega napada je, da napadalec žrtev povede na lažno spletno stran, ki je narejena tako, da izgleda kot original. Na te spletni strani uporabnik po navadi vpiše svoje poverilnice z namenom, da se prijavi in jih na ta način razkrije napadalcu. (SI-CERT, 2023)

2. Lažna verifikacija računa:

- Pri prevarah z lažno verifikacijo računa napadalec pošlje uporabniku sporočilo, v katerem trdi, da je treba račun preveriti zaradi varnostnih razlogov. Napadalec navaja, da banka izvaja neko posodobitev varnostnih protokolov in da mora uporabnik potrditi svojo identiteto in podatke o računu, da se izogne nevšečnostim.
- Namen takega napada je, da uporabnik razkrije svoje podatke, kot so PIN-koda, številka računa ali številko socialnega zavarovanja. (Shweta et al., n. d.)

3. Napad, ki vključuje vishing:

- Tak napad zahteva večji trud napadalca, ker vključuje metodo vishing. Vishing je podvrsta phishinga, ki ima enake cilje pridobitve zasebnih informacij z razliko v temu, da se vishing izvaja preko glasovnih sporočil in klicev
- Napadalec napad začne s smishing sporočilom, v katerem trdi, da je v banki nujna situacija. Po sporočilu, ki v uporabniku vzbudi paniko, napadalec osebno pokliče uporabnika in se predstavi kot uslužbenec banke. Med klicem poskuša čim bolj prestrašiti uporabnika, da mu razkrije poverilnice in osebne podatke ali pa da klikne na škodljivo hiperpovezavo, ki mu je bila poslana. (Center for internet security, 2023)

4. Prevare z lažno obljubo nagrade:

- Pri taki prevari napadalec pošlje sporočilo, v katerem trdi, da je bil uporabnik izžreban za denarno nagrado v posebni promociji.
- Napadalec želi izkoristiti uporabnikovo radovednost do nagrade. Za prevzem nagrade mora uporabnik posredovati osebne podatke ali pa plačati provizijo. (Diana Panduru, 2021)

5. Smishanje za kodo 2-stopenjske avtentikacije:

- V taki vrsti prevare se napadalec poskuša izogniti dobremu varnostnemu protokolu, znanem kot 2-stopenjska avtentikacija. Izogniti se mu poskuša tako, da uporabniku pošlje lažno zahtevo za prijavo.
- Napadalec poskuša pridobiti kodo 2FA, ki je poslana na uporabnikov telefon. Po poizkusu prijave pošlje uporabniku smishing sporočilo, v katerem trdi, da je banka ter da potrebuje kodo 2FA, ki je bila poslana na njegov telefon. Če uporabnik posreduje to kodo, jo bo napadalec pridobil dostop do uporabnikovega računa. (Global Guardian, n. d.)

6. Smishanje za osebne informacije:

- V taki prevari napadalec pošlje sporočilo, v katerem se pretvarja, da je banka. V sporočilo napiše, da mora uporabnik preveriti in posodobiti podatke na njegovem računu elektronskega bančništva.
- Cilj napadalca je pridobitev zaupanja in pridobitev podatkov. Če mu uspe pridobiti zaupanje, se mu odprejo vrata za dostop do številke računa, številke socialnega zavarovanja in gesla. Vsi te podatki ponujajo možnosti za izvedbo prevar. (Bank of America, n. d.)

7. Zahteve za plačilo:

- Cilj te prevare je prestrašiti uporabnika v nakazilo denarja z grozečim sporočilom. V sporočilu ponavadi piše, da prejemnik dolguje denar ali pa zamuja s plačilom. Napadalec kdaj doda grožnjo s tožbo, če se plačilo ne izvede takoj.
- Sporočilu, ki vsebuje zahtevo za plačilo, je dodana hiperpovezava, s katere napadalec zbira podatke o poverilnicah in osebnih podatkih. (Center for internet security, 2023)

6.1 Rešitve in predlogi za preprečevanje smishinga

Phishing in njemu sorodna prevara smishing oba spadata v napade socialnega inženiringa, ki so najpogostejša vrsta napada v kibernetskem prostoru. Ti napadi temeljijo na zvijači in se ne zanašajo na tipične tehnološke metode, kakor bi pričakovali od hekerjev, kar je eden izmed razlogov za nevarnost in pogostost takih napadov. Napadalci se zanašajo na to, da je človek najšibkejši člen v obrambi, zato je ocenjeno, da 98 % kibernetskih napadov uporablja neko vrsto socialnega inženiringa. Kar pomeni, da je to velika grožnja za banke, ker uporaba dodatnih tehničnih sredstev ne more premagati človeških napak. (Rock, 2021)

Preprečevanje smishinga zahteva celovit pristop, ki vključuje kombinacijo izobraževanja uporabnikov, tehničnih rešitev, sodelovanje med bankami ter varnostnimi strokovnjaki.

Ukrepe bi lahko na grobo razdelil v dve kategoriji, in sicer človeški faktor (uporabniki) in tehnične rešitve. Obe kategoriji sta med seboj povezani in igrata pomembno vlogo pri preprečevanju smishing napadov. Rešitve za uporabnike poskrbijo, da se prevara zaradi ozaveščenosti ustavi, še preden ima, preden ima priložnost oškodovati uporabnika. Tehnične rešitve so pa primarno samo dodatna pregrada, čeprav ne morejo popolnoma preprečiti napadov. Lahko bi rekli, da več kot je tehničnih rešitev več časa mora napadalec porabiti v fazi direktnega kontakta in manipulaciji žrtve. Ta dodatni čas velikokrat omogoča uporabniku, da prepozna prevaro, preden postane žrtev. (Anshul Kumar et al., 2015)

6.1.1 Izobraževanje uporabnikov

Ker sposobnost uporabnika pri prepoznavanju groženj na telefonu prevzema največjo vlogo pri prepoznavanju smishing sporočil je smiselno, da je največji poudarek potreben pri izobraževanju uporabnikov mobilnih bank. Dejstvo je, da si vsi uporabniki mobilnih bank niso enaki. Večina ljudi nima nobenega znanja o kibernetski varnosti še posebej, če niso v poklicu, kjer morajo uporabljati informacijske sisteme. Ljudje, ki v svojem poklicu uporabljajo računalnik in so v sklopu službe imeli izobraževanja in teste za prepoznavo phishing sporočil imajo večjo možnost prepoznave smishing sporočil, ker se znanje zaradi podobnosti napadov do določene mere prenese. Ampak je tudi to v veliki meri odvisno od previdnosti osebe. (Ahsenali et al., 2016)

Dejavnik, ki je pomemben, je, da uporabnik pri uporabi mobilne banke nima nobene obveznosti za izobraževanje, ker je sam odgovoren za svoja dejanja. To pa ne pomeni, da banka ni dolžna ponuditi uporabniku vsaj nekaj osnovnih informacij, kot so:

- kaj je smishing,
- pogoste strategije napadov smishinga,
- opis posledic uspešnega napada,
- pomoč pri identifikaciji smishing sporočil,
- mesto, kam in kako se lahko prijavijo prevare.

Dobra možnost za izobraževanje, ki pa v slovenski obliki na žalost ne obstaja, je izobraževanje v obliki iger. To so interaktivne igre, ki, jih je možno igrati v kratkem časovnem obdobju. V tujini so razvili igro z imenom Anti-phishing Phil. V igri lahko ljudje na interaktivni način preizkusijo svoje znanje o prepoznavi hiperpovezav, domenskih imen in lažnih spletnih straneh. Igra Anti-phishing Phil je bila preizkušena na 4500 ljudeh in je pokazala, da je pri ljudeh brez prejšnjega znanja o raznih vrstah ribarjenja izboljšala sposobnost za prepoznavo prevar za 61 %. (Hong, 2012)

6.1.2 Tehnične rešitve

Čeprav je poudarek na izobraževanju uporabnikov ključni dejavnik kibernetske varnosti, je vseeno pomembno, da banke izboljšujejo svojo tehnično varnost, ker s tem omogočijo uporabniku več orodij za zaščito proti napadom.

UPORABA AVTENTIKACIJE

Tehnološka rešitev, ki se je izkazala za uspešno proti vsem vrstam napadov socialnega inženiringa, je 2-stopenjska avtentikacija (2FA). Dvostopenjsko preverjanje je sistem za upravljanje dostopa do računov, ki zahteva več kot samo geslo. 2FA deluje tako, da uporabnik po vpisu gesla v aplikaciji dobi SMS-sporočilo s kodo, ki jo mora vpisati v aplikacijo, da lahko dobi dostop do računa. (Ray Allison Peter, 2019)

Največja prednost 2-stopenjske avtentikacije in večstopenjske avtentikacije je, da napadalec ne dobi takoj popolnega dostopa do žrtvinega računa in mora vložiti dodatni trud, kar pa da uporabniku večjo možnost za prepoznavo in reagiranje na prevaro.

