

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE
**ZAVEDANJE PORABNIKOV O VARNOSTI PRI SPLETNEM
NAKUPOVANJU**

Ljubljana, september 2024

PAVLINA PETERCA

IZJAVA O AVTORSTVU

Podpisana Pavlina Peterca, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Zavedanje porabnikov o varnosti pri spletnem nakupovanju, pripravljenega v sodelovanju s svetovalko izr. prof. dr. Matejo Kos Koklič

IZJAVLJAM

1. da sem predloženo delo pripravila samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;
7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.
11. da sem preverila verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne _____

Podpis študentke: _____

KAZALO

1	UVOD	1
2	SPLETNO NAKUPOVANJE	2
2.1	Zgodovina spletnega nakupovanja	2
2.2	Digitalna preobrazba	4
3	KIBERNETSKA VARNOST	6
3.1	Razumevanje spletnih groženj	6
3.2	Vrste varnostnih groženj	7
3.2.1	Zlonamerna programska oprema	7
3.2.2	Socialni inženiring	8
3.2.3	Ribarjenje.....	8
3.2.4	Lažne spletne trgovine	8
3.2.5	Človek v sredini	9
3.2.6	Drive-by prenosi	9
3.2.7	Napadi z ugibanjem gesel	9
3.3	Sprejemanje varnostnih ukrepov	9
3.4	Zavedanje porabnikov o kibernetiski nevarnosti.....	11
4	EMPIRIČNA RAZISKAVA ZAVEDANJA PORABNIKOV O VARNOSTI PRI SPLETNEM NAKUPOVANJU.....	12
4.1	Namen in cilji empirične raziskave	12
4.2	Metodologija	13
4.3	Analiza podatkov.....	15
4.3.1	Opis vzorca	15
4.3.2	Analiza vsebinskih vprašanj	15
4.3.3	Preverjanje hipotez	19
4.4	Interpretacija ugotovitev	21
5	SKLEP	22
	LITERATURA IN VIRI	23
	PRILOGE	27

KAZALO TABEL

Tabela 1: Pregled hipotez	21
---------------------------------	----

KAZALO PRILOG

Priloga 1: Anketni vprašalnik.....	1
Priloga 2: Analiza anketnih vprašanj in analiza hipotez	6

SEZNAM KRATIC

angl. – angleško

AI – (angl. artificial reality); umetna inteligenca

AR – (angl. augmented reality); obogatena resničnost

VR – (angl. virtual reality); navidezna resničnost

1 UVOD

V svetu, ki ga zaznamujeta hiter tempo življenja in vse najpornejši urnik, se je spletno nakupovanje izkazalo kot rešilna bilka za številne porabnike. Predvsem pandemija je pospešila premik k bolj digitalnemu svetu in trajno vplivala na porabnike, saj so bili zaradi vseh omejitev prisiljeni v uporabo spletnih alternativ, ki pa so hitro postale najpriročnejši način pridobivanja osnovnih dobrin, različne opreme ali oblačil. Ta premik v vedenju porabnikov ni bil le začasna prilagoditev, temveč je preoblikoval naš način razmišljanja o nakupovanju (Unctad, 2020).

V moderni dobi je tehnologija močno spremenila način življenja in vsakodnevne dejavnosti ljudi, vključno z nakupovanjem. Z leti so se ti procesi vse bolj razvijali, da bi porabnikom ponudili predvsem več priročnosti in udobja. Spletno nakupovanje je postalo zelo priljubljeno, saj porabnikom omogoča hiter dostop do izdelkov iz različnih virov in pri tem tudi dostop do geografsko oddaljenih lokacij (Aseri, 2021).

Medtem ko spletno nakupovanje ponuja številne prednosti za porabnike, ima tudi svojo slabo stran. Njegovo ranljivost predstavljajo predvsem tako imenovane spletne grožnje, ki lahko ogrozijo zasebnost in tudi varnost porabnika ter njegovih podatkov, kar pa lahko posledično vpliva na porabnikove odločitve in povečuje negotovost pri zaupanju spletnim trgovinam (Othman in drugi, 2017).

Nevarnosti spletnega nakupovanja večini porabnikom ostajajo neznane, kar povzroča napačno predstavo o spletnem nakupovanju. Med najpogostejšimi varnostnimi grožnjami za spletne porabnike so predvsem lažno predstavljanje (angl. phishing), ponarejene spletne trgovine, kraja podatkov, različna oglaševalska programska oprema in kraja identitete porabnika (Aseri, 2021).

Pri pisanju se želim osredotočiti predvsem na analizo dojemanja težav z varnostjo in zasebnostjo porabnikov pri spletnem nakupovanju, saj lahko to v današnjem digitalnem svetu predstavlja problematičen vidik e-trgovine, ki pa lahko posredno vpliva na nakupne odločitve porabnikov.

Ključni namen zaključne naloge je proučiti odnos porabnikov do spletnega nakupovanja in pridobiti vpogled v njihove nakupovalne navade ter izvedeti kako, dobro so obveščeni o različnih kibernetских grožnjah. Na podlagi pridobljenih podatkov želim podati priporočila, ki bodo prispevala k boljšemu razumevanju spletnega nakupovanja in boljši ozaveščenosti porabnikov o različnih tveganjih, ter priporočila za večjo varnost in zaupanje porabnikov v spletno okolje.

Moj glavni cilj teoretičnega dela zaključne strokovne naloge je, da pridobim globlje razumevanje izbrane tematike. Želim se poglobiti v obstoječe in trenutne raziskave, ki mi bodo v pomoč pri razumevanju ključnih vidikov obravnavane problematike. Teoretični del se začne z analizo literature o spletnem nakupovanju, kjer bom pisala o zaznavanju spletnega nakupovanja in vplivu digitalne preobrazbe. Naslednje poglavje bom namenila analizi kibernetске varnosti in kibernetским grožnjam, ki sledijo porabnikom pri uporabi spletnih trgovin. Teoretični del bom zaključila z napotki za boljše sprejemanje varnostnih ukrepov in analizo zavedanja porabnikov glede kibernetских nevarnosti.

Cilj empiričnega dela je izvedeti, kako velik delež slovenskih porabnikov je dobro informiranih in izobraženih o varnostnih vidikih spletnega nakupovanja. Zanima me predvsem, kateri dejavniki vplivajo na porabnike, tako da nakup raje opravijo prek spleta namesto, da odidejo v tradicionalno fizično trgovino. Svojo pozornost bom usmerila tudi v porabnikove odločitve. Tukaj me bo zanimalo predvsem, kako se porabniki pri spletnem nakupovanju zavarujejo proti spletnim zlorabam svojih osebnih podatkov.

Zaključna naloga je sestavljena iz dveh delov, teoretičnega in empiričnega dela. Pri pisanju teoretičnega dela zaključne naloge sem opravila obsežno analizo strokovnih člankov in relevantne teorije, ki je dostopna na spletu. Pri pregledovanju teorije sem se posebej osredotočila na področje spletnega nakupovanja in varnosti porabnikov pri spletnem nakupovanju.

V drugem delu je predstavljena empirična raziskava, kjer sem kot primarno orodje za zbiranje podatkov uporabila spletni anketni vprašalnik. Izbrani pristop mi je omogočal zbiranje svežih in prilagojenih podatkov, ki so neposredno v skladu z mojimi raziskovalnimi cilji. Zaključno nalogo sem sklenila s sklepnim poglavjem.

2 SPLETNO NAKUPOVANJE

2.1 Zgodovina spletnega nakupovanja

V svetu sodobnega poslovanja se je razširilo elektronsko poslovanje, splošno znano kot e-poslovanje. To je dejavnost, pri kateri blago, storitve in podatki nemoteno potujejo po elektronskih poteh ter pri tem spreminjajo način izvajanja transakcij in medsebojnega delovanja. V središču e-poslovanja je internet, ki je ključni medij za izmenjavo blaga, storitev in finančnih transakcij. Prav tako ima pomembno vlogo pri povezovanju porabnikov na družbenih medijih ali pri ustvarjanju spletnih trgovin. Vključuje izvajanje transakcij z uporabo elektronskih sredstev, kot so računalniki, pametni telefoni ali čitalniki kreditnih kartic (Patro in drugi, 2016).

Spletno nakupovanje je del e-trgovine, pri kateri transakcije potekajo elektronsko, spletno nakupovanje pa predstavlja središče dejavnosti, zaradi česar se imenuje tudi medmrežni

trg, na katerem porabnik izbere spletno mesto prodajalca, artikel in način plačila, ki vključuje kreditno ali debetno kartico ali plačilo po prevzemu pošiljke (Market Business News, brez datuma).

Pri nakupovanju veliko prednost predstavlja tudi dobra svetovna pokritost. To pomeni, da lahko porabnik, čeprav proizvajalec svoje blago prodaja v drugi državi, še vedno dobi želeni izdelek, saj mu za izvedbo učinkovitega nakupa izdelkov ali storitev ni treba živeti v isti državi. Ta globalna dostopnost odpravlja fizične omejitve in posameznikom omogoča dostop do obširne ponudbe izdelkov in storitev, ki presega lokalno ponudbo na njihovem območju (Market Business News, brez datuma).

Na splošno spletno nakupovanje v primerjavi s tradicionalnim nakupovanjem zmanjšuje ogljični odtis, saj zmanjša potrebo porabnikov po potovanju v fizične trgovine, s čimer se zmanjšajo emisije prevoza. Poleg tega zagotavlja tudi druge prednosti, kot sta priročnost in dostopnost. Na izboljšano nakupno izkušnjo pa vplivajo tudi spletne platforme z uporabo analize podatkov, na podlagi katere porabnikom ponujajo prilagojena priporočila. Porabniki cenijo možnost nakupovanja iz ugodja svojega doma, saj se lahko tako izognejo dolgim čakalnim vrstam, ki so še posebej pogoste v času praznikov (Market Business News, brez datuma).

Spletno nakupovanje je z leti doživelo velik razvoj in se uveljavilo kot pomemben dejavnik sodobnega poslovanja. Razvilo se je v brezmejen trend, ki je spremenil način, kako porabniki dostopajo do blaga in storitev (Computer Hope, 2023).

Trend elektronskega nakupovanja, ki ga je uvedel angleški izumitelj Michael Aldrich, predstavlja pomemben dosežek v razvoju trgovine. Leta 1979 je Aldrich predstavil prvo obliko e-trgovine, ki je olajšala spletno obdelavo transakcij med podjetji in strankami. Njegovo delo je postavilo temelje za razvoj spletnega nakupovanja, kot ga poznamo danes, oblikovalo prihodnost maloprodaje in spremenilo način interakcij podjetij s strankami (Computer Hope, 2023).

Leta 1994, po vzpostavitvi svetovnega spleta, so se pojavili sistemi spletnih transakcij, kot sta bančništvo in nakupovanje. Ustvarjen je bil tudi trend spletnega nakupovanja, ko sta NetMark in Internet Shopping Network porabnikom omogočila prve nakupovalne transakcije. Hitro sta jima sledila še Amazon in eBay, ko sta leto kasneje predstavila svoje spletne strani, s katerimi sta ponudila možnosti spletnega nakupovanja (Computer Hope, 2023).

Leta 2000 so se močno povečale povezave med prodajalcem in kupcem, ko je Google predstavil marketinško aplikacijo Adwords, ki je prodajalcem omogočala ciljanje oglasov na podlagi iskanih preferenc porabnikov. Paypal, ki je leta 2006 uvedel možnosti mobilnega plačevanja, je prav tako dodatno spremenil spletno nakupovanje z omogočanjem neposrednih nakupov prek mobilnih telefonov.