Pomanjkljivost 2-stopenjske avtentikacije je, da metoda ni zmožna popolnoma odpraviti smishinga, ker lahko napadalec z manipulacijo pridobi tudi kodo za enkratno uporabo.(Jansen, 2023)

UPORABA BIOMETRIKE

Biometrična avtentikacija je oblika preverjanja pristnosti, ki uporablja biometriko za zaznavanje in preverjanje identitete uporabnika, ki ima željo dostopati do mobilnih aplikacij. Obstaja več vrst biometrike na primer prstni odtisi, prepoznavanje obraza, prepoznavanje glasu. Metoda biometrike je lahko uporabljena kot dodatek pri prijavi v aplikacijo ali pa nadomestilo uporabniškemu imenu in geslu. (Sharma Rajeev, n. d.)

Bistvo biometrike je omogočanje napravam, da uporabljajo fizične značilnosti uporabnikov, kot so prstni odtisi, obraz ali glas. Za aplikacije in račune, ki morajo biti zaradi občutljive narave dela dodatno zaključeni, je biometrika lahko odličen dodatek večfaktorski avtentikaciji. (Sharma Rajeev, n. d.)

Velik delež uporabnikov mobilnega bančništva je že seznanjen z biometrično avtentikacijo, ki je uporabljena za dostop do mobilne aplikacije banke. Poleg prijave v račun se pa prstni odtis in prepoznava obraza uporabljata tudi pri plačilih, ki se izvajajo preko mobilne aplikacije. (Onfido, 2022)

Največji prednosti pri uporabi biometrike na mobilnih telefonih sta:

- priročnost,
- večjo varnost pri avtentikaciji.

Glavni prednosti prihajata iz dejstva, da za uporabo biometrike na pametnih telefonih ne potrebujemo nobene specializirane strojne opreme in da je večina uporabnikov modernih pametnih telefonov že seznanjena z biometrično avtentikacijo za odklepanje naprave. Pri prijavi v aplikacijo morajo uporabniki le pogledati v telefonsko kamero ali pa položiti svoj prst na senzor prstnega odtisa. To je hitreje kot vpisovanje kompleksnega gesla, ki ima lahko veliko posebnih znakov. Kljub uporabi biometrike bodo gesla še vedno v rezervi za mobilno aplikacijo. Kar pomeni, da se bodo gesla vnašala manj pogosto in

bodo banke posledično lahko uvedle pogoje za bolj kompleksna gesla brez, da bi s tem zmanjšale uporabnost in prijaznost uporabe. (National Cyber Security Centre, 2022)

Omejitve in pomanjkljivosti biometrike se po navadi nanašajo na natančnost in zanesljivost. Na to vplivajo razni dejavniki, kot so kakovost senzorja, osvetlitev, koti in okoljski pogoji. Na senzorje vplivajo tudi poškodbe, staranje in nošenje mask. Vsi našteti dejavniki lahko vodijo v lažno pozitivne ali lažno negativne rezultate. Poleg tega biometrična avtentikacija nima enake prilagodljivosti kakor gesla. Če pride do situacije, da so biometrični podatki razkriti, izgubljeni ali ukradeni jih ni tako preprosto zamenjati ali ponastaviti. Ta togost vpliva na težavnost pri obnovitvi računa, spreminjanju biometričnih podatkov in poveča možnost kraje identitete. (Dmitry et al., 2023)

Vzpon naprednih deepfake tehnologij ima potencial, da postane v prihodnosti grožnja biometrični varnosti. Deepfake tehnologija, ki je pod nadzorom umetne inteligence, ima možnost ponarejati zvok, vizualne vsebine in besedilo. Možnost ponarejanja vizualne vsebine je lahko nevarna pri uporabnikih, ki uporabljajo prepoznavo obraza. Napadalci imajo potencial, da preko slik, ki so najdene na socialnih omrežjih, ustvarijo modele obraza, ki so zmožni pretentati bančno avtentikacijo. (Kvartalnyi Nazar, 2023)

PROGRAMSKA OPREMA

Programska oprema za telefone, ki se uporablja za preprečevanje smishinga in drugih prevar, običajno uporablja algoritme in baze podatkov, v katerih pridobijo znane lažne številke. Ko program zazna sumljivo SMS-sporočilo, lahko programska oprema opozori uporabnika, blokira sporočilo ter obvesti uporabnika, kakšen je najboljši postopek ukrepov. Načeloma ima taka programska oprema razne funkcije, kot so skeniranje, filtriranje sporočil in blokiranje znanih smishing virov. (Pradeep Kumar Roy et al., 2020)

Poleg stalne zaščite programska oprema velikokrat nudi tudi izobraževanja za uporabnike o pogostih taktikah napadov, kar uporabnikom poveča možnosti, da sami prepoznajo možne grožnje. To znanje, če je upoštevano, omogoča uporabnikom sprejemanje pametnih odločitev, ki onemogočijo napade. S koristenjem programske opreme lahko uporabniki zmanjšajo možnost smishing sporočila tudi za 99 %.(Zimperium, n. d.)

Eden izmed ponudnikov programske opreme proti smishingu in vishingu je Robokiller. V svoji aplikaciji uporabljajo naslednje ukrepe:

1. Algoritem za blokiranje klicev, ki deluje tako, da proaktivno analizira klic v manj kot sekundi, kar omogoča blokiranje klice, preden uporabniku zazvoni telefon.
2. Avdio odtis, ki beleži edinstvene zvočne posnetke napadalca in ga primerja s podobnimi avdio odtisi v globalni zbirki podatkov. Ta rešitev omogoči, da se napad prepreči že v samem začetku.
3. Strojno učenje in umetna inteligenca omogočata programu, da se uči in sprejema odločitve brez usmerjenega programiranja. Te tehnologiji se uporabljata z analizo metapodatkov, kot so informacije o telefonskih klicih, telefonske številke, časi klicev in trajanja klicev.
4. Blokiranje neželenih sporočil, program uporablja lastniški algoritem, umetno inteligenco in strojno učenje za analizo izvora vsebine in priponk vsakega sporočila. Ko je sporočilo poslano, aplikacija ugotovi, ali je varno sporočilo ali neželeno sporočilo. V primeru, da je sporočilo neželeno, bo sporočilo premaknjeno v posebno mapo in ne bo motilo uporabnika.
5. Prilagodljivo blokiranje, kjer si lahko uporabnik nastavi želeno raven moči filtriranja.(Robokiller, n. d. a)

7 METODOLOGIJA

V okviru raziskave o smishingu v bančništvu, smo se osredotočili na uporabe kvantitativne metode s pomočjo ankete, pri kateri je bilo anketiranih 155 ljudi. Demografska sestava vzorca je skoraj popolnoma identična, s 57 ženskimi in 56 moškimi odgovori. Pri starostnih skupinah je bila najbolj procentualno najbolj beležena skupina kategorija od 18 do 24 let z deležem 30 %, sledile so starostne skupine 25−35 let (25 %), 36−50 let (14 %) ter 61+ let (3 %).

Kvantitativna metoda, ki je bila implementirana preko ankete, je bila ustvarjena z namenom ugotovitve ozaveščenosti uporabnikov o smishing prevarah. Analiza rezultatov ankete je omogočila pridobitev podatkov, ki nam pokažejo sliko o stopnji ozaveščenosti anketirancev glede obstoja smishing prevar ter dejavnikih, na katere so uporabniki pozorni, ko se odločajo, ali se bodo odzvali na SMS-sporočilo. Poleg tega smo pridobili tudi podatke o ukrepih, ki jih anketiranci uporabljajo, da se zaščitijo pred smishing napadi med uporabo e-bank. Anketa za zbiranje podatkov je bila narejena in izvedena preko spletne platforme 1ka.si v časovnem obdobju od 23. 11. 2023 do 2. 12. 2023, pri čemer je bilo pridobljenih 115 izpolnjenih anket. Ta metodološki pristop nam bo omogočil razumevanje ravni ozaveščenosti in pripravljenosti uporabnikov na izzive varne uporabe mobilnih bank. Pomagal nam bo pa tudi identificirati možne šibkosti uporabnikov za bodoče izboljšanje varnosti.

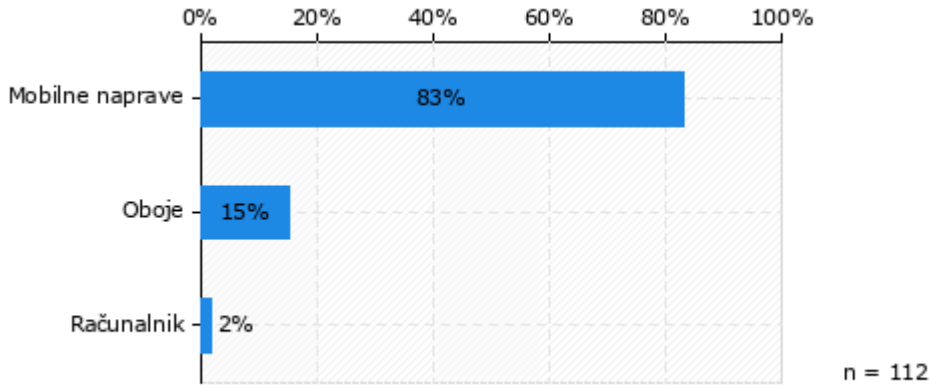
7.1 Rezultati in analiza anket

Prvo vprašanje »Na katerih napravah najpogosteje uporabljate e-banko?« je namenjeno pridobitvi informacij o trendih uporabe e-bančništva v današnjem času. Izjemno visok odstotek, 81 % udeležencev raziskave najpogosteje uporablja e-banko na mobilnih napravah, kar jasno dokazuje priljubljenost in praktičnost mobilnega bančništva.

Samo 2 % anketirancev e-banko uporablja na računalniku, kar kaže izredno mali obseg uporabe računalnikov za storitve e-banke.

Izmed danih možnosti obstaja pa tudi 15 % delež anketirancev, ki se poslužujejo uporabe obeh vrst naprav.

Podatki jasna kažejo na to, da je mobilno bančništvo prevladujoča oblika uporabe e-bank, kar pomeni, da si varnost mobilnih naprav in ozaveščanje uporabnikov v prihodnosti zaslužita prioriteto.



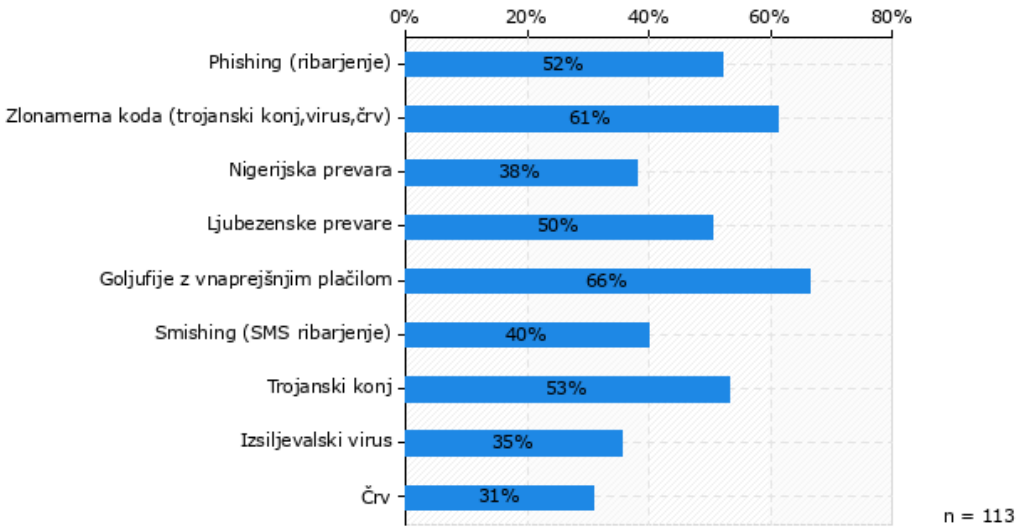
Graf 7.1: Na katerih napravah najpogosteje uporabljate e-banko?

Naslednje vprašanje se spusti v anketirančevo splošno ozaveščenost glede kibernetskih prevar. Odgovori nam pokažejo, koliko so ljudje ozaveščeni glede raznih kibernetskih groženj. Prepoznava je nad 60 % prišla samo pri dveh podvprašanjih, in sicer pri »Goljufije z vnaprejšnjim plačilom«, ki je doseglo najvišjo stopnjo prepoznavnosti pri 66 % in »Zlonamerna koda (trojanski konj, virus, črv)« z 61 %.

Najmanjši prepoznavi sta bili pri izsiljevalskem virusu (35 %) in črvom s 31 % prepoznavo, kar ni presenetljivo, ker sta oba kibernetska napada med najmanj številnimi v zadnjih nekaj letih.

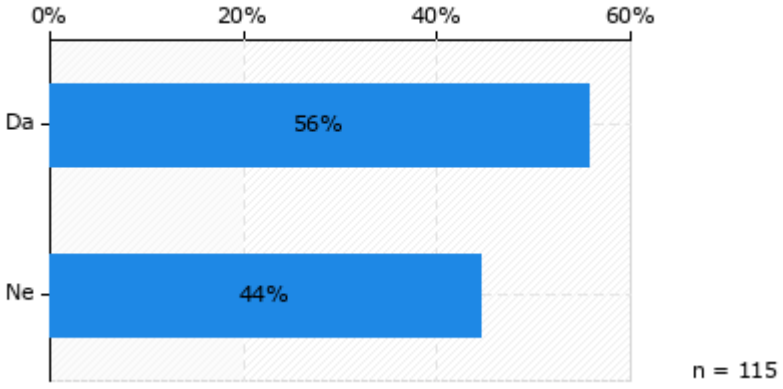
Med drugimi prevarami je 53 % anketirancev seznanjenih s trojanskim konjem, 38 % z nigerijskimi prevarami in 50 % z ljubezenskimi prevarami.

Phishing je že leta najbolj razširjena kibernetska prevara v slovenskem prostoru. Kljub letnim naraščajem pa seznanjenost ni najboljša z 52-% seznanjenostjo. Phishingu sorodna prevara smishing dosega pa 40-% prepoznavo, kar ni niti polovica anketirancev.



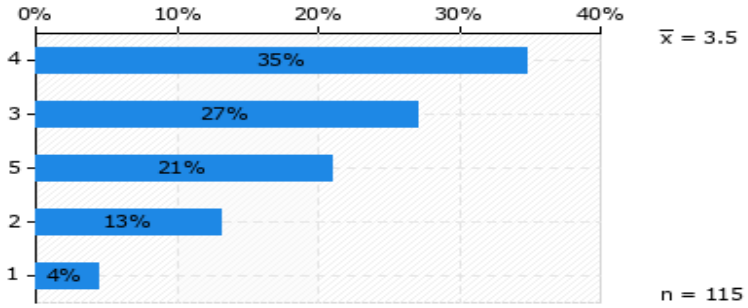
Graf 7.2: S katerimi vrstami prevar v kibernetskem prostoru ste seznanjeni? (Možnih je več odgovorov.)

Rezultati ankete o ozaveščenosti glede obstoja smishinga v bančništvu razkrivajo, da je znanje o obstoju takega napada pomanjkljivo. Samo 56 % udeležencev je seznanjenih z možnostjo ribarjenja preko SMS-sporočil, medtem ko 44 % ljudi še ni slišalo za to vrsto napada. Po teh podatkih lahko sklepamo, da je dodatno ozaveščanje ljudi nujno za preprečitev naraščanja napadov.



Graf 7.3: Ali veste, da je ribarjenje preko SMS-sporočil možno?

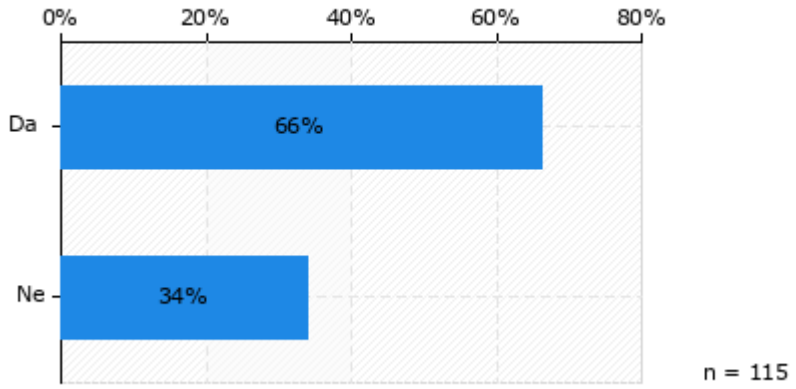
Rezultati vprašanja o samozavesti pri razlikovanju med lažnimi in legitimnimi SMS-sporočili v kontekstu smishinga v bančništvu kažejo, da se samo 4 % uporabnikov oceni s številko 1, kar odraža najnižjo stopnjo samozavesti, medtem ko 13 % uporabnikov ocenjuje svojo samozavest z oceno 2. Delež anketirancev 27 % nima ne dobrega ne slabega mnenja o svojih sposobnostih in se ocenjujejo z oceno 3. Največji delež uporabnikov, ki dosega 56 %, je skupek ocene 4 in 5 in odraža dejstvo, da večina ljudi meni, da so sposobni prepoznavati lažna sporočila.



Graf 7.4: Na lestvici od 1 do 5 ocenite, kako samozavestno se počutite pri razlikovanju med lažnimi in legitimnimi SMS-sporočili, kjer 1 pomeni najmanjšo stopnjo samozavesti in 5 najvišjo stopnjo samozavesti

Naslednje vprašanje v anketi pridobiva informacije o tem, ali so anketiranci že prejeli SMS-sporočilo, ki jih prosi za posredovanje osebnih informacij. Visok odstotek

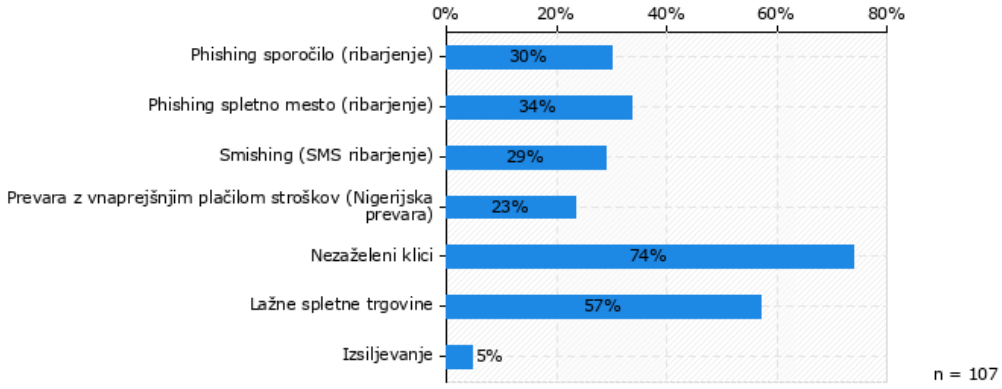
anketiranih (66 %) poroča, da so že prejeli SMS-sporočila, ki jih pozivajo k odprtju povezav ali posredovanju zasebnih informacij, kar poudarja široko razširjenost kibernetskih groženj. To kaže na potrebo povečanja ozaveščanja in izobraževanja uporabnikov glede prepoznave ter ravnanja s potencialno nevarnimi SMS-sporočili.