V sodobnem času je internet doživel silno preobrazbo in se spremenil v medmrežno središče, kjer lahko porabniki brskajo, izmenjujejo in kupujejo izdelke in storitve. Za prihodnost spletnega nakupovanja pa se zdi, da se vse bolj oddaljuje od tradicionalnega nakupovanja v trgovinah. Vse bolj bodo priljubljeni tehnološki izumi, kot so blokovne verige, kriptovalute, glasovno iskanje, obogatena (angl. augmented reality v nadaljevanju AR) in navidezna resničnost (angl. virtual reality v nadaljevanju VR) (Laliberte, 2023).

Napredek v tehnologiji utira pot prav tako impresivni prihodnosti spletnega nakupovanja, polni novih priložnosti, ki se iz dneva v dan nadgrajujejo. Primer tega sta tudi AR in VR, ki predstavljata napredno tehnologijo in porabnikom ponujata poglobljene izkušnje. Nove tehnologije bodo popolnoma preoblikovale vedenje porabnikov pri nakupovanju, na primer vizualizacija izdelkov pred odločitvijo o nakupu. Ta lahko porabnikom olajša nakup, saj jim omogoča, da vidijo, kako bi izdelek izgledal in ustrežal njihovem osebemu okolju, ter tako zmanjša število vračil kupljenih izdelkov (Faster Capital, 2024).

Tehnologija je zdaj bistvenega pomena v e-trgovini, saj podjetjem ponuja možnosti za rast in inovacije. Med ključnimi dosežki sodobne tehnologije je tudi umetna inteligenca (angl. artificial reality v nadaljevanju AI), ki je povsem spremenila način delovanja podjetij in interakcijo s porabniki. AI je na splošno za podjetja orodje, s katerim avtomatizirajo različne vidike svojega delovanja, izboljšajo sisteme priporočil in zagotovijo prilagojene izkušnje svojih strank ter s tem izboljšajo svojo uspešnost in konkurenčnost na trgu (Advent Biztech Solution, 2023).

Strojno učenje ima pomembno vlogo v e-trgovini, kjer se algoritmi uporabljajo za selekcijo ogromnih količin podatkov o strankah, različnih vzorcih in trendih. Prav tako lahko oceni učinkovitost različnih marketinških strategij in omogoča ugotavljanje, kateri izdelki so najbolj priljubljeni. Lahko tudi predvidi, pri katerih strankah je večja možnost, da bodo odšle drugam.

AI je ustvarila tako imenovane klepetalne robote (angl. chatbots), ki predstavljajo pomemben napredek pri storitvah za stranke in prodajnih strategijah. To so učinkovita orodja za opravljanje analiz o porabnikih, obenem pa pomagajo pri priporočanju izdelkov, pri čemer koristijo podatkovno bazo porabnikove zgodovine nakupov in brskanja (Advent Biztech Solution, 2023).

2.2 Digitalna preobrazba

V sodobnem digitaliziranem svetu je e-trgovina postala ključna sila, ki poenostavlja svetovno trgovino in s tem dosega obsežnejšo množico porabnikov. Ta razcvet e-trgovine je spremenil tradicionalne poslovne modele in spodbudil rast različnih poslovnih sektorjev.

Nadaljnje inovacije bodo nastajale tudi zaradi vse večje povezljivosti ljudi in predmetov, bolj znane kot internet stvari (angl. Internet of Things), podatkovne analitike in mobilnih plačil. Prav tako pa e-trgovina podjetjem in drugim porabnikom omogoča dragocene vpoglede v vedenje porabnikov ter vse večje vključevanje porabnikov v družbene medije, kar je tudi vzrok za bolj poglobljene odnose med podjetji in porabniki (Fenech in drugi, 2015).

Zaradi naraščajočega obsega podatkov, ustvarjenih v digitalnem okolju, nastajajo pomembni varnostni izzivi, zaradi česar so nujno potrebni močni varnostni ukrepi. Čeprav novodobne tehnologije, kot so virtualne valute in internet stvari, prinašajo velika varnostna tveganja, lahko v tem primeru izvajanje strategij, kot so digitalne identitete, pomaga zmanjšati ta tveganja (Fenech in drugi, 2015).

S prihodom interneta se je tako ustvarilo novo digitalno okolje, polno informacij in povezav, ki zajemajo ves svet. Ustvarilo se je med seboj povezano okolje brez meja med državami. Internet se je med porabniki hitro uveljavil kot priljubljen dejavnik sodobnega razvoja, ki z enim samim klikom odpira vrata do brezmejne možnosti. Porabniki prav tako niso več vezani na časovne omejitve, saj lahko po e-trgovinah brskajo v prostem času ali na svojem delovnem mestu ne glede na uro ter se tako izognejo čakalnim vrstam in najdejo najboljše ponudbe med različnimi ponudniki. Spletno nakupovanje je postalo priljubljeno tudi zaradi udobja, ki ga ponuja porabniku, ko ta dostopa do zelenih izdelkov ali storitev. Spletni ponudniki so v svoje platforme vključili tudi različne plačilne rešitve, da bi povečali udobje za stranke (Ingaldi in Brožova, 2020).

Način nakupovanja, povezovanja in interakcije s svetom okoli nas se je v preteklih letih zaradi občutnega napredka v spletnem okolju za vedno spremenil. Njegova hitra širitev je nedvomno spremenila način našega poslovanja in interakcije na spletu, vendar pa s to hitro rastjo udobja in priložnosti, ki jih ponuja digitalno napredovanje, prihaja vrsta izzivov, zlasti v zvezi z zbiranjem in uporabo porabnikovih podatkov s strani spletnih trgovcev (Aseri, 2021).

Pomembna skrb se nanaša na ogromno količino podatkov, ki jih spletni trgovci zbirajo od porabnikov med spletnimi interakcijami, saj se z vsakim klikom ali nakupom zbira zakladnica informacij, s katerimi podjetja pridobijo podatke o vedenju porabnikov, njihovih preferencah in demografske podatke. Prav tako imajo lahko dostop tudi do podatkov o dejavnostih na družbenih omrežjih in zgodovini brskanja. Ti podatki imajo izjemno vrednost pri izboljševanju trženjskih pristopov in pripomorejo k izboljšanju interakcij s strankami, vendar pa med porabniki povzročajo veliko skrbi glede zasebnosti in varnosti osebnih podatkov. Združevanje podatkov na spletu predstavlja veliko tveganje, saj lahko porabnik svoje občutljive informacije posledično da na voljo napačnim posameznikom ali organizacijam, zaradi česar so porabniki ranljivi za različne grožnje, kot so lažno pretvarjanje, internetne goljufije, spletne prevare in zlonamerni spletni naslovi (Aseri, 2021).

Vse večje vključevanje interneta v naša življenja je iz dneva v dan vse vidnejše. Internet se zdaj uporablja kot orodje za izobraževalne raziskave, socialno interakcijo in dostop do svetovnih informacij. Zaradi njegove vse večje dostopnosti je še zlasti pomembno zagotoviti varnost na spletu. Za porabnike pa je predvsem pomembno, da ostajajo pozorni pri prepoznavanju morebitnih nevarnosti in si tako zagotovijo varno uporabo interneta (Hunwick Primary, brez datuma).

3 KIBERNETSKA VARNOST

3.1 Razumevanje spletnih groženj

Zdaj digitalno okolje poznamo kot okolje, v katerem se ustvarja neskončno medsebojnih povezav in informacij, ki prosto potujejo iz enega omrežja v drugo. Pojavi se bistven pojem, imenovan kibernetika varnost.

Temeljna značilnost kibernetike varnosti vključuje varovanje sistemov, omrežij in podatkov, shranjenih v digitalnem okolju, pri tem pa zajema vrsto tehnoloških ukrepov, namenjenih urejanju dostopa in zaščiti pred nepooblaščenimi vdori, zagotavljanju celovitosti in zaupnosti informacij (Fumudoh in Viswanathan, 2014).

Na področju varnosti pri uporabi e-trgovine se lahko grožnje pokažejo bodisi kot naključne nesreče bodisi kot zlonamerna dejanja. Za zmanjšanje ranljivosti in dobro zaščito spletnih mest je potrebno izvajanje nadzornih ukrepov skupaj z vsemi potrebnimi postopki (Hiral, 2020).

Zlonamerne grožnje sistemom e-trgovine vključujejo različne oblike vdorov hekerjev, ki želijo manipulirati ali dostopati do občutljivih informacij. Vdori lahko vključujejo nepooblaščen dostop do zasebnih podatkov, lažno pretvarjanje, zlonamerno programsko opremo in socialni inženiring. Poleg tega se zlonamerni subjekti lahko lažno predstavljajo kot zakoniti porabniki ali ustvarijo zavajajoča spletna mesta, ki so videti pristna. Druge možne zlonamerne taktike vključujejo tudi razširjanje e-poštnih sporočil, ki lahko vsebujejo skrite komponente, namenjene ogrožanju sistemov, kar lahko posledično vodi do nepooblaščenega pridobivanja osebnih podatkov. Vse težje je prepoznati prisotnost nepooblaščenih oseb in ugotoviti pravi pomen kibernetike grožnje ter njenih skritih komponent, saj delujejo vedno bolj prikrito in zavajajoče (Hiral, 2020).

Porabniki se pri uporabi spletnih brskalnikov kot glavnih strežnikov za izvajanje transakcij soočajo z dodatnimi skrbmi glede varnosti in zasebnosti. Obisk neznanih ali dvomljivih povezav bistveno poveča možnost tveganja. Pri tem ima veliko vlogo tudi nalaganje ali prenašanje datotek, saj se lahko zelo hitro zgodi, da porabniki nehote vnesejo svoje podatke v lažno varne sisteme, kar pa lahko posledično privede do tega, da bodo informacije izpostavljene nepooblaščenemu subjektu (Hiral, 2020).

Vse bolj prevladujoče orodje v spletni tehnologiji, piškotki (angl. cookies), prav tako vzbujajo pomisleke glede zasebnosti. Te majhne enote podatkov, ki se izmenjujejo med strežniki in odjemalci v spletnem okolju, se lahko uporabljajo za sledenje vzorcev brskanja porabnikov, vendar brez njihovega izrecnega soglasja. Vzorci brskanja se nato kažejo v predstavitvi prilagojenih povezav in oglasov (Hiral, 2020).

3.2 Vrste varnostnih groženj

S široko razširjenostjo spletnega nakupovanja in udobja nakupovanja le z enim klikom se je razširjenost groženj kibernetiki varnosti močno povečala. Ker porabniki za nakup izdelkov ali storitev, od gospodinjskih aparatov in vse do modnih dodatkov, vse pogostejše uporabljajo računalnike in pametne telefone, je digitalni trg postal glavna tarča kibernetičnih kriminalcev (Ecpi-edu, brez datuma).

Računalniški sistemi so tarča kibernetičnih napadov. Glavni namen kibernetičnih napadov je ukrasti, spremeniti ali izbrisati osebne podatke porabnikov. Storilci so lahko bodisi posamezniki bodisi organizirane skupine, ki želijo pridobiti nepooblaščen dostop do podatkovnih sistemov za različne zlonamerne namene. Pri svojem delu napadalci uporabljajo različne tehnike ali kode, ki posledično povzročijo neželene učinke na programski opremi (Biju in drugi, 2019).

Napredek tehnologije sicer poenostavlja življenje, vendar hkrati predstavlja grožnjo varnosti. Med primeri udobja na spletu je shranjevanje občutljivih podatkov, kot so gesla in podatki o kreditnih karticah, v osebnih računalnikih ali mobilnih telefonih. Takšne ranljivosti za dostop se lahko hitro izkoristijo za različne oblike kibernetičnih napadov (Biju in drugi, 2019). V nadaljevanju natančneje predstavljam najpogostejše primere varnostnih spletnih groženj in najboljše prakse za obrambo pred njimi.