Graf 7.5: Ste že prejeli SMS-sporočila, ki vas pozivajo k odprtju povezave ali posredovanju zasebnih informacij?

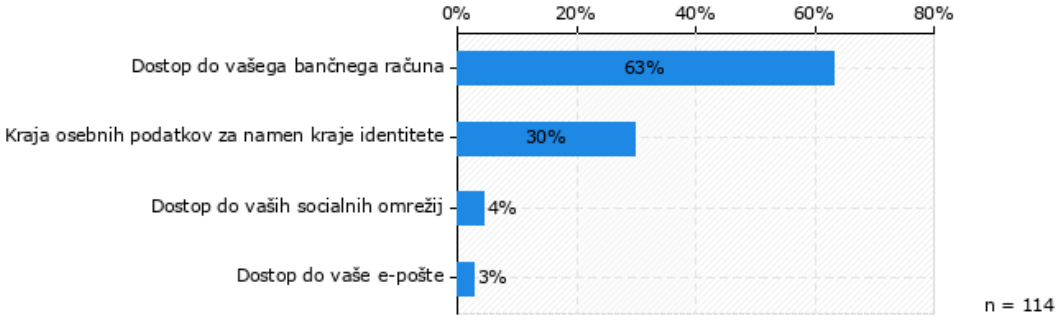
Rezultati vprašanja, ki raziskuje, če so anketiranci že kdaj bili tarča ene ali več groženj, razkrivajo raznolikost napadov, s katerimi se srečujejo uporabniki. Prva opazka, ki izstopa, so nezaželeni klici, ki jih je beležilo kar 74 % anketirancev, kar izpostavlja pogostost groženj na mobilnih napravah. Takoj za klici so na drugem mestu lažne spletne trgovine s 57 % anketiranci, medtem ko so phishing spletna mesta in phishing sporočila dosegla 34 % in 30 %. S smishingom se je srečalo 29 % anketirancev.

Na prevaro z vnaprejšnjim plačilom stroškov je naletelo 23 % ljudi. Izsiljevanje je najmanj prisotno, saj je na to grožnjo naletelo samo 5 % anketirancev.



Graf 7.6: Ste že kdaj bili tarča ene ali več naslednjih spletnih groženj? (Možnih je več odgovorov.)

Rezultati vprašanja o posledicah uspešne smishing prevare jasno kažejo, da se 63 % ljudi najbolj boji možnosti izgube dostopa do njihovega bančnega računa. Izguba računa pomeni potencialne finančne izgube, ki lahko prinašajo hude posledice za posameznike, ki so žrtve tega napada. Poleg tega se 30 % boji kraje osebnih podatkov za krajo identitete, kar izpostavlja strah za kasnejše zlorabe. Minimalni delež anketiranih pa skrbi za dostop do socialnih omrežij (3 %) in dostop do e-pošte (3 %).

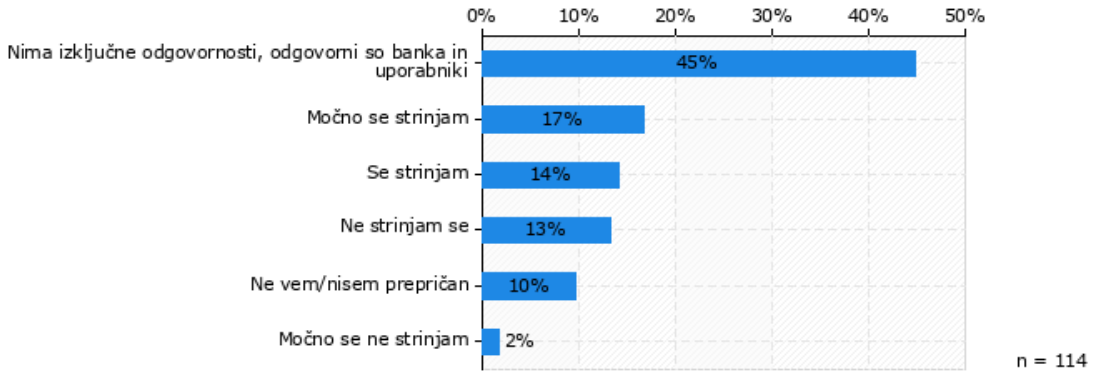


Graf 7.7: Kakšne posledice uspešne smishing prevare so po vašem mnenju najhujše?

Analiza rezultatov vprašanja, kako močno se strinjajo s trditvijo, da je varnost uporabnikov izključna odgovornost banke, odraža raznolike rezultate anketirancev. Zanimivo je, da je 10 % anketirancev brez jasnega mnenja, kar kaže na potrebo po boljšem razumevanju koncepta kibernetske varnosti. Nadaljnji podatki razkrivajo, da 15

% uporabnikov ne meni, da je banka izključno odgovorna za varnost uporabnikov e-bank, kar pomeni, da se zavedajo svoje odgovornosti pri varnosti na internetu.

Največji delež, ki znaša 45 %, pa izraža prepričanje, da sta uporabnik in banka skupno odgovorna za varnost. Ta delež anketirancev ima večjo možnost, da se izobrazi o kibernetski varnosti. Hkrati pa opažamo, da 31 % anketiranih meni, da odgovornost leži večinoma ali v celoti na strani bank, kar postavlja vprašanje o zaupanju uporabnikov v varnostne ukrepe bančnih organizacij.



Graf 7.8: Kako močno se strinjate z naslednjo trditvijo: "Varnost uporabnikov je izključno odgovornost banke."

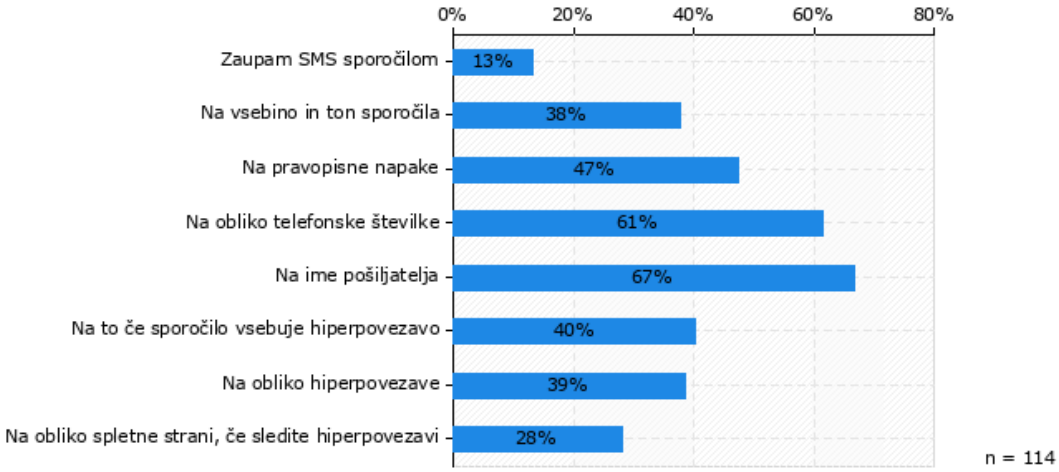
Pri naslednjem vprašanju je bilo za uporabnike postavljeno vprašanje, na katere dejavnike so pozorni pri odločanju o pristnosti sporočila, da se ugotovi, kaj vpliva na odločanje uporabnika o pristnosti sporočila v kontekstu smishinga v bančništvu.

Izstopata dva dejavnika, na katera so anketiranci najbolj pozorni pri prepoznavanju pristnosti sporočil. Kar 67 % vprašanih se zanaša na ime pošiljatelja, medtem ko si 61 % ljudi ogleda obliko telefonske številke. To kaže, da se večina ljudi osredotoči samo na najbolj osnovne načine prepoznave, ki pa zaradi iznajdljivosti napadalcev niso več zanesljivi pri preprečevanju smishing napadov.

Na pravopisne napake se osredotoča približna polovica anketirancev oz. 47 %, na vsebino in ton sporočila pa manj kot polovica (38 %), kar razkriva, da je manjšina ljudi seznanjena z napadi socialnega inženiringa ter psihološkimi strategijami, ki so uporabljene pri takih napadih.

Velik delež uporabnikov, kar 40 %, je pozornih tudi na to, če sporočilo vsebuje hiperpovezavo, kar pomeni, da so seznanjeni s potencialnimi grožnjami zlonamernih povezav. Poleg pozornosti na hiperpovezavo je skoraj identičen delež ljudi pozoren na obliko hiperpovezave 39 %, kar pomeni, da ima ta del ljudi vsaj osnovno znanje prepoznave hiperpovezav. V primeru odprtja hiperpovezave je pa na obliko spletne strani pozornih samo 28 %, kar pomeni, da večina ljudi ni seznanjena z grožnjo, ki jo predstavljajo lažne spletne strani.

Najmanjši, a opazen delež vprašanih (13 %), je odgovorilo, da zaupa SMS-sporočilom. Čeprav to število ni velik delež vprašanih, nakazuje, da obstaja skupina ljudi, ki se morda na podlagi prejšnjih pozitivnih izkušenj zanaša na SMS-sporočila kot zanesljiv in varen način komunikacije. Teh 13 % je s popolnim zaupanjem v največji nevarnosti v primeru napada. Poudariti pa je treba, da čeprav je večina ljudi pozorna vsaj na obliko telefonske številke (61 %) in ime pošiljatelja (67 %), to ni niti približno zanesljiv način potrjevanja pristnosti, ker lahko napadalci s spoofingom identifikacije pošiljatelja z lahkoto preslepijo uporabnike e-bank.



Graf 7.9: Na katere dejavnike ste pozorni pri odločanju o pristnosti sporočila? (Možnih je več odgovorov.)

Odgovori na vprašanje, katere ukrepe uporabljajo, da svojo e-banko zaščitijo proti SMS-ribarjenju, kažejo, da je več kot polovica ljudi (58 %) izključni uporabnik svojih mobilnih naprav.

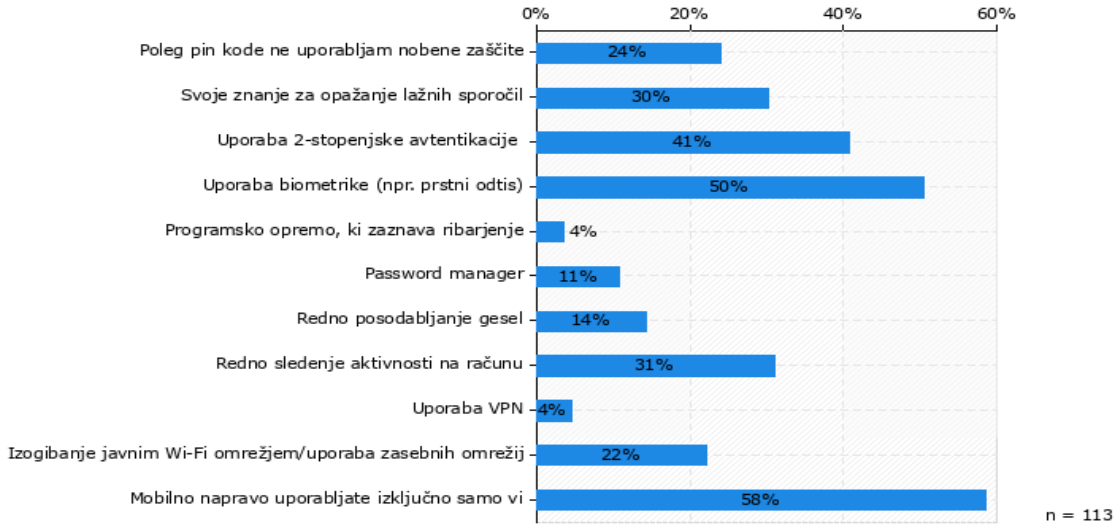
Nadaljuje se s tem, da je več kot 40 % anketirancev označilo, da uporabljajo dodatne varnostne ukrepe pri prijavi, kot so 2-stopenjska avtentikacija in uporaba biometrika, ki dosega 50 % anketirancev. Po teh rezultatih sklepamo, da se približno polovica ljudi zaveda, da dodatne varnostne plasti zmanjšujejo možnost, da postanejo žrtve kibernetskega kriminala.

Poleg tehničnih rešitev nekateri uporabljajo tudi druge metode. 30 % anketirancev je kot pomemben del zaščite navedlo svoje znanje prepoznavanja lažnih sporočil, kar pomeni, da so zelo samozavestni glede svojega znanja o preprečevanju napadov socialnega inženiringa.

Nekateri anketiranci (24 %) razkrivajo, da poleg PIN-kode ne uporabljajo nobene dodatne zaščite. Ta skupina se morda ne zaveda grožnje kibernetskega kriminala ali pa je prepričana, da se iz raznih razlogov njim to ne more zgoditi.

Obstaja pa tudi manjšinski del udeležencev, ki za zaščito uporablja programsko opremo. 4 % anketirancev uporablja programsko opremo, ki zaznava ribarjenje, 11 % anketirancev uporablja password managerje, 4 % pa VPN.

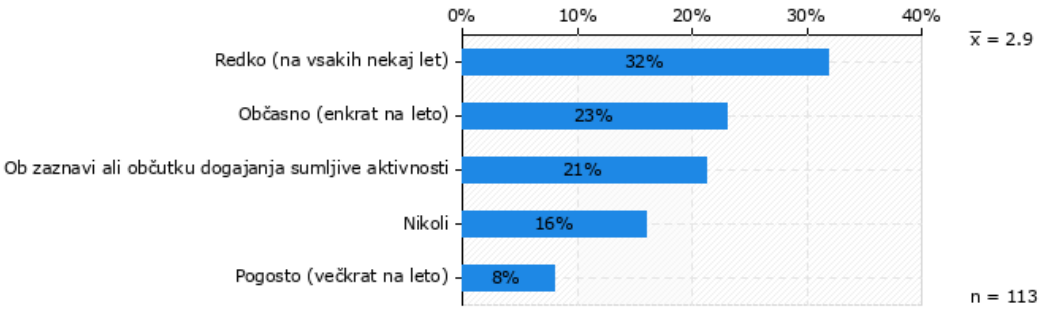
Drugi ukrepi, ki jih nekateri uporabljajo, so tudi izogibanje javnim Wi-Fi omrežjem (22 %), redno sledenje in preverjanje aktivnosti na bančnem računu (31 %) ter redno posodabljanje gesel (14 %).



Graf 7.10: Kakšne ukrepe uporabljate, da svojo e-banko zaščitite proti SMS-ribarjenju? (Možnih je več odgovorov.)

Vprašanje o pogostosti spreminjanja gesla za dostop do bančnega računa je prineslo naslednje ugotovitve: delež ljudi, ki nikoli ne spreminjajo gesla, predstavlja manjšina s 16 %, sledijo jim ljudje, ki geslo redko spreminjajo; teh je 31 %.

Približno 23 % udeležencev svoje geslo spreminja občasno, enkrat na leto, kar odraža zavedanje pozitivne strani redne menjave gesel. Najmanjši delež ljudi (8 %) geslo spreminja pogosto, večkrat na leto. 21 % gesla ne spreminja nikoli, razen ob zaznavi ali občutku dogajanja sumljive aktivnosti.



Graf 7.11: Kako pogosto spreminjate geslo za dostop do svojega računa?

8 RAZPRAVA

Namen zaključnega dela je bil ugotoviti, v kolikšni meri so uporabniki seznanjeni s smishingom v kontekstu mobilnega bančništva in posledicami, ki jih uspešno izveden napad pusti za sabo. V teoretičnem delu je bila najprej preučena teorija na temo mobilnih omrežij in tehnologije pošiljanja SMS-sporočil. Analizirane so bile strukture mobilnih omrežij ter načini komunikacije preko SMS-sporočil, kjer so bile izpostavljene ranljivosti, ki jih izkoriščajo napadalci pri izvajanju kibernetskih napadov. Nadaljevali smo raziskovanje mobilnega bančništva in razvoja, ki mu je sledil z vzponom interneta v poznih 90. letih prejšnjega stoletja, ko se je začelo mobilno bančništvo. Na začetku so bile storitve osnovne, a s pojavom pametnih telefonov leta 2007 je mobilno bančništvo doživelo hitro evolucijo. Čeprav so bile mobilne banke zaradi starejše tehnologije slabo dostopne in so imele slabše varnostne ukrepe, so se banke prilagodile in uvajale varnostne rešitve, vključno z večfaktorskim preverjanjem in biometriko. Z napredkom tehnologije so mobilne banke postale dostopne za vse ljudi, ki imajo v lasti pametno napravo.