3.2.1 Zlonamerna programska oprema

Zlonamerna programska oprema (angl. malware) se je izkazala za eno od najresnejših zunanjih groženj računalniškim sistemom. Nanaša se na kateri koli program ali kodo, zasnovano z zlonamernim namenom nezakonitega vdiranja v računalniške sisteme ali omrežja. Ko je škodljiva programska oprema nameščena, lahko ogrozi zaupnost podatkov s krajo občutljivih informacij, kot so osebni podatki, gesla ali finančni podatki. Prav tako lahko ogrozi celovitost podatkov s spreminjanjem ali poškodovanjem datotek, zaradi česar lahko postanejo neuporabne. Na splošno prisotnost zlonamerne programske opreme predstavlja veliko tveganje za varnost in funkcionalnost digitalnih sistemov (Mass.gov, brez datuma).

Nekatere pogoste vrste zlonamerne programske opreme so (Coursera, 2023):

- trojanski konj (angl. Trojans),

- oglaševalska programska oprema (angl. adware),
- vohunska programska oprema (angl. spyware),
- izsiljevalska programska oprema (angl. ransomware),
- virus,
- črv (angl. worm).

3.2.2 Socialni inženiring

Socialni inženiring (angl. social engineering), tukaj napadalci uporabljajo tehniko manipulacije in različne psihološke tehnike z namenom, da škodujejo posameznikom in pri tem pridobijo njihove osebne podatke, ki jih po navadi izkoristijo za finančne zlorabe. Tehnike, s katerimi nas kibernetiski napadalci poskušajo prepričati v takšna dejanja, so običajno zelo domiselne in žal pogosto uspešne. V sedanji digitalni dobi, v kateri prevladuje nenehen pretok informacij, to še posebej koristi posameznikom, ki želijo s socialnim inženiringom izoristiti zaupanje ljudi. Primer tega je predvsem Facebook, ki je znan kot platforma, na kateri porabniki množično delijo svoje osebne podatke, kar povečuje tveganja, povezana s taktikami socialnega inženiringa. Eden od pogostih primerov socialnega inženiringa je lažno predstavljanje (Ip.rs, 2009).

3.2.3 Ribarjenje

Ribarjenje (angl. phishing) ali z drugo besedo napad z lažnim predstavljanjem vključuje predvsem pošiljanje zavajajočih e-poštnih sporočil, v katere napadalec vstavi povezave ali različne priloge iz datoteke, ki jih je mogoče klikniti. V veliko primerih so te povezave videti povsem neškodljive in zakonite, saj so zasnovane tako, da je njihov resnični namen dobro prikrit. Porabnik lahko tako namesti zlonamerno programsko opremo na svojo osebno napravo in tako ogrozi svojo kibernetisko varnost, saj se ob kliku nanjo sprožijo uničujoča dejanja (Biju in drugi, 2019).

3.2.4 Lažne spletne trgovine

Med vrste lažnega predstavljanja spadajo tudi lažne trgovine. Porast lažnih spletnih trgovin je v zadnjih letih privedel do precejšnjega povečanja pritožb porabnikov, saj te vse pogosteje zavajajo spletne porabnike v nakupe neobstoječih ali ponarejenih izdelkov in želijo, da bi porabniki izdali svoje občutljive informacije. Lažna spletna mesta so predvsem uspešna z ustvarjanjem lažnih oglasov na družbenih medijih in drugih platformah, predvsem v obdobjih povečanega spletnega nakupovanja, kot so različna praznična obdobja (Mayford, 2023).

3.2.5 Človek v sredini

»Človek v sredini« (angl. man in the middle (MitM)) predstavlja resno grožnjo varnosti omrežja, pri kateri se napadalec postavi med dva porabnika, ki komunicirata prek spletnega omrežja. Brez njune vednosti jima lahko prisluškuje pri pogovoru in manipulira s pridobljenimi informacijami, ki se izmenjujejo v pogovoru. Ta dejavnost ogroža zaupnost in celovitost prenesenih podatkov, saj lahko napadalec prestreže občutljive podatke in tako spremeni komunikacijo v svojo korist. To se lahko zgodi v različnih komunikacijskih storitvah, vključno z GSM, Wi-Fi in Bluetooth.

Kot primer lahko omenimo dinamično prisluškovanje (angl. dynamic eavesdropping). Tukaj se napadalec prikrade med dve osebi, ki klepetata na spletu, in opazuje njuna sporočila, ki jih prav tako lahko tudi spreminja z namenom, da bi manipuliral z njunim zaupanjem v sogovornika (Javeed in drugi, 2020).

3.2.6 Drive-by prenosi

Drive-by prenosi (drive-by download attack) se običajno zgodijo, ko porabnik nevede klikne na škodljivo povezavo, prenos pa se lahko zgodi tudi, če porabnik ne klikne nikamor, saj je za prenos dovolj, da porabnik zgolj obišče zlonamerno spletno stran. Kibernetski napadalci pogosto izkoriščajo zakonita spletna mesta tako, da njihove spletne strani okužijo z zlonamernim programom. Ob kliku na takšno povezavo se na porabnikovo napravo prenese škodljiva vsebina, ki lahko povzroči različne nezaželeni namestitve zlonamerne programske opreme, opravi krajo podatkov ali pa to izkoristi za nepooblaščen nadzor nad porabnikovo napravo (Biju in drugi, 2019).

3.2.7 Napadi z ugibanjem gesel

Ti napadi so običajna metoda kibernetskih napadalcev za pridobitev nepooblaščenega dostopa do uporabniških računov porabnikov na spletu. Lahko so ročni ali avtomatizirani. Pri ročnih napadih se napadalec zanaša na svoje predhodno znanje o ciljnem porabniku, da bi lažje ugotovil njegovo geslo. Primer takšnega gesla je lahko otrokovo ime ali datum rojstva. Po drugi strani pa avtomatizirani napadi uporabljajo različna programska orodja, zaradi česar imajo večjo verjetnost uspeha (Hiral, 2020).

3.3 Sprejemanje varnostnih ukrepov

Za posameznike je pomembno, da pri pregledovanju spletnih strani ali trgovin ostanejo pozorni na pomisleke glede varnosti in zasebnosti. Prav tako je pomembno, da zaradi različnih varnostnih groženj, ki so bile že predhodno omenjene, zasebnost ostaja najpomembnejša skrb. Za zmanjšanje tveganj bi morali posamezniki sprejemati

proaktivne ukrepe. Sledi nekaj nasvetov za izboljšanje varnosti in zasebnosti (Ontario, 2013).

Pri spletnem nakupovanju je ključnega pomena, da damo prednost zaupanja vrednim spletnim stranem in se ne zanašamo zgolj na rezultate spletnih iskalnikov. Nakupovanje na spletnih mestih, kot so priljubljeni trgovci na drobno ali priznane spletne trgovine, pomaga zmanjšati možnosti, da bi naleteli na različne spletne goljufije, saj imajo ta spletna mesta po navadi varnostne funkcije, ki omogočajo zaščito osebnih in finančnih podatkov pred zunanjimi nevarnostmi (Patro in drugi, 2016).

Zagotavljanje, da ima spletno mesto nameščeno šifriranje SSL (Secure Sockets Layer), je ključnega pomena pri spletnih nakupih, zlasti pri zavarovanju občutljivih podatkov, kot so podatki o kreditni kartici. Spletna mesta, ki se začnejo s »HTTPS://« namesto samo s »HTTP://«, so primerno zavarovana s tovrstnim šifriranjem. Črka »S« v »HTTPS« pomeni, da je spletno mesto varno za uporabo. Za posameznike je ključnega pomena, da podatke vnašajo le na preverjenih in zaupanja vrednih spletnih straneh in da se, če niso prepričani o svoji varnosti, izogibajo razkrivanju podatkov o svoji kreditni kartici (Patro in drugi, 2016).

Pri sprejemanju varnostnih ukrepov je izjemno pomembno tudi zavedanje posameznikov, da verificirane spletne strani od strank ne bi nikoli zahtevale njihovih občutljivih podatkov. Kopičenje osebnih podatkov poveča tveganje kraje identitete, kar kriminalcem omogoča zlorabo identitete žrtev. Dajanje prednosti zaščiti osebnih podatkov in previdnosti na spletu zmanjšujeta tveganje kraje identitete. Previdnost je ključnega pomena za varno spletno nakupovanje (Patro in drugi, 2016).

Pri posameznikih, ki nemalokrat kupujejo prek spleta, predvsem s transakcijami na tujih spletnih mestih, je pomembno redno pregledovanje elektronskih izpiskov za morebitne nepooblaščne bremenitve kartic, tekočih računov ali PayPala. Če pri tem ugotovijo neskladja, morajo o tem najprej obvestiti svojo banko (Patro in drugi, 2016).

Za ohranjanje varnosti sta prav tako pomembna redno spreminjanje gesel in uporaba različnih gesel za različna spletna omrežja. Uporaba močnih in edinstvenih gesel ter dvojna potrditev gesla bosta omogočili večjo varnost, prav tako pa bo tako tudi zmanjšano tveganje za možnosti vdorov v osebne račune (Patro in drugi, 2016).

Prav tako so pomembni še številni vidiki, pri katerih je ključno, da jih porabniki opazijo na spletnih mestih, še preden zaključijo svoje nakupe, in si tako zagotovijo varne transakcije. Pri spletnem nakupovanju je za porabnike pomembno, da pregledajo izjavo o zasebnosti, ki je ključni sestavni del pri preglednosti podjetja glede ravnanja z osebnimi podatki strank ter vključuje izjave o postopkih, ki jih podjetje uporablja pri zbiranju, uporabi in varovanju osebnih podatkov. Odsotnost jasne izjave o zasebnosti je lahko pomemben negativen kazalnik za porabnike pri ocenjevanju zanesljivosti spletnega mesta (Kaspersky, brez datuma).

Prav tako je zelo pomembno, da so porabniki previdni pri spletnih ponudbah, ki se zdijo izjemno privlačne, zlasti na spletnih mestih, ki ponujajo dizajnerska oblačila, nakit ali elektroniko po bistveno nižjih cenah. V številnih primerih lahko spletna mesta, ki oglašujejo močno znižane izdelke, prodajajo ponarejene izdelke ali replike izdelkov, zaradi česar porabniki nehote kupijo slabše ali ponarejeno blago (Kaspersky, brez datuma).

Običajno zakonita podjetja informacije o svojih kontaktnih številkah in fizičnem naslovu vidno prikažejo na svojem spletnem mestu. Tako lahko porabnik, če se pojavijo dvomi o pristnosti spletne trgovine, uporabi preprosto metodo preverjanja s tem, da preveri podatke podjetja v spletnem iskalniku. Nasprotno pa lahko goljufivi prodajalci izpustijo ali ponaredijo podatke o naslovu ali telefonski številki, zato je za porabnikovo varnost pomembno, da takšne spletne strani pred nakupom tudi osebno preveri (Kaspersky, brez datuma).

Porabniki bi morali biti pozorni tudi na črkovalne in slovnične napake pri krmarjenju po spletnih nakupovalnih straneh. Pri uglednih spletnih straneh se nič kaj pogosto ne zgodi, da bi imele slabo kakovost besedila ali slik na svojih straneh (Kaspersky, brez datuma).

Veliko pomoč pri preverjanju legitimnosti spletne strani in uporabnosti izdelka pa so spletne ocene. Čeprav je pomembno vedeti, da so lahko nekatere ocene izmišljene, lahko proučevanje skupnega vzorca povratnih informacij drugih strank vseeno zagotovi dragocene vpogleds. Ocene na zaupanja vrednih spletnih straneh so lahko zanesljiv vir informacij, ki kupcem omogočajo razumevanje pristnosti prodajalca in povratne ocene prejšnjih strank. Zato je tudi za porabnike pomembno, da pred nakupom dobro preverijo ocene in tako zmanjšajo tveganje pri nakupu goljufivih izdelkov pri nezanesljivih prodajalcih (Kaspersky, brez datuma).