Ker je uporabnik v velikem delu odgovoren za svojo varnost na internetu, smo raziskali tudi napade socialnega inženiringa. Napadalci se pri takem napadu osredotočajo na manipulacijo ljudi namesto uporabe tehničnih sredstev za vdor v sisteme. Pogostost teh napadov se iz leta v leto povečuje, še posebej zato, ker ljudje pogosto precenjujejo svojo zmožnost prepoznavanja tovrstnih napadov. Po predstavitvi grožnje napadov socialnega inženiringa smo se osredotočili na to, kaj je smishing, kjer smo ugotovili, da si smishing deli potek in psihološke strategije napada z ostalimi napadi socialnega inženiringa. Poleg psiholoških strategij smishing napadalci uporabljajo tudi SMS-spoofing, ki z manipulacijo identifikacije daje žrtvi lažni občutek zaupanja. Po predstavitvi samega smishing napada smo se osredotočili na smishing v kontekstu bančništva, kjer smo predstavili pogoste primere in posledice napadov, ki prizadenejo tako uporabnike e-bank kot pa tudi bančne institucije. Naslednja raziskana tema v sklopu smishinga v bančništvu so bile rešitve in predlogi, ki so primerni za preprečevanje smishinga v bančništvu. Obravnavane so bile

obstoječe prakse ter tehnološke rešitve, ki so v uporabi za povečanje varnosti uporabnika. Posebej smo poudarili, da ima uporabnik veliko odgovornost za svojo ozaveščenost in izobraževanje o nevarnostih smishinga. Predstavljeni so bili tudi za uporabnika pomembne varnostne navade in protokoli, ki jih lahko uporablja, kot so napredne avtentikacijske metode in izboljšani postopki preverjanje identitete.

Raziskovalni del naloge v obliki ankete je bil ustvarjen, da s pomočjo odgovorov anketirancev pridobimo odgovore na zastavljene hipoteze. Prvo hipotezo lahko potrdimo na podlagi vprašanja, ali so bili že kdaj tarča ene ali več spletnih groženj, kjer pri dveh možnih odgovorih presežemo polovico anketirancev, in sicer z nezaželenimi klici (74 %) in lažnimi spletnimi trgovinami (57 %). Preostale možnosti se vključno s smishingom gibljejo pri približno tretjini vprašanih z izjemo izsiljevanja, s katerim se je srečalo samo 5 % vprašanih.

Sledi druga hipoteza, pri kateri črpamo podatke iz treh anketnih vprašanj v naslednjem vrstnem redu:

- S katerimi vrstami prevar v kibernetskem prostoru ste seznanjeni?
- Ali veste, da je ribarjenje preko SMS-sporočil možno?
- Ste že kdaj bili tarča ene ali več naslednjih spletnih groženj?

Pri vprašanju, s katerimi vrstami prevar v kibernetskem prostoru so anketiranci seznanjeni, so anketiranci v 40 % izbrali odgovor smishing, kar je relativno blizu številki tistih, ki so pri vprašanju, ali so že kdaj bili tarča ene ali več spletnih groženj, označili smishing (29 %). Pri vprašanju, ali vejo, da je možno ribarjenje preko SMS-sporočil, je 56 % ljudi izbralo možnost, da so s to možnostjo seznanjeni, kar pomeni, da je razlika med odgovori prepoznave smishinga pri prvih dveh vprašanjih 16 %. Zaradi teh odgovorov lahko sklepamo, da se ozaveščenost grožnje smishinga giblje med 40 in 56 %.
Tretja hipoteza je kljub zabeleženemu porastu smishing primerov, kot kažejo podatki SI-CERT, in sicer iz 22 primerov v letu 2022 na 35 primerov do meseca julija leta 2023 ovržena, kar je pa še vedno veliko manjši delež v primerjavi s 362 primeri phishinga v bančništvu.

Četrta hipoteza je potrjena na podlagi dveh vprašanj v anketi. Prvo vprašanje, ki je pomembno za potrditev, je, kakšne posledice uspešne smishing prevare so po mnenju anketirancev najhujše, kjer je izmed štirih možnosti kar 63 % ljudi odgovorilo, da se jim izguba dostopa do bančnega računa zdi najhujši razplet uspešne smishing prevare. Ta 63-% delež kaže, da imajo napadalci večjo možnost manipulacije s čustvi pri pošiljanju smishing sporočil. Drugo vprašanje, ki nam pomaga pri potrditvi hipoteze, je, na katere dejavnike so anketiranci pozorni pri odločanju o pristnosti sporočila.« To vprašanje nam je koristno zaradi naslednjih pridobljenih podatkov: kar 13 % anketirancev je odgovorilo, da zaupa SMS-sporočilom, kar izredno olajša nalogo preslepitve in manipulacije. Naslednji odgovori kažejo na preveliko samozavest anketirancev (kar 56 % vprašanih se je v anketi ocenilo za samozavestne pri odkrivanju lažnih sporočil) in slabo seznanjenostjo (iz 1. hipoteze vemo, da se seznanjenost giblje med 40 in 56 %).

Izpostavljena odgovora sta tudi:

- pozornost na obliko telefonske številke (61 %),
- pozornost na ime pošiljatelja (67 %).

Te dve vrsti pregledovanja legitimnosti sporočil sta nezanesljivi, ker lahko napadalci brez večjih težav uporabljajo SMS-spoofinga, ki maskira identiteto napadalca in ustvari lažno zaupanje v SMS-sporočilo.

Manj kot polovica ljudi ima pri odkrivanju legitimnosti bolj napredne strategije, kot so:

- Pozornost na vsebino in ton sporočila (38 %), ki jim da možnost prepoznave poskusa čustvene manipulacije s strani napadalca.
- Pozornost na to, če sporočilo vsebuje hiperpovezavo (40 %), ki pomeni možno zavedanje obstoja zlonamernih hiperpovezav.
- Pozornost na obliko spletne strani, če sledijo hiperpovezavi, ki je zelo pomembno znanje za odkrivanje spoofinga, ki pa je v manjšini (samo 28 %).

9 ZAKLJUČEK

Živimo v času, kjer so mobilne naprave postale integriran del nas, to integracijo pa omogoča internet s svojimi 3 milijardami uporabnikov, ki generirajo milijardne dobičke. (Patterson & Nurse, 2022) Zaradi vsesplošne uporabe se morajo današnje organizacije sprijazniti, da se bodo soočale z neizogibnimi varnostnimi incidenti. Po podatkih World Economic Foruma kar 95 % incidentov kibernetske varnosti izvira iz človeških napak, kar razkriva potrebo po vlaganju v izobraževanje zaposlenih (World Economic Forum, 2022). Poleg večanja uporabnikov pametnih naprav se pa z digitalizacijo veča tudi uporaba mobilnega bančništva. Storitve e-bančništva so zaradi množične uporabe in ranljivosti uporabnikov zelo dobičkonosna tarča napadalcev. Najpogostejša metoda, s katero se je srečal že skoraj vsak uporabnik spleta, je phishing ali ribarjenje. Do leta 2018 so v Sloveniji phishing prevare predstavljale 9,21-% delež napadov, ki se je leta 2022 povzpel na kar 40% vseh napadov (SI-CERT, 2023b). Phishing se najpogosteje izvaja preko elektronske pošte ali lažnih spletnih strani. Kljub utemeljenim metodam phishinga se je začela pojavljati nova sorodna metoda, ki se imenuje smishing.

Prevara smishing dobi ime iz kombinacije besed phishing in SMS in je oblika kibernetske prevare, pri kateri napadalci z vzpostavljanjem neposrednega odnosa z žrtvijo poskušajo z uporabo metod socialnega inženiringa pridobiti zaupanje žrtve. Napadalci to storijo že v samem začetnem sporočilu, ki je namensko oblikovano tako, da v uporabniku vzbuja skrb. Če so napadalci s psihološko manipulacijo uspešni, je večja možnost, da bo uporabnik e-banke ukrepal nepremišljeno ter storil napako. Cilj napadalcev je pridobitev osebnih podatkov, poverilnic, finančnih podatkov ter vodenje žrtev na zlonamerne spletne strani. Leta 2022 je bilo pri nas zabeleženih 1432 incidentov phishinga, vključno s smishingom, ki kaže na strmo rast primerov. (SI-CERT, 2023b)

Smishing prevare so izvedljive samo, če je napadalec uspešen z uporabo strategij socialnega inženiringa. Zaradi tega bi morala biti ozaveščanje in izobraževanje ključnega pomena za znižanje primerov ne samo v kontekstu smishinga, temveč pri vseh napadih

socialnega inženiringa. Raziskava v obliki ankete je izpostavila, da večino uporabnikov (63 %) v primeru prevare najbolj skrbi izguba dostopa njihovega računa. Kljub dokaj visoki stopnji ozaveščenosti in 56-% samooceni visoke samozavesti pri razlikovanju med lažnimi in legitimnimi sporočili večina uporabnikov ni dovolj pozorna na bolj napredne in zanesljive načine prepoznavanja pristnosti SMS-sporočil. Zaradi tega je za učinkovito zaščito pred smishingom potrebna kombinacija ozaveščanja, izobraževanja, interaktivnih pristopov in tehnoloških rešitev, kot sta biometrika ter 2-stopenjska avtentikacija. Kot pri vseh kibernetskih napadih se pričakuje, da se bo grožnja smishinga prilagodila in razvijala na nove varnostne ukrepe, zato bo ključno, da se bodo tako uporabniki kot banke nenehno razvijali skupaj z novimi izzivi v kibernetskem okolju.

VIRI IN LITERATURA

Ahsenali Chaudry, J., Chaudry, S. in Rittenhouse, G. R. (2016). Phishing Attacks and Defenses. *International Journal of Security and Its Applications.* (str. 247-256). Research Gate. https://www.researchgate.net/publication/296916234_Phishing_Attacks_and_Defenses

Alsayed, A. O. in Bilgrami, A (2017*).* E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities*. International Journal of Emerging Technology and Advanced Engineering.* Research Gate. https://www.researchgate.net/profile/Anwar-Bilgrami/publication/315399380_E-Banking_Security_Internet_Hacking_Phishing_Attacks_Analysis_and_Prevention_of_Fraudulent_Activities/links/59f19d7c0f7e9beabfca5f17/E-Banking-Security-Internet-Hacking-Phishing-Attacks-Analysis-and-Prevention-of-Fraudulent-Activities.pdf

Ammouss, S. (2016). *Blockchain Technology: What is it good for?* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832751

Anshul, K., Chaudhary, M. in Kumar, N. (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology.* 2(11), (str. 15-19). ISSN. https://ejaet.com/PDF/2-11/EJAET-2-11-15-19.pdf

Din, A. (2022). *What Is Smishing? Definition, Types of Attacks, Protection Measures, and More.* Heimdalsecurity. https://heimdalsecurity.com/blog/what-is-smishing/

Babenko, D., Alemayehu, S. in Jay, V. (2023). *How do you balance convenience and security when using biometric authentication for mobile apps?* Linkedin. https://www.linkedin.com/advice/0/how-do-you-balance-convenience-security-when

Bank of America. (n.d.). *Five tips to help avoid smishing scams.* https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html

Bhalla, V. A. in Bhalla R. M. (2010). Generations of Mobile Wireless Technology: A Survey. *International Journal of Computer Applications.* Research gate. https://www.researchgate.net/publication/45601908_Generations_of_Mobile_Wireless_Technology_A_Survey

Carrington M. (2022). *Pros and Cons of Blockchain in Mobile App.* Velvetech. https://www.velvetech.com/blog/blockchain-in-mobile/

Center for internet security. (2023). *Vishing and Smishing: What You Need to Know.* https://www.cisecurity.org/insights/newsletter/vishing-and-smishing-what-you-need-to-know

Patterson, C. M. in Nurse, J. (2022). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security, 123.* Science Direct. https://www.sciencedirect.com/science/article/pii/S0167404823002195#bib0004

Cleveland, C. M. (2016). A Study on How Mobile Banking Has Affected the Banking Industry: Has Mobile Banking Improved Bank Performance? Industry: Has Mobile Banking Improved Bank Performance? *Honors Theses.* eGrove. https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1227incontext=hon_thesis

Panduru, D. (2021). *5 Smishing Examples Everyone Should Be Aware Of.* Attack simulator. https://attacksimulator.com/blog/5-smishing-examples-everyone-should-see/

Jansen, H. J. (2023). *What is Two-Factor Authentication and 2. How hackers are using social engineering techniques to bypass two-factor authentication.* Linkedin. https://www.linkedin.com/pulse/1-what-two-factor-authentication-2-how-hackers-using-social-jansen

Salahdine, F. in Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet.* MDPI. https://www.mdpi.com/1999-5903/11/4/89

Ghafir, I., Prenosil, V., Alhejailan, A. in Hammoudeh, M. (2016*).* Social Engineering Attack Strategies and Defence Approaches. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud).* IEEE. https://ieeexplore.ieee.org/document/7575856

Global Guardian. (n.d.). *TWO-FACTOR AUTHENTICATION SCAMS - WHAT TO KNOW.* https://www.globalguardian.com/global-digest/two-factor-authentication

Hong, J. (2012). The Current State of Phishing Attacks*. Communications of the ACM*. ACM. https://dl.acm.org/doi/abs/10.1145/2063176.2063197

IBM. (n.d.-a). *What is scareware?* https://www.ibm.com/topics/scareware

IBM. (n.d.-b). *What is smishing (SMS phishing)?* https://www.ibm.com/topics/smishing

Imperva. (n.d.). *Pretexting.* https://www.imperva.com/learn/application-security/pretexting/

Kakkar, A. (2016). Generations of Mobile Communication. *International Journal of Advanced Research in Computer Science and Software Engineering*. Research Gate. https://www.researchgate.net/profile/Ashna-Kakkar/publication/326462813_Generations_of_Mobile_Communication/links/5b4f2438a6fdcc8dae286f73/Generations-of-Mobile-Communication.pdf

Kaspersky. (n.d.). *What is Smishing and How to Defend Against it.* https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Kazuaki, M. (2023). *11 Best Practices for Future-proofing Mobile Banking Security Testing.* Headspin. https://www.headspin.io/blog/security-tips-for-banking-application-testing

Koyun, A. in Al Janabi, E. (2017). Social Engineering attacks*. Journal of Multidisciplinary Engineering Science and Technology.* ISSN. https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf

Krombholz, K., Hobel, H., Huber M. in Weippl E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 113–122.* Science Direct. https://www.sciencedirect.com/science/article/pii/S2214212614001343

Kvartalnyi, N. (2023). *Role of Biometric Authentication in Mobile Banking App Security: Benefits, Features, Risks.* Inoxoft. https://inoxoft.com/blog/role-of-biometric-authentication-in-mobile-banking-app-security-benefits-features-risks/

Lemzy, A. (2022). *How Do Scammers Get Your Cellphone Number and How to Protect Yourself.* Textmagic. https://www.textmagic.com/blog/how-do-scammers-get-your-cellphone-number/

Lenaerts-Bergmans, B. (2023). *WHAT IS SPEAR-PHISHING? DEFINITION WITH EXAMPLES.* Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/

MiPi. (2023). *Poleg phishinga, vse pogostejši tudi SMISHING.* https://www.mipi.si/teme/informacijska-pismenost/poleg-phishinga-vse-pogostejsi-tudi-smishing

Monteith, S., Bauer, M., Alda, M., Geddes J., Whybrow, P. in Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Psychiatry in the Digital Age.* Springer. https://link.springer.com/article/10.1007/s11920-021-01228-w

Mulliner, C., Borgaonkar, R., Stewin, P. in Seifert, J. P. (2014). SMS-based One-Time Passwords: Attacks and Defense. *Proceedings of the 10th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Research Gate. https://api-depositonce.tu-berlin.de/server/api/core/bitstreams/2b74f199-ddd7-464e-a65a-70d10fc5a305/content

National Cyber Security Centre. (2022). *Device Security Guidance.* https://www.ncsc.gov.uk/collection/device-security-guidance

Onfido. (2022). *The future of biometrics in banking.* https://onfido.com/blog/the-future-of-biometrics-in-banking/

PCMAG. (n.d.). *Cellular generations.* https://www.pcmag.com/encyclopedia/term/cellular-generations

Roy, P. K., Singh, Y. P. in Banarjee, S. (2020). Deep learning to filter SMS Spam. *Future Generation Computer Systems.* Science Direct. https://www.sciencedirect.com/science/article/abs/pii/S0167739X19306879

Rahmani, Z., Tahvildari, A., Honermand, H., Yousefi, H. in Daghighi, S. M. (2012). MOBILE BANKING AND ITS BENEFITS. *Oman Chapter of Arabian Journal of Business and Management Review.* Research Gate. https://www.researchgate.net/publication/269786060_Mobile_Banking_and_its_Benefits

Ray Allison, P. (2019). *Mitigating social engineering attacks with MFA*. Computerweekly.com. https://www.computerweekly.com/feature/Mitigating-engineering-attacks-with-multifactor-authentication

Robokiller. (n.d.-a). *Spam fighters, choose your weapons.* https://www.robokiller.com/best-robocall-blocker-app

Robokiller. (n.d.-b). *Spam texts 101: How to block spam texts.* https://www.robokiller.com/block-spam/spam-texts#Why-am-I-getting-spam-texts

Robokiller. (2022). *2022 Mid-Year Phone Scam Insights.* https://www.robokiller.com/the-robokiller-report

Rock, T. (2021). *Understanding the real danger of social engineering*. Invenioit.com. https://invenioit.com/security/danger-of-social-engineering/

Rupprecht, D., Dabrowski, A., Holz, T., Weippl, E. in Popper, C. (2018). On Security Research Towards Future Mobile Network Generations. *Cryptography and Security.* Arxiv. https://arxiv.org/pdf/1710.08932.pdf

Siddiqui, S. in Singh, T. (2016). Social Media its Impact with Positive and Negative Aspects. *International Journal of Computer Applications Technology and Research.* ISSN. https://ijcat.com/archives/volume5/issue2/ijcatr05021006.pdf

Rajeev, S. (n.d.). *Introduction to Mobile Biometric Authentication.* Loginradius. https://www.loginradius.com/blog/identity/what-is-mob-biometric-authentication/

Shweta, Main, K. in Evans, K. (n.d.). *What Is Smishing? Definition, Examples in Protection.* Forbes. https://www.forbes.com/advisor/business/what-is-smishing/

SI-CERT. (2022). *Poročilo o kibernetski varnosti za leto 2021*. https://www.cert.si/wp-content/uploads/2022/08/Porocilo-o-kibernetski-varnosti-2021_splet.pdf

SI-CERT. (2023a). *Kibernetska varnost leta 2022 v številkah*. https://www.cert.si/kibernetska-varnost-leta-2022-v-stevilkah/