3.4 Zavedanje porabnikov o kibernetiski nevarnosti

Leta 2015 je Deloitte izvedel anketo, ki je bila osredotočena na kibernetiski kriminal in varnost porabnikov. Njihova raziskava kaže na naraščajočo zaskrbljenost porabnikov glede varnosti osebnih podatkov pri interakciji s podjetji na spletu. Porabniki za svojo zaščito vse pogosteje sprejemajo proaktivne ukrepe, to je z izvajanjem varnostnih pregledov, in ostajajo previdni glede deljenja svojih podatkov na spletu, saj še vedno ostaja nejasnost glede podrobnosti o tem, kateri podatki se dejansko zbirajo in kdo točno jih zbira. Prav tako jih veliko trdi, da bi zmanjšali svoje spletne interakcije, če bi bili tako bolje zaščiteni (Fenech in drugi, 2015).

Vse večjo zaskrbljenost povzročajo vse številčnejši primeri kibernetiskih napadov, ki vodijo v goljufije in kraje. Zaupanje porabnikov v varnost svojih osebnih podatkov upada, pri čemer jih (73 %) trdi, da bi ponovno premislili o sodelovanju s podjetjem, če to ne bi dovolj prispevalo k varovanju njihovih podatkov, prav tako pa bi vsak tretji porabnik

prenehal sodelovati s podjetjem, za katero meni, da je odgovorno za kršitev varnosti. Med podjetji veljajo za najbolj zaskrbljujoča glede varnosti predvsem podjetja, ki vodijo družbene medije ali spletne trgovine (Fenech in drugi, 2015).

V današnjem digitalnem okolju, kjer je zaskrbljenost glede zasebnosti in varnosti podatkov iz dneva v dan večja, imajo podjetja idealno priložnost, da se izkažejo tako, da dajo prednost varovanju informacij svojih porabnikov. Tako bi pomirili strahove porabnikov ter obenem zadovoljili njihova vse večja pričakovanja glede orodij in ukrepov za zaščito osebnih podatkov (Fenech in drugi, 2015). Prav tako je raziskava pokazala, da bi podjetjem koristila večja odprtost pri izvajanju zbiranja podatkov, saj bi porabniki tako lahko bolje razumeli, kateri podatki se zbirajo in za katere namene.

Porabniki vse bolj dajejo prednost podjetjem, ki cenijo njihovo zasebnost in jim zagotavljajo nadzor nad uporabo njihovih osebnih podatkov. Z izvajanjem tovrstnih praks bi tako podjetja pridobila in ohranila zaupanje porabnikov (Fenech in drugi, 2015).

4 EMPIRIČNA RAZISKAVA ZAVEDANJA PORABNIKOV O VARNOSTI PRI SPLETNEM NAKUPOVANJU

4.1 Namen in cilji empirične raziskave

Namen empiričnega dela zaključne strokovne naloge je na podlagi sekundarne literature proučiti zavedanje porabnikov glede spletnih tveganj in groženj pri spletnem nakupovanju ter oceniti njihovo ozaveščenost za sprejemanje varnostnih ukrepov pri spletnem nakupovanju. Cilji empiričnega dela so sestavljeni iz treh delov:

- proučiti ozaveščenost porabnikov o spletnih nevarnostih pri spletnem nakupovanju,
- raziskati, kateri dejavniki vplivajo na porabnikovo odločitev, da opravi nakup prek spleta namesto v fizični trgovini,
- se poglobiti v vprašanje, katere varnostne ukrepe sprejemajo porabniki za zaščito svojih osebnih in finančnih podatkov pri spletnem nakupovanju.

Rezultati empiričnega dela raziskave bodo prispevali k boljšemu razumevanju porabnikov o varnosti pri spletnem nakupovanju. Utemeljitev za raziskovalne hipoteze so naslednje:

Spletna raziskava podjetja KPMG iz leta 2016 (Mlada, 2021) je pokazala, da (55 %) porabnikov z vsega sveta ne bo kupilo izdelka ali storitve prek spleta zaradi pomislekov glede zasebnosti. Zasebnost podatkov je za porabnike v zadnjih letih vse pomembnejša. Predpostavljam, da se je odstotek porabnikov, ki so zaskrbljeni glede zasebnosti, do leta 2024 še povečal. Predpostavljam prvo hipotezo:

Hipoteza 1: Porabniki so nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke.

Raziskava SURS iz leta 2022 (Mlakar, 2022) predstavlja statistične podatke o glavnih razlogih za spletno nakupovanje pri slovenskih porabnikih. Na vprašanje, kateri je vaš glavni razlog, da opravite nakup prek spleta namesto v živo, je (82 %) porabnikov navedlo, da je najpomembnejši razlog prihranek časa. Zaradi sprememb v življenjskem slogu in iskanju po bližnjicah predpostavljam drugo hipotezo:

Hipoteza 2: Glavni razlog za spletni nakup pri porabnikih je časovni prihranek.

Iz raziskave o ukrepih, ki jih porabniki sprejemajo za zaščito svoje zasebnosti, ki jo je izvedel Cisco leta 2023, je bilo razvidno, da (42 %) porabnikov, starih od 18 do 24 let, preišljeno ukrepa, da bi zaščitili svojo varnost. Vendar pa preišljeno ukrepa le (6 %) porabnikov, starih 75 let in več. Menim, da so porabniki večinskega mnenja, da splet postaja vse nevarnejši za osebne in finančne podatke ter da je pomembno, da sprejemamo čim več proaktivnih ukrepov, predvsem preden opravimo spletni nakup, zato predpostavljam tretjo hipotezo:

Hipoteza 3: Večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov.

Na podlagi raziskave SURS o spletnem nakupovanju iz leta 2023 (Mlakar, 2023) je bilo ugotovljeno, da porabniki v obdobju treh mesecev najpogosteje opravijo en ali dva nakupa prek spletnih omrežij. Na podlagi te raziskave sklepam, da večina porabnikov prek spleta opravi nakup več kot enkrat mesečno. Zato predpostavljam četrto hipotezo:

Hipoteza 4: Večina porabnikov opravi nakup prek spleta več kot enkrat mesečno.

Na podlagi podatkov SURS iz leta 2023 (Mlakar, 2023) lahko vidimo, da dve tretjini porabnikov pri spletnem nakupu uporabi debetno ali kreditno kartico. Zaradi vse večje digitaliziranosti nakupovanja so kartična plačila ključna komponenta elektronskih transakcij, ki porabnikom omogočajo, da opravijo varna spletna plačila (Patro in drugi, 2016). Na splošno so kartična plačila temelj pri spletnem nakupovanju, zato predpostavljam peto hipotezo:

Hipoteza 5: Največ porabnikov plačilo spletnega nakupa opravi z debetno ali kreditno kartico.

4.2 Metodologija

Oblikovanje empirične raziskave v tej zaključni nalogi je temeljilo na informacijah in ugotovitvah, predstavljenih v teoretičnem delu. Glede na naravo proučevanega problema je bila kot najprimernejša izbrana kvantitativna metoda.

Kvantitativno raziskovanje vključuje uporabo statističnih ali numeričnih podatkov za poglobljeno analiziranje družbenih pojavov. Osredotoča se na dejstvo, da je proučevani pojav mogoče izmeriti. Pri tovrstnih raziskavah se podatki zbirajo z meritvami, analizirajo in preverja se točnost meritev (Watson, 2015).

Pri izbrani metodi sem uporabila spletni anketni vprašalnik, ki je bil porabnikom posredovan prek družbenih medijev. Vprašalnik sem izdelala na spletni strani lka in nato povezavo do njega delila z znanci.

Spletno anketo sem izbrala zaradi enostavnosti priprave vprašalnika, zbiranja podatkov in shranjevanja pridobljene vsebine. Ta pristop mi bo omogočil tudi pridobitev svežih in prilagojenih podatkov, ki neposredno podpirajo moje raziskovalne cilje. Prednost predstavlja tudi hiter odzivni čas anketirancev in možnost širokega dosega. Vsaka vrsta ankete ima svoje prednosti in slabosti oziroma izzive. Pri spletni anketi so izzivi lahko oblike vzorčenja, stopnja odziva, ohranjanje zaupnosti podatkov in etična vprašanja (Mudavath Nayak, 2019).

Kot ciljno populacijo v spletni anketi sem izbrala slovenske porabnike vseh spolov, ki so že kdaj opravili spletni nakup. Velikost vzorca, uporabljenega za zaključno nalogo, je bila 104 anketirancev. Vprašalnik je bil namenjen porabnikom različnih starostnih skupin, ki nakupujejo prek spleta. Preden sem vprašalnik javno objavila sem ga še preizkusno uporabila pri bližnjih osebah, ki so mi zaupale svoje komentarje, namenjene nadaljnjemu preoblikovanju anketnega vprašalnika.

Vprašalnik je oblikovan za raziskovanje vidikov vedenja in zavedanja porabnikov pri spletnem nakupovanju. Sestavljen je iz dvaindvajsetih vprašanj, od katerih se jih devetnajst nanaša na temo spletnega nakupovanja in spletnih nevarnosti, tri vprašanja pa so demografska. Gradivo za izdelavo merskih lestvic in oblikovanje vprašanj je bilo pretežno črpano iz teoretičnega dela zaključne naloge, vprašalnik pa je razdeljen na podobne sklope kot sama naloga.

Vprašalnik najprej vključuje vprašanja na temo nakupovalnih navad porabnikov, skupaj devet vprašanj. Predvsem me zanimajo pogostost spletnih nakupov, najpogostejše kupljene kategorije, prednostni načini plačila, priljubljene spletne platforme in ključni dejavniki, ki vplivajo na odločitev za spletno nakupovanje namesto nakupovanja v fizični trgovini.

Vprašalnik nato preide v drugi del, ki se poglobi v področje zavedanja porabnikov glede spletnih nevarnosti. Sestavljen je iz desetih vprašanj. Tukaj želim od porabnikov izvedeti predvsem, kako velik pomen pripisujejo varnosti svojih osebnih podatkov in kako dobro so po njihovem mnenju informirani o varnosti svojih osebnih podatkov pri spletnem nakupovanju. Zanima me tudi, ali so ozaveščeni o kibernetiskih nevarnostih, ki vse bolj prežijo na neizkušene porabnike. Tukaj želim prav tako preveriti njihovo sposobnost prepoznavanja kibernetiskih groženj ter njihovo poznavanje in uporabo prokativnih

ukrepov, torej kako dobro sprejemajo proaktivne ukrepe za zaščito svojih osebnih podatkov in kako učinkovito izvajajo te ukrepe.

Vprašalnik se zaključí z demografskimi vprašanji, pri katerih morajo anketiranci navesti spol, stopnjo izobrazbe in njihov povprečni mesečni dohodek. Zadnji del vprašalnika naj bi sestavljala lažja vprašanja, ki pa lahko vsebujejo tudi bolj občutljiva vprašanja, kot je npr. vprašanje o dohodku zaradi česar obstaja možnost, da bi anketiranec že pred začetkom zaključil anketo. Ti podatki bodo v pomoč pri podrobnejši analizi pridobljenih podatkov (Sultan in Uddin, 2011).

Anketa, izdelana na spletni strani 1ka.si, je bila aktivna od 7. 8. 2024 do 12. 8. 2024, skupaj pet dni. V tem kratkem obdobju sem pridobila skupaj 197 enot, vendar so od teh le 104 enote (53 %) anketo končali v celoti.

4.3 Analiza podatkov

V tem poglavju nadaljujem z analizo vzorca in vsebinskih vprašanj, ki mi bodo tudi v veliko korist pri doseganju globljega razumevanja sodobnih spletnih porabnikov pri spletnem nakupovanju in pri nadaljnjem preverjanju zastavljenih hipotez.

4.3.1 Opis vzorca

Vzorec je zajemal 104 anketirance ter je bil oblikovan iz (26 %) moške populacije in (74 %) ženske populacije. Rezultati so podrobneje prikazani v prilogi 2 – tabela 1.

Nato je sledilo vprašanje o statusu, kjer se je z največ odgovori (60 %) na prvo mesto uvrstil razred »zaposleni/a«, sledil je razred »študent/ka« (33 %), nato razred »upokojenec/ka« (6 %) in na predzadnjem mestu (1 %) razred »dijak/inja«. Pod drugo (1 %) sem dobila odgovor »stay at home mum«. Rezultati so podrobneje prikazani v prilogi 2 – tabela 2.

Največ anketiranih ima povprečni mesečni prihodek v razredu »do 1000 €« (38 %), sledil je razred »od 1001 € do 2000 €« (35 %), nato razred »od 2001 € do 3000 €« (17 %) in nato »od 3001 € do 4000 €« (1 %). Pod drugo so anketiranci (9 %) navedli »brez odgovora, 0 in ne želim odgovoriti«. Rezultati so bolj podrobno prikazani v prilogi 2 – tabela 3.

4.3.2 Analiza vsebinskih vprašanj

Sedaj sledi analiza vsebinski vprašanj, kjer bom pri porabnikih analizirala predvsem širše razumevanje spletnih groženj in njihovo vedenje pri spletnem nakupovanju.

Uvodno vprašanje je bilo: »Kako pogosto kupujete prek spleta?«. Analiza je pokazala, da največ porabnikov (38 %) prek spleta kupuje nekajkrat letno, sledi odgovor mesečno (35 %), (12 %) anketirancev je označilo odgovor tedensko, naslednje mesto pa si delita odgovora manj kot nekajkrat letno in nikoli s (7 %) anketirancev. (1 %) anketirancev je označilo odgovor drugo, kjer so navedli »kar pogosto«. Rezultati prvega vprašanja so prikazani v prilogi 2 – tabela 4.

Pri drugem vprašanju me je zanimalo, katero kategorijo izdelkov/storitev sodelujoči najpogosteje kupujejo prek spleta. Rezultati kažejo, da prek spleta največ nakupujejo oblačila in obutev (50 %), sledijo kozmetični izdelki (13 %), elektronika (7 %), knjige (6 %), gospodinjski izdelki (6 %) ter izdelki za zdravje (5 %). Majhen delež anketirancev (10 %) je izbral možnost drugo, kjer so kot odgovore navedli »napotki za ročna dela, šport, urbana in dobroimetje, prigrizki in pijača, igre, živila« ter druge. Rezultati drugega vprašanja so prikazani v prilogi 2 – tabela 5.

Pri naslednjem vprašanju sem preverila, katero vrsto plačila anketiranci najpogosteje izberejo pri spletnih nakupih. Največ anketirancev je izbralo odgovor »plačilo s kartico« (54 %), sledil je odgovor »plačilo po povzetju« (25 %), »digitalne denarnice (PayPal, Google Pay, Apple Pay)« pa je izbralo (18 %) anketiranih. Le (2 %) anketiranih sta izbrala odgovor »bančno nakazilo«. Kot drugo je bil naveden odgovor »plačilo na prevzemnem mestu«. Rezultati tretjega vprašanja so prikazani v prilogi 2 – tabela 6.

V četrtem vprašanju sem analizirala, katere platforme porabniki najpogosteje uporabljajo za spletno nakupovanje. Analiza je pokazala naslednje: Aboutyou (42 %), Mimovrste (39 %), Temu (20 %), Amazon (19 %), Aliexpress (19 %), Ebay (8 %) in družbena omrežja (Facebook, Instagram itd.) (8 %). Pod odgovor »drugo« (38 %) so porabniki navedli odgovore »steam, Bigbang, Shoppster, Shein, Notino, Buzz, Etsy« in drugo. Rezultati četrtega vprašanja so prikazani v prilogi 2 – tabela 7.

V okviru petega vprašanja sem anketirance prosila, da za izbrane kriterije opredelijo, kako pomembni so jim pri spletnem nakupovanju. Pri tem je 1 pomenilo »sploh mi ni pomembno« in 5 »je zelo pomembno«. Na prvem mestu je bil kot najpomembnejši kriterij izbran odgovor »varnost plačila« s povprečno vrednostjo 4,9 (standardni odklon, SO = 0,52). Sledi mu »enostavna plačila in zamenjave« s povprečno vrednostjo 4,3 (SO = 1,06). S povprečno vrednostjo 4 (SO = 0,86) je bil izbran odgovor »ocene strank«, sledita mu »hitra dostava« s povprečno vrednostjo 3,9 (SO = 1,01) in »pomoč strankam« s povprečno vrednostjo 3,7 (SO = 1,18). Na zadnjem mestu je ostal najmanj priljubljen kriterij »kode za popust« s povprečno vrednostjo 3,6 (SO = 1,06). Rezultati petega vprašanja so prikazani v prilogi 2 – tabela 8.

Pri šestem vprašanju me je zanimalo, kako bi porabniki ocenili svoje zadovoljstvo pri spletnem nakupovanju. Kar (80 %) anketirancev je zadovoljnih, (18 %) je zelo zadovoljnih, po (1 %) pa je »zelo nezadovoljen/na« in »niti zadovoljen/na niti

nezadovoljen/na«. Povprečna vrednost pri šesti trditvi je 4,1 (standardni odklon, SO = 0,5). Rezultati šestega vprašanja so prikazani v prilogi 2 – tabela 9.

Sledilo je sedmo vprašanje, pri katerem me je zanimalo, kako verjetno je, da bodo porabniki za svoj naslednji nakup izbrali spletno nakupovanje namesto fizičnega. Manj kot polovica bo verjetno izbrala spletni kanal namesto fizičnega (40 %). (21 %) anketirancev je izbralo odgovor »zelo verjetno«, (20 %) porabnikov pa odgovor »niti verjetno niti neverjetno«. Za (13 %) porabnikov je spletno nakupovanje kot naslednji nakup »malo verjetna« izbira, za (7 %) porabnikov pa »zelo malo verjetna«. Povprečna vrednost pri sedmi trditvi je 3,5 (SO = 1,2). Rezultati sedmega vprašanja so prikazani v prilogi 2 – tabela 10.

Pri osmem vprašanju sem želela preveriti, zaradi katerih dejavnikov se porabniki po navadi raje odločijo za izbiro spletnega nakupa namesto fizičnega, pri čemer so lahko izbrali več odgovorov. Največ jih je izbralo odgovor »časovni prihranek« (68 %), dobra polovica (57 %) anketiranih je izbrala odgovor »širši izbor izdelkov«. »Izogib gneči« je izbralo (53 %) anketiranih, medtem ko je (49 %) anketiranih izbralo odgovor »udobje«. Sledita »lažja cenovna primerjava izdelkov« s (36 %) in »finančni prihranek« s (35 %). Na predzadnjem mestu je odgovor »spletne ocene in mnenja kupcev«, ki ga je izbralo (26 %) anketirancev, na zadnjem mestu pa drugi odgovori (6 %) kot so »ne obstaja fizična trgovina, nedostopnost knjig v knjigarnah, popusti« in drugi. Rezultati osmega vprašanja so prikazani v prilogi 2 – tabela 11.

Deveto vprašanje je bilo namenjeno mesečni porabi pri spletnem nakupovanju. Rezultati so pokazali, da največ anketirancev mesečno zapravi med 21 € in 40 € (23 %), na drugem mestu sledita razpon od 0 € do 20 € (22 %) in od 41 € do 60 € (22 %). Odgovor »Več kot 100 €« je izbralo (13 %) anketirancev, od 81 € do 100 € pa (11 %). Le majhen delež porabnikov je izbral odgovor od 61 € do 80 € (9 %). Rezultati devetega vprašanja so prikazani v prilogi 2 – tabela 12.

Pri desetem vprašanju me je zanimalo, ali so bili porabniki že kdaj žrtev spletnih goljufij. Največ porabnikov (72 %) je izbralo trditev »ne«, (16 %) porabnikov je izbralo trditev »da«, (7 %) jih je izbralo trditev »ne vem«. Najmanj porabnikov (5 %) je trdilo, da se jim je uspelo rešiti, še preden bi se jim zgodilo kaj resnega. Rezultati desetega vprašanja so prikazani v prilogi 2 – tabela 13.

V okviru enajstega vprašanja sem pri porabnikih raziskovala, kako pomembna jim je varnost njihovih osebnih podatkov. Velika večina porabnikov je trdila, da jim je njihova varnost zelo pomembna (61 %), nato so sledili porabniki, ki jim je varnost pomembna (38 %). Le (1 %) porabnikov je trdil, da jim varnost ni niti pomembna niti nepomembna. Nihče od porabnikov ni trdil, da jim varnost ni pomembna, niti, da jim varnost njihovih osebnih podatkov na spletu sploh ni pomembna. Povprečna vrednost pri enajsti trditvi je 4,6 (SO = 0,5). Rezultati enajstega vprašanja so prikazani v prilogi 2 – tabela 14.

Pri dvanajstem vprašanju sem anketirance spraševala, kako močno zaupajo v varnost svojih osebnih podatkov pri spletnem nakupovanju. Njihovi odgovori so bili razporejeni tako: zaupam (48 %), niti ne zaupam niti zaupam (38 %), ne zaupam (13 %), sploh ne zaupam (1 %) in povsem zaupam (1 %). Povprečna vrednost pri dvanajsti trditvi je 3,4 (SO = 0,8). Rezultati dvanajstega vprašanja so prikazani v prilogi 2 – tabela 15.

Trinajsto vprašanje se je nanašalo na varnostne ukrepe. Anketirance sem povprašala po tem, kako dobro poznajo različne ukrepe za večjo varnost pri spletnem nakupovanju. Pri analizi sem pridobila naslednje odgovore: poznam (44 %), niti ne poznam niti poznam (38 %), ne poznam (9 %), zelo dobro poznam (7 %) in sploh ne poznam (2 %). Povprečna vrednost pri trinajsti trditvi je 3,4 (SO = 0,8). Rezultati trinajstega vprašanja so prikazani v prilogi 2 – tabela 16.

Pri štirinajstem vprašanju sem anketirancem na kratko opredelila izraz »kibernetška nevarnost«, nato pa je sledilo vprašanje na to temo. Zanimalo me je, ali porabniki poznajo predhodno omenjen izraz. Velika večina (85 %) porabnikov je odgovorila, da ga pozna, (15 %) porabnikov pa je odgovorilo, da izraza ne pozna. Rezultati štirinajstega vprašanja so prikazani v prilogi 2 – tabela 17.

Pri petnajstem vprašanju sem od anketirancev želela izvedeti, za katere izmed navedenih vrst kibernetških nevarnosti so že slišali. Najpogosteje so slišali za »lažne spletne trgovine« (82 %), druga trditev je bila »ribarjenje« (69 %), tretja trditev je bila »zlonamerna programska oprema« (58 %), četrta trditev je bila »socialni inženiring« (33 %), peta trditev je bila »drive-by prenosi« (23 %), šesta trditev je bila »človek v sredini« (15 %) in sedma trditev je bila »nič od tega« (10 %). Rezultati petnajstega vprašanja so prikazani v prilogi 2 – tabela 18.

Sledilo je šestnajsto vprašanje, kjer me je zanimalo, katere ukrepe uporabljajo porabniki za boljšo zaščito svojih osebnih podatkov pri spletnem nakupovanju, izbrali pa so lahko več odgovorov. Odgovori so bili naslednji: kupovanje le pri preverjenih spletnih straneh (94 %), previdnost pri deljenju osebnih podatkov (61 %), pozoren/a sem na HTTPS in URL (51 %), uporaba močnih in edinstvenih gesel (47 %), redno pregledovanje denarnih izpiskov (42 %), dvojna avtentikacija gesel (31 %), ne sprejemam nobenih posebnih podatkov (17 %), pregled izjave o zasebnosti (5 %) in drugo (1 %), kjer je bil naveden odgovor »preverjam naslov trgovca«. Rezultati šestnajstega vprašanja so prikazani v prilogi 2 – tabela 19.

Pri naslednjem vprašanju sem anketirancem predstavila trditev, da podjetja zagotavljajo jasno in razumljivo politiko o varstvu zasebnosti, ter jih prosila za oceno strinjanja. Polovica (50 %) je izbrala odgovor »popolnoma se strinjam«, sledi odgovor »se strinjam« (42 %), nato »niti se ne strinjam niti se strinjam« (7 %) ter »sploh se ne strinjam« (1 %), nihče pa ni izbral odgovora »se ne strinjam«. Povprečna vrednost pri sedemnajsti trditvi je 4,1 (SO = 0,7). Rezultati sedemnajstega vprašanja so prikazani v prilogi 2 – tabela 20.

Pri osemnajstem vprašanju sem anketirance spraševala, kako pogosto preberejo pravilnik o varstvu osebnih podatkov na spletnih straneh trgovin, preden ga sprejmejo. Rezultati kažejo, da (42 %) porabnikov redko prebere pravilnik o varstvu osebnih podatkov, (29 %) nikoli, (26 %) občasno, (3 %) anketirancev pa trdijo, da ga vedno preberejo. Rezultati osemnajstega vprašanja so prikazani v prilogi 2 – tabela 21.

Pri zadnjem devetnajstem vprašanju me je zanimalo, koliko so porabniki zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke. Odgovori so bili naslednji: niti nisem zaskrbljen/a (44 %), sem zaskrbljen/a (32 %), nisem zaskrbljen/a (17 %), sem zelo zaskrbljen/a (5 %) in sploh nisem zaskrbljen/a (2 %). Povprečna vrednost pri devetnajsti trditvi je 3,2 (SO = 0,9). Rezultati devetnajstega vprašanja so prikazani v prilogi 2 – tabela 22.

4.3.3 Preverjanje hipotez

Sedaj sledi podrobnejša analiza preverjanja zastavljenih hipotez.

Hipoteza 1: Porabniki so nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke.

Pri prvi hipotezi sem postavila domnevo, da so porabniki nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke, pri čemer sem pri devetnajstem vprašanju v anketi postavila vprašanje, kako zaskrbljeni so porabniki glede tega, kako podjetja uporabljajo njihove osebne podatke. Hipotezo sem preverjala z Wilcoxonovim testom za en vzorec, kjer sem določila testno mediano (3), ki sem jo nato primerjala s pridobljenimi rezultati. Podrobnejša statistična analiza mi je pokazala, da so porabniki res nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke, kar nakazujejo tudi rezultati, ki so pokazali, da so vrednosti višje od testne mediane (3) ($p = 0,016$). Na podlagi p -vrednosti, ki je manjša od 0,05, postavljeno hipotezo lahko sprejemem. To je razvidno v prilogi 2 – tabela 23 in graf 1.

Hipoteza 2: Glavni razlog za spletni nakup pri porabnikih je časovni prihranek.

Pri drugi hipotezi sem postavila domnevo, da je glavni razlog za spletni nakup pri porabnikih časovni prihranek. Hipotezo sem preverjala pri osmem vprašanju, kjer sem anketirance spraševala, zaradi katerih dejavnikov se po navadi raje odločijo za izbiro spletnega nakupa namesto fizičnega. Hipotezo sem preverjala s Hi-kvadrat testom za preizkus hipoteze enake verjetnosti. Pri analizi je bilo 96 veljavnih odgovorov, preostalih 25 pa zaradi lažje analize nisem uporabila. Na podlagi pridobljenih rezultatov, sem ugotovila, da je največ anketirancev izbralo odgovor »časovni prihranek«, poleg odgovora »drugo« pa je najmanj anketirancev izbralo odgovor »spletne ocene in mnenja kupcev«. Na podlagi pridobljenih rezultatov iz statistične analize lahko na podlagi p -vrednosti, manjše od 0,05, ovržem ničelno hipotezo in sprejemem hipotezo, da je glavni

razlog za spletni nakup pri porabnikih časovni prihranek. To je razvidno v prilogi 2 – tabela 24 in 25.

Hipoteza 3: Večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov.

Pri tretji hipotezi se postavila domnevo, da večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov, pri čemer sem pri šestnajstem vprašanju v anketi povprašala anketirance po tem, katere ukrepe uporabljajo pri spletnem nakupovanju za boljšo zaščito svojih osebnih podatkov. Hipotezo sem preverjala s Hi-kvadrat testom za preizkus hipoteze enake verjetnosti. Anketirance sem razdelila v dve skupini. Prva skupina so tisti, ki sprejemajo vsaj en proaktiven ukrep, druga skupina pa so tisti, ki proaktivnih ukrepov ne sprejemajo. Na podlagi statistične analize sem ugotovila, da med vsemi, ki so anketo izpolnili, pri spletnem nakupovanju samo ena oseba ne sprejema proaktivnih ukrepov za zaščito svojih osebnih podatkov. Na drugi strani pa je 95 anketirancev izbralo odgovor, da sprejemajo proaktivne ukrepe. Ta skupina predstavlja večinski delež oziroma več kot (50 %) anketiranih. Na podlagi pridobljenih rezultatov lahko pri p-vrednosti, manjši od 0,05, ničelno hipotezo zavrnem in sprejemam hipotezo, da večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih osebnih podatkov. To je razvidno v prilogi 2 – tabela 26 in 27.

Hipoteza 4: Večina porabnikov opravi nakup prek spleta več kot enkrat mesečno.

Pri četrti hipotezi sem postavila domnevo, da večina porabnikov opravi nakup prek spleta več kot enkrat mesečno. Hipotezo sem preverjala pri prvem vprašanju, kjer sem anketirance spraševala, kako pogosto kupujejo prek spleta. Hipotezo sem preverjala s Hi-kvadrat testom za preizkus hipoteze enake verjetnosti. Za podrobnejšo analizo hipoteze sem ustvarila novo spremenljivko »več kot enkrat mesečno«, ki bi med navedenimi skupinami iz ankete zajemala odgovore, kot so »dnevno, tedensko in mesečno«. Rezultati testa so pokazali, da manj kot (50 %) anketirancev spletne nakupe opravi pogosteje kot enkrat mesečno. Na podlagi pridobljenih rezultatov sem ugotovila, da je delež anketiranih, ki nakupujejo prek spleta več kot enkrat mesečno, manj kot (50 %), torej hipoteze pri stopnji značilnosti $p = 0,05$ ne morem sprejeti. To je razvidno v prilogi 2 – tabela 28 in 29.

Hipoteza 5: Največ porabnikov plačilo spletnega nakupa opravi z debetno ali kreditno kartico.

Pri peti hipotezi sem postavila domnevo, da največ porabnikov plačilo spletnega nakupa opravi z debetno ali kreditno kartico, pri čemer sem pri tretjem vprašanju v anketi anketirance povprašala, katero vrsto plačila najpogosteje izberejo pri spletnih nakupih. Hipotezo sem preverjala s Hi-kvadrat testom za preizkus hipoteze enake verjetnosti, saj me je zanimalo, ali lahko razlike, ki so nastale med pridobljenimi odgovori iz ankete, tudi

posplošim na populacijo. Razvidno je bilo, da največ ljudi uporablja plačila s kartico, najmanj pa bančna nakazila. P-vrednost je manjša od meje statistične vrednosti $p = 0,05$, iz česar sem lahko ugotovila, da je med odgovori o izbiri vrste plačila statistično pomembna razlika. Prav tako je iz tabele razvidno, da je največ anketirancev izbralo plačevanje s kartico, torej lahko hipotezo potrdim. To je razvidno v prilogi 2 – tabela 30.

4.4 Interpretacija ugotovitev

S pomočjo empirične raziskave sem raziskovala, kako dobro se porabniki zavedajo spletnih nevarnosti med tem spletnim nakupovanjem in kateri dejavniki vplivajo na njihovo nakupno odločitev, da nakup izdelkov ali storitev raje opravijo prek spleta kot v tradicionalnih fizičnih trgovinah. Pri spletnih porabnikih sem želela tudi raziskati, katere proaktivne varnostne ukrepe že poznajo in če katerega od njih za boljšo zaščito svojih podatkov na spletu tudi sami sprejemajo.

Tabela 1 prikazuje zaključne ugotovitve, ki sem jih lahko sprejela na podlagi analize preverjanja hipotez. Sledi tudi podrobnejša interpretacija ugotovitev hipotez, povezanih z drugimi raziskavami.

Tabela 1: Pregled hipotez

Hipoteza	Ugotovitev
H1: Porabniki so nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke.	Sprejemem.
H2: Glavni razlog za spletni nakup pri porabnikih je časovni prihranek.	Sprejemem.
H3: Večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov.	Sprejemem.
H4: Večina porabnikov opravi nakup prek spleta več kot enkrat mesečno.	Ne morem sprejeti.
H5: Največ porabnikov plačilo spletnega nakupa opravi z debetno ali kreditno kartico.	Sprejemem.

Vir: lastno delo.

Pri prvi hipotezi sem na podlagi raziskave podjetja KPMG (2021), ki navaja, da se je odstotek porabnikov, ki so zaskrbljeni glede zasebnosti do leta 2024 še povečal, oblikovala hipotezo, da so porabniki nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke. Empirična analiza je pokazala, da so porabniki res nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke. Torej lahko tudi potrdim da, trditev raziskave KPMG drži.

Pri drugi hipotezi me je zanimal glavni razlog za spletni nakup pri porabnikih. Na podlagi raziskave SURS (2022) sem postavila hipotezo, da je glavni razlog za spletni nakup pri porabnikih časovni prihranek, kar lahko tudi sprejemem, saj je časovni prihranek kot glavni dejavnik za spletno nakupovanje izbralo (68 %) anketirancev, kar je bil tudi najpogostejši odgovor. Torej lahko tudi potrdim, da trditev raziskave SURS drži.

Pri tretji hipotezi sem analizirala, ali večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov. Hipotezo sem oblikovala na podlagi raziskave, ki jo je izvedel Cisco (2023). Tudi tretjo hipotezo sem lahko sprejela, saj so rezultati pokazali, da so statistično pomembne razlike med tistimi, ki proaktivne ukrepe sprejemajo, in med tistimi, ki jih ne, pri čemer je tistih, ki sprejemajo proaktivne ukrepe več kot (50 %). Torej lahko hipotezo, ki sem jo postavila na podlagi raziskave, ki jo je izvedel Cisco, potrdim.

Pri čerti hipotezi sem na podlagi raziskave, ki jo je izvedel SURS (2023), oblikovala hipotezo, s katero sem preverjala, ali večina porabnikov opravi nakup prek spleta več kot enkrat mesečno. Ugotovitve empirične raziskave so mi pokazale, da te trditve ne morem sprejeti, saj je bil pri analizi rezultatov delež tistih, ki nakupujejo prek spleta več kot enkrat mesečno, manjši od (50 %).

Pri peti hipotezi sem uporabila raziskavo, ki jo je prav tako tako izvedel SURS (2023) in pri kateri so rezultati pokazali, da največ porabnikov pri spletnem nakupu uporabi debetno ali kreditno kartico. Na podlagi teh podatkov sem oblikovala hipotezo, da največ uporabnikov plačilo spletnega nakupa opravi z debetno ali kreditno kartico. S pomočjo analize sem lahko sprejela hipotezo, ki je bila tudi v skladu z navedbo SURS.

5 SKLEP

V zaključni strokovni nalogi sem pisala o spletnem nakupovanju, pri čemer sem opisala njegovo zgodovino ter kako se je skozi leta razvoja in napredka zgodila digitalna preobrazba, ki je kljub svojim prednostim prinesla tudi veliko tveganj in skrbi za spletne porabnike, tako na področju zasebnosti kot tudi na področju varnosti osebnih in finančnih podatkov.

Razne bližnjice za porabnike na spletu s seboj prinašajo tudi vedno večje nevarnosti, kar sem podrobneje opisala v poglavju kibernetske varnosti. Tukaj sem pisala predvsem o njihovem splošnem razumevanju, opisala pa sem tudi različne vrste varnostnih groženj, ki jih je iz leta v leto več. Globlje sem raziskovala tudi področje sprejemanja varnostnih ukrepov, ki bi jih moral upoštevati prav vsak spletni porabnik, da svojo zasebnost ohrani dobro zaščiten pred raznimi kibernetskimi napadi in kraji. Zanimalo me je tudi, kako dobro se porabniki zavedajo kibernetskih nevarnosti. Anketa (Deloitte) iz leta 2015 je bila že velik pokazatelj, da skrb za varnost osebnih podatkov pri spletnih porabnikih strmo narašča ter da porabniki ne zaupajo več popolnoma spletnim omrežjem, saj predvsem v

sodobnem času ne moreš nikoli ne moreš nikoli resnično vedeti, kdo sedi na drugi strani računalniškega zaslona in kakšni so njegovi nameni.

To sem še podrobneje raziskala v empiričnem delu raziskave, kjer je sem želela predvsem raziskati, kako dobro so porabniki ozaveščeni o spletnih nevarnostih in kateri dejavniki vplivajo na njihovo nakupno odločitev, da nakup raje opravijo prek spleta namesto v tradicionalni fizični trgovini. Zanimalo pa me je tudi, kako dobro poznajo različne proaktivne ukrepe za boljšo varnost pri spletnem nakupovanju in ali katerega od njih tudi sami sprejemajo.

Lahko sem uspešno potrdila vse hipoteze, razen ene, ki sem si jih zastavila že na začetku pisanja zaključne naloge. Na podlagi analize hipotez lahko zaključim, da so porabniki nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke. Njihov glavni razlog za spletni nakup je časovni prihranek, večina porabnikov pa pri spletnem nakupovanju sprejema proaktivne ukrepe. Prav tako lahko trdim, da največ porabnikov pri plačilu na spletu uporablja debetno ali kreditno kartico. Menim, da sem sem s pomočjo empiričnega dela lahko dosegla svoje namene in cilje, ki sem si jih zastavila že v uvodu zaključne naloge.

Pri omejitvah raziskovanja lahko izpostavim, da je bil zaradi kratkega obdobja izvedbe ankete vzorec dokaj majhen in poleg tega nenaključno izbran, zato ne morem trditi, da bi rezultati, ki sem jih pridobila z empirično raziskavo lahko veljali za širšo populacijo. Prav tako sem za pomoč pri pridobivanju odgovorov uporabila način spletnega vprašalnika, pri katerem se lahko zgodi, da odgovori niso povsem resnični, in čeprav je anketa bila anonimna, bi to lahko povzročilo nenatančne rezultate. Lahko trdim, da sem imela pri izbrani temi zelo dobro podlago virov, predvsem tujih, ki so mi pomagali pri pisanju teorije.

V zaključku raziskovalne naloge pa bi porabnike in tudi vse druge, ki ne opravljajo spletnih nakupov, vendar vseeno radi raziskujejo po različnih spletnih straneh, opozorila na to, kako pomembna sta sprejemanje varnostnih ukrepov in ohranjanje pozornosti, saj nas lahko že manjši nepozorni kliki spravijo v velike težave. Podjetjem pa bi svetovala, da v svoje programe izobraževanj vključijo tudi usposabljanje svojih zaposlenih o kibernetski varnosti. Zelo pomembno je, da zaposleni vedo, kako prepoznati različne kibernetske napade in kako se jim izogniti. Takšna izobraževanja bi koristila tako posameznikom kot tudi podjetjem, saj lahko zgolj le klik na napačno e-pošto povzroči škodo za informacijsko varnost podjetja.

LITERATURA IN VIRI

1. Advent Biztech Solution. (2023). *The e-commerce industry has seen unprecedented growth in recent years, thanks to the rapid advancement of*

- technology. <https://www.linkedin.com/pulse/e-commerce-industry-has-seen-unprecedented>
2. Aseri, A. M. (2021). Security Issues For Online Shoppers. *International Journal of Trend in Scientific Research and Development*, 10(3), 2277–8616.
 3. Biju, J. M., Gopal, N. in Prakash, A. J. (2019). Cyber attacks and its different types. *International Research Journal of Engineering and Technology*, 6(3), 2395–0056.
 4. Brožova, S. in Ingaldi, M. (2020). Safety of online shopping according to customers. V *System Safety: Human - Technical Facility - Environment* (str.73–81). Sciendo.
 5. Cisco. (2023). *Privacy's Growing Importance and Impact*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf
 6. Computer Hope. (2023). *Online shopping*. <https://www.computerhope.com/jargon/o/online-shopping.htm>
 7. Coursera. (2023). *5 Cybersecurity threats to know in 2024*. https://www.coursera.org/articles/cybersecurity-threats?utm_medium=sem&utm_source=gg&utm_campaign=B2C_EMEA__coursera_FTCOF_career-academy_pmax-multiple-audiences-country-multi&campaignid=20858198824&adgroupid=&device=c&keyword=&matchtype=&network=x&devicemodel=&adposition=&creativeid=&hide_mobile_promo&gad_source=1&gclid=EAIaIQobChMIuJHx09rfhwMVuKODBx0McgoLEAAYASAAEgLGvPD_BwE
 8. ECPI University. (brez datuma). *Online shopping security issues and how cyber security can help* [objava na blogu]. <https://www.ecpi.edu/blog/online-shopping-security-issues-and-how-cyber-security-can-help>
 9. Faster Capital. (2024, 22. junij). *Mobile Devices and Moore's Law: The Evolution of Portable Technology*. <https://fastercapital.com/content/Mobile-Devices-and-Moore-s-Law--The-Evolution-of-Portable-Technology.html#AR--VR--and-Beyond.html>
 10. Fenech, C., Hamilton, L., Borwick, S. in Perkins, B., (2015). *The Deloitte Consumer Review. Consumer data under attack: The growing threat of cyber crime*. <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/consumer-review-nov-2015.pdf>
 11. Fumudoh, S. in Viswanathan, U. (2014). *Exploring the relationship between online privacy on cyber security* (magistrsko delo). Luleå University of Technology, Švedska.
 12. Hiral, B. P. (2020). E-commerce security threats, defenses against attacks and improving security. *International Journal of Multidisciplinary Educational Research*, 9(4), 2277–7881.

13. Hunwickprimary. (brez datuma). *Parental internet safety*. <https://www.hunwickprimary.org.uk/files/file/esafety/Parental%20Internet%20Safety.pdf>
14. Ip-rs. (2009, 4. september). *Socialni inženiring in kako se pred njim ubraniti?* https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf
15. Javeed, D., Badamasi, U. M., Ndubuisi, C. O., Soomro, F. in Asif, M. (2020). Man in the middle attacks: analysis, motivation and prevention. *International Journal of Computer Networks and Communications Security*, 8(7), 2308–9830.
16. Kaspersky. (brez datuma). *Online shopping safety risks and how to protect yourself*. <https://www.kaspersky.com/resource-center/threats/how-safe-is-online-shopping>
17. Laliberte, M. (2023, 27. marec). *A brief history of online shopping* [objava na blogu]. <https://www.odmworld.com/blog/brief-history-of-online-shopping/>
18. Market Business News. (brez datuma). *Online shopping – definition and meaning*. <https://marketbusinessnews.com/financial-glossary/online-shopping-definition-meaning/>
19. Mass.gov. (brez datuma). *Know the types of cyber threats*. <https://www.mass.gov/info-details/know-the-types-of-cyber-threats>
20. Mayford, Z. (2023, 5. oktober). *How to spot fake internet shopping sites before they scam you* [objava na blogu]. <https://ebrand.com/blog/fake-internet-shopping-sites-and-how-to-spot-them/>
21. Mlada, P. (2021, 21. maj). *Privacy concerns stop customers from buying* [objava na blogu]. Pridobljeno 15. maja 2024 iz <https://openli.com/blog/privacy-concerns>
22. Mlakar, T. (2022, 3. november). *Spletno nakupovanje*. <https://www.stat.si/StatWeb/sl/News/Index/10637>
23. Mlakar, T. (2023, 2. november). *Spletno nakupovanje*. <https://www.stat.si/StatWeb/News/Index/11446>
24. Mudavath Nayak, S. K A, N. (2019). Strengths and Weakness of Online Surveys. *IOSR Journal of Humanities and Social Sciences*, 24(5), 1–38.
25. Ontario. (2013). *E-commerce: Purchasing and selling online*. <https://dr6j45jk9xcmk.cloudfront.net/documents/435/medi-booklet-e-commerce-accessible-e-final.pdf>
26. Othman, Y., Mustaffa, M. S. A., Joni, E. K. E., Badrolhisam, N. I., Hasan, Z., in Ahmad, S. N. A. (2017). Online shopping: Consumers' awareness of their rights and protection. *Advanced Science Letters*, 23(8), 7907–7910.
27. Patro, S., P., Padhy, N. in Panigrahi, R. (2016). Security Issues over E-Commerce and their Solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(12), 2278–1021.

28. Sultan, M. U., Uddin, M. N. (2011). *Consumers' Attitude towards Online Shopping. Factors influencing Gotland consumers to shop online* (magistrsko delo). Univerza Gotland.
29. Unctad. (2020, 8. oktober). *COVID-19 has changed online shopping forever, survey shows*. <https://unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows>
30. Watson, R. (2015). Quantitative research. Nursing standard. *Official newspaper of the Royal College of Nursing*, 29(31), 44–48.

PRILOGE

Priloga 1: Anketni vprašalnik

Pozdravljeni sem Pavlina Peterca, študentka Ekonomske fakultete v Ljubljani, in ob zaključku študija pripravljam zaključno nalogo o varnosti pri spletnem nakupovanju. S tem namenom zbiram podatke s pomočjo ankete. Anketa je anonimna, za izpolnjevanje boste potrebovali približno 5 minut. Zbrani podatki bodo obravnavani strogo zaupno in analizirani na splošno in ne na ravni posameznika. Uporabljeni bodo izključno za pripravo te zaključne strokovne naloge.

Q1 - Kako pogosto kupujete prek spleta?

- ☐ Dnevno
- ☐ Tedensko
- ☐ Mesečno
- ☐ Nekajkrat letno
- ☐ Manj kot nekajkrat letno
- ☐ Nikoli
- ☐ Drugo:

Q2 - Katero kategorijo izdelkov/storitev najpogosteje kupujete prek spleta?

- ☐ Oblečila in obutev
- ☐ Elektronika
- ☐ Knjige
- ☐ Glasba
- ☐ Izdelki za zdravje
- ☐ Gospodinjski izdelki
- ☐ Kozmetični izdelki
- ☐ Izdelki za hišne ljubljence
- ☐ Drugo:

Q3 - Katero vrsto plačila najpogosteje izberete pri spletnih nakupih?

- ☐ Plačilo s kartico
- ☐ Bančno nakazilo
- ☐ Plačilo po povzetju
- ☐ Digitalne denarnice (PayPal, Google Pay, Apple Pay)
- ☐ Drugo:

Q4 - Katere spletne platforme najpogosteje uporabljate za spletno nakupovanje?

Možnih je več odgovorov

- ☐ Aboutyou
- ☐ Temu
- ☐ Amazon

- ☐ Ebay
- ☐ Aliexpress
- ☐ Mimovrste
- ☐ Družbena omrežja (Facebook, Instagram,...)
- ☐ Drugo:

Q5 - Prosim, da za spodnje kriterije opredelite, kako pomembni so vam pri spletnem nakupovanju. Pri tem je 1 »Sploh ni pomembno«, 5 pa je »Je zelo pomembno«.

	1	2	3	4	5
Hitra dostava	☐	☐	☐	☐	☐
Enostavna vračila in zamenjave	☐	☐	☐	☐	☐
Pomoč strankam	☐	☐	☐	☐	☐
Varnost plačila	☐	☐	☐	☐	☐
Kode za popust	☐	☐	☐	☐	☐
Ocene strank	☐	☐	☐	☐	☐

Q6 - Kako bi na splošno ocenili vaše zadovoljstvo pri spletnem nakupovanju?

- ☐ Zelo nezadovoljen/a
- ☐ Nezadovoljen/a
- ☐ Niti zadovoljen/a niti nezadovoljen/a
- ☐ Zadovoljen/a
- ☐ Zelo zadovoljen/a

Q7 - Kako verjetno je, da boste za naslednji nakup izbrali spletno nakupovanje namesto fizičnega?

- ☐ Zelo malo verjetno
- ☐ Malo verjetno
- ☐ Niti verjetno niti neverjetno
- ☐ Verjetno
- ☐ Zelo verjetno

Q8 - Zaradi katerih dejavnikov se ponavadi raje odločite za izbiro spletnega nakupa namesto fizičnega nakupa?

Možnih je več odgovorov

- ☐ Časovni prihranek
- ☐ Finančni prihranek
- ☐ Širši izbor izdelkov
- ☐ Udobje
- ☐ Izogib gneči
- ☐ Lažja cenovna primerjava izdelkov
- ☐ Spletne ocene in mnenja kupcev
- ☐ Drugo:

Q9 - Koliko na mesec povprečno zapravite za spletne nakupe?

- ☐ 0 - 20 €
- ☐ 21 - 40 €
- ☐ 41 - 60 €
- ☐ 61 - 80 €
- ☐ 81 - 100 €
- ☐ Več kot 100 €

Q10 - Ali ste že kdaj bili žrtev spletnih goljufij?

- ☐ Da
- ☐ Ne
- ☐ Uspelo se mi je rešiti, preden bi se zgodilo kaj resnega
- ☐ Ne vem

Q11 - Kako pomembna vam je varnost vaših osebnih podatkov?

- ☐ Mi sploh ni pomembna
- ☐ Mi ni pomembna
- ☐ Mi ni niti pomembna niti nepomembna
- ☐ Pomembna mi je
- ☐ Zelo mi je pomembna

Q12 - Kako močno zaupate v varnost vaših osebnih podatkov pri spletnem nakupovanju?

- ☐ Sploh ne zaupam
- ☐ Ne zaupam
- ☐ Niti ne zaupam niti zaupam
- ☐ Zaupam
- ☐ Povsem zaupam

Q13 - Kako dobro poznate različne ukrepe za večjo varnost pri spletnem nakupovanju?

- ☐ Sploh ne poznam
- ☐ Ne poznam
- ☐ Niti ne poznam niti poznam
- ☐ Poznam
- ☐ Zelo dobro poznam

Q14 - Med spletnim nakupovanjem se pojavlja vedno več tako imenovanih »kibernetskih nevarnosti«, ki nam lahko hudo poškodujejo računalniški sistem ali zlorabijo naše osebne podatke.

Ali poznate izraz kibernetike nevarnosti?

- ☐ Da
- ☐ Ne

Q15 - Za katere izmed naslednjih vrst kibernetičnih nevarnosti ste že slišali?

Možnih je več odgovorov

- ☐ Zlonamerna programska oprema (angl. Malware)
- ☐ Socialni inženiring
- ☐ Ribarjenje (angl. Phishing)
- ☐ Lažne spletne trgovine
- ☐ Drive-by prenosi (angl. Drive-by download attacks)
- ☐ Človek v sredini (angl. Man in the Middle)
- ☐ Nič od tega
- ☐ Drugo:

Q16 - Katere izmed ukrepov uporabljate za boljšo zaščito vaših osebnih podatkov pri spletnem nakupovanju?

Možnih je več odgovorov

- ☐ Kupovanje le pri preverjenih spletnih straneh
- ☐ Uporaba močnih in edinstvenih gesel
- ☐ Dvojna avtentikacija gesel
- ☐ Pozoren/a sem na HTTPS in URL
- ☐ Pregled izjave o zasebnosti
- ☐ Redno pregledovanje denarnih izpiskov
- ☐ Previdnost pri deljenju osebnih podatkov
- ☐ Ne sprejemam nobenih posebnih podatkov
- ☐ Drugo:

Q17 - Prosim, da za spodnjo trditev o politiki varstva osebnih podatkov opredelite, do kakšne mere se strinjate z njo.

Pomembno je, da podjetja zagotavljajo jasno in razumljivo politiko o varstvu zasebnosti.

- ☐ Sploh se ne strinjam
- ☐ Se ne strinjam
- ☐ Niti se ne strinjam niti se strinjam
- ☐ Se strinjam
- ☐ Popolnoma se strinjam

Q18 - Kako pogosto preberete pravilnik o varstvu osebnih podatkov na spletnih straneh trgovin, preden ga sprejmete?

- ☐ Vedno
- ☐ Občasno
- ☐ Redko
- ☐ Nikoli

Q19 - Do kakšne mere ste zaskrbljeni glede tega, kako podjetja uporabljajo vaše osebne podatke?

- ☐ Sploh nisem zaskrbljen/a
- ☐ Nisem zaskrbljen/a
- ☐ Niti nisem zaskrbljen/a niti ne zaskrbljen/a
- ☐ Sem zaskrbljen/a
- ☐ Sem zelo zaskrbljen/a

Q20 - Spol

- ☐ Moški
- ☐ Ženska

Q21 - Status

- ☐ Dijak/inja
- ☐ Študent/ka
- ☐ Zaposleni/a
- ☐ Brezposelni/a
- ☐ Upokojenec/ka
- ☐ Drugo:

Q22 - Vaš povprečni mesečni prihodek

- ☐ Do 1000 €
- ☐ Od 1001 do 2000 €
- ☐ Od 2001 do 3000 €
- ☐ Od 3001 do 4000 €
- ☐ Od 4001 do 5000 €
- ☐ Nad 5000 €
- ☐ Drugo:

Priloga 2: Analiza anketnih vprašanj in analiza hipotez

Tabela 1: Analiza anketirancev po spolu

Spol	Frekvenca	Odstotek (%)
Ženska	77	74 %
Moški	27	26 %
SKUPAJ	104	100 %

Vir: lastno delo.

Tabela 2: Analiza anketirancev po statusu

Status	Frekvenca	Odstotek (%)
Dijak/inja	1	1 %
Študent/ka	34	33 %
Zaposleni/a	62	60 %
Brezposelni/a	0	0 %
Upokojenec/ka	6	6 %
Drugo	1	1 %
SKUPAJ	104	100 %

Vir: lastno delo.

Tabela 3: Analiza anketirancev po prihodku

Povprečni mesečni dohodek	Frekvenca	Odstotek (%)
Do 1000 €	39	38 %
Od 1001 do 2000 €	36	35 %
Od 2001 do 3000 €	18	17 %
Od 3001 do 4000 €	1	1 %
Od 4001 do 5000 €	0	0 %
Nad 5000 €	0	0 %
Drugo	0	9 %
SKUPAJ	103	100 %

Vir: lastno delo.

Tabela 4: Pogostost nakupa

Odgovori	Frekvenca	Odstotek (%)
Oblačila in obutev	48	50 %
Kozmetični izdelki	12	13 %
Elektronika	7	7 %
Knjige	6	6 %
Gospodinjski izdelki	6	6 %

Izdelki za zdravje	5	5 %
Izdelki za hišne ljubljence	2	2 %
Glasba	0	0 %
Drugo	10	10 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 5: Najpogosteje izbrana kategorija

Odgovori	Frekvenca	Odstotek (%)
Olačila in obutev	48	50 %
Kozmetični izdelki	12	13 %
Elektronika	7	7 %
Knjige	6	6 %
Gospodinjski izdelki	6	6 %
Izdelki za zdravje	5	5 %
Izdelki za hišne ljubljence	2	2 %
Glasba	0	0 %
Drugo	10	10 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 6: Najpogostejša izbira plačila

Odgovori	Frekvenca	Odstotek (%)
Plačilo s kartico	52	54 %
Plačilo po povzetju	24	25 %
Digitalne denarnice (PayPal, Google Pay, Apple Pay)	17	18 %
Bančno nakazilo	2	2 %
Drugo	1	1 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 7: Najpogosteje uporabljene spletne platforme

Odgovori	Frekvenca	Odstotek (%)
Aboutyou	40	42 %
Mimovrste	37	39 %
Temu	19	20 %

Amazon	18	19 %
Aliexpress	18	19 %
Ebay	8	8 %
Družbena omrežja (Facebook, Instagram,..)	8	8 %
Drugo	36	38 %
SKUPAJ	96	193 %

Vir: lastno delo.

Tabela 8: Pomembnost kriterijev pri spletnem nakupovanju

Odgovori						Skupaj	Povprečje	Std. odklon
Trditev	Sploh ni pomembno	Ni pomembno	Ni pomembno, niti nepomembno	Je pomembno	Je zelo pomembno			
Varnost plačila	1 1 %	0 0 %	1 1 %	7 7 %	86 91 %	95 100 %	4,9	0,52
Enostavnost vračila in zamenjave	3 3 %	3 3 %	15 16 %	13 14 %	61 64 %	95 100 %	4,3	1,06
Ocene strank	1 1 %	3 3 %	19 20 %	43 45 %	29 31 %	95 100 %	4	0,86
Hitra dostava	2 2 %	5 5 %	24 25 %	30 32 %	34 36 %	95 100 %	3,9	1,01
Pomoč strankam	4 4 %	11 12 %	26 27 %	21 22 %	33 35 %	95 100 %	3,7	1,18
Kode za popust	3 3 %	11 12 %	31 33 %	29 31 %	21 22 %	95 100 %	3,6	1,06

Vir: lastno delo.

Tabela 9: Zadovoljstvo pri spletnem nakupovanju

Odgovori	Frekvenca	Odstotek (%)
Zelo malo verjetno	7	7 %
Malo verjetno	12	13 %
Niti verjetno, niti neverjetno	19	20 %
Verjetno	38	40 %
Zelo verjetno	20	21 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 10: Verjetnost za naslednji spletni nakup

Odgovori	Frekvenca	Odstotek (%)
Zelo malo verjetno	7	7 %
Malo verjetno	12	13 %
Niti verjetno, niti neverjetno	19	20 %
Verjetno	38	40 %
Zelo verjetno	20	21 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 11: Dejavniki za izbor spletnega nakupa

Odgovori	Frekvenca	Odstotek (%)
Časovni prihranek	65	68 %
Širši izbor izdelkov	55	57 %
Izogib gneči	51	53 %
Udobje	47	49 %
Lažja cenovna primerjava izdelkov	35	36 %
Finančni prihranek	34	35 %
Spletne ocene in mnenja kupcev	25	26 %
Drugo	6	6 %
SKUPAJ	96	330 %

Vir: lastno delo.

Tabela 12: Koliko na mesec povprečno zapravite za spletne nakupe?

Odgovori	Frekvenca	Odstotek (%)
0 - 20 €	21	22 %

21 - 40 €	22	23 %
41 - 60 €	21	22 %
61 - 80 €	9	9 %
81 – 100 €	11	11 %
Več kot 100 €	12	13 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 13: Ali ste že kdaj bili žrtev spletnih goljufij?

Odgovori	Frekvenca	Odstotek (%)
Da	15	16 %
Ne	69	72 %
Uspelo se mi je rešiti, preden bi se zgodilo kaj resnega	5	5 %
Ne vem	7	7 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 14: Kako pomembna vam je varnost vaših osebnih podatkov?

Odgovori	Frekvenca	Odstotek (%)
Mi sploh ni pomembna	0	0 %
Mi ni pomembna	0	0 %
Mi ni