SI-CERT. (2023b). *Poročilo o kibernetski varnosti za leto 2022.* https://www.cert.si/letna_porocila/porocilo-o-kibernetski-varnosti-za-leto-2022/

Apandi, S. H. Jamaludin, S. in Mohd Sidek, R. (2020). Types of anti-phishing solutions for phishing attack. *IOP Conference Series: Materials Science and Engineering.* IOP Science. https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/meta

SMS - Magic. (2020). *SMS 101 – Basics of SMS Technology.* https://www.sms-magic.com/docs/messaging-guides/knowledge-base/sms-101-basics-of-sms-technology/

Sorbet, A. (2022). *History of mobile banking – how it all started?* Finanteq. https://finanteq.com/blog/fintech-trends/history-of-mobile-banking-how-it-all-started/#mobile-banking-history

Taylor, S. A. in Vincent, J. (2005). A SMS history. *Mobile world: Past, present and future.* Research Gate. https://www.researchgate.net/publication/226340906_An_SMS_history

Jones, T. (2022, December 1). *The 12 Latest Types of Social Engineering Attacks (2023).* Aura. https://www.aura.com/learn/types-of-social-engineering-attacks

Wadhwani, S. (2021). *Facebook Data Leak: 533M Users Exposed on a Dark Web Forum.* Spiceworks. https://www.spiceworks.com/it-security/data-security/news/facebook-data-leak-533m-users-exposed-on-a-dark-web-forum/

Washo Hetro, A. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports.* Science Direct. https://www.sciencedirect.com/science/article/pii/S2451958821000749

Kaspersky. (n.d.-a). What is Spear Phishing? https://www.kaspersky.com/resource-center/definitions/spear-phishing

IBM. (n.d.-b). *What is spear phishing?* https://www.ibm.com/topics/spear-phishing

World Economic Forum. (2022). *Global Risks Report 2022.* https://www.weforum.org/reports/global-risks-report-2022/

Wenyuan, X., Hossen, A.M. in Steffen, S. (2014). You Can Call but You Can't Hide: Detecting Caller ID Spoofing Attacks. *Dependable Systems and Networks.* Research Gate. https://www.researchgate.net/publication/263847197_You_Can_Call_but_You_Can%27t_Hide_Detecting_Caller_ID_Spoofing_Attacks

Yeboah-Boateng, E. O. in Mateko Amanor, P. (2014). Phishing, SMiShing in Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences.* ISSN. https://e-tarjome.com/storage/btn_uploaded/2020-09-12/1599891065_11216-etarjome%20English.pdf

Zimperium. (n.d.). *Mobile Phishing Protection*. https://www.zimperium.com/mobile-phishing-protection/

PRILOGA A: ANKETA

Prosimo, če si vzamete nekaj minut in s klikom na gumb Naslednja stran začnete z izpolnjevanjem ankete.

Q1 – SPOL

- Moški.
- Ženski.

Q2 – STAROST

- 18−24.
- 25−35.
- 36−50.
- 50−60.
- 61+.

Q3 – NA KATERIH NAPRAVAH UPORABLJATE E-BANKO?

- Mobilne naprave.
- Računalnik.
- Oboje.

Q4 - S KATERIMI VRSTAMI PREVAR V KIBERNETSKEM PROSTORU STE SEZNANJENI?

- Phishing (ribarjenje).
- Zlonamerna koda (trojanski konj, virus, črv).
- Nigerijska prevara.
- Ljubezenske prevare.
- Goljufije z vnaprejšnjim plačilom.
- Smishing (SMS ribarjenje).
- Trojanski konj.
- Izsiljevalski virus.

- Črv.

Q5 – ALI VESTE, DA JE RIBARJENJE PREKO SMS-SPOROČIL MOŽNO?

- Da.
- Ne.

Q6 - NA LESTVICI OD 1 DO 5 OZNAČITE, KAKO SAMOZAVESTNO SE POČUTITE PRI RAZLIKOVANJU MED LAŽNIMI IN LEGITIMNIMI SMS-SPOROČILI, KJER 1 POMENI NAJMANJŠO STOPNJO SAMOZAVESTI IN 5 NAJVIŠJO STOPNJO SAMOZAVESTI.

- 1.
- 2.
- 3.
- 4.
- 5.

Q7 - STE ŽE PREJELI SMS-SPOROČILA, KI VAS POZIVAJO K ODPRTJU POVEZAVE ALI POSREDOVANJU ZASEBNIH INFORMACIJ?

- Da.
- Ne.

Q8 - STE ŽE KDAJ BILI TARČA ENE ALI VEČ NASLEDNJIH SPLETNIH GROŽENJ?

- Phishing sporočilo (ribarjenje).
- Phishing spletno mesto (ribarjenje).
- Smishing (SMS ribarjenje).
- Prevara z vnaprejšnjim plačilom stroškov.
- Nezaželeni klici.
- Lažne spletne trgovine.
- Izsiljevanje.

Q9 - KAKŠNE POSLEDICE USPEŠNE SMISHING PREVARE SO PO VAŠEM MNENJU NAJHUJŠE?

- Dostop do vaših socialnih omrežij.
- Dostop do vaše e-pošte.
- Kraja osebnih podatkov za namen kraje identitete.
- Dostop do vašega bančnega računa.

Q10 - KAKO MOČNO SE STRINJATE Z NASLEDNJO TRDITVIJO: "VARNOST UPORABNIKOV JE IZKLJUČNO ODGOVORNOST BANKE."

- Močno se strinjam.
- Se strinjam.
- Ne vem/Nisem prepričan.
- Ne strinjam se.
- Močno se ne strinjam.
- Nima izključne odgovornosti, odgovorni so banka in uporabniki.

Q11 - NA KATERE DEJAVNIKE STE POZORNI PRI ODLOČANJU O PRISTNOSTI SPOROČILA?

- Zaupam SMS-sporočilom.
- Na vsebino in ton sporočila.
- Na pravopisne napake.
- Na obliko telefonske številke.
- Na ime pošiljatelja.
- Na to, če sporočilo vsebuje hiperpovezavo.
- Na obliko hiperpovezave.
- Na obliko spletne strani, če sledite hiperpovezavi.

Q12 - KATERE UKREPE UPORABLJATE, DA SVOJO E-BANKO ZAŠČITITE PROTI SMS RIBARJENJU?

- Poleg PIN-kode ne uporabljam nobene zaščite.
- Svoje znanje za opažanje lažnih sporočil.
- Uporaba 2-stopenjske avtentikacije.

- Uporaba biometrike (npr. prstni odtis).
- Programsko opremo, ki zaznava ribarjenje.
- Password manager.
- Redno posodabljanje gesel.
- Redno sledenje aktivnosti na računu.
- Uporaba VPN.
- Izogibanje javnim Wi-Fi omrežjem/uporaba zasebnih omrežij.
- Mobilno napravo uporabljate izključno samo vi.

Q13 – KAKO POGOSTO SPREMINJATE GESLO ZA DOSTOP DO SVOJEGA RAČUNA?

- Nikoli.
- Redko (na vsakih nekaj let).
- Občasno (enkrat na leto).
- Pogosto (večkrat na leto).
- Ob zaznavi ali občutku dogajanja sumljive aktivnosti.

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE ZAKLJUČNEGA DELA

ZD-2

Univerza v Mariboru

Fakulteta za varnostne vede

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE ZAKLJUČNEGA DELA

Ime in priimek študent-a/-ke: Domen Zorko

Študijski program:
Informacijska varnost

Naslov zaključnega dela:
Uporaba smishinga v bančništvu

Mentor: izr. prof. dr. Blaž Markelj

Somentor: _____

Podpisan-i/-a študent/-ka Domen Zorko

- izjavljam, da je zaključno delo rezultat mojega samostojnega dela, ki sem ga izdelal/-a ob pomoči mentor-ja/-ice oz. somentor-ja/-ice;
- izjavljam, da sem pridobil/-a vsa potrebna soglasja za uporabo podatkov in avtorskih del v zaključnem delu in jih v zaključnem delu jasno in ustrezno označil/-a;
- na Univerzo v Mariboru neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve avtorskega dela v elektronski obliki, pravico reproduciranja ter pravico ponuditi zaključno delo javnosti na svetovnem spletu preko DKUM; sem seznanjen/-a, da bodo dela deponirana/objavljena v DKUM dostopna široki javnosti pod pogoji licence Creative Commons BY-NC-ND, kar vključuje tudi avtomatizirano indeksiranje preko spleta in obdelavo besedil za potrebe tekstovnega in podatkovnega rudarjenja in ekstrakcije znanja iz vsebin; uporabnikom se dovoli reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo;
- dovoljujem objavo svojih osebnih podatkov, ki so navedeni v zaključnem delu in tej izjavi, skupaj z objavo zaključnega dela;
- izjavljam, da je tiskana oblika zaključnega dela istovetna elektronski obliki zaključnega dela, ki sem jo oddal/-a za objavo v DKUM.

Uveljavljam permisivnejšo obliko licence Creative Commons:_____(navedite obliko)

CC BY NC ND

Kraj in datum: Škofja Loka, 14.12.2023

Podpis študent-a/-ke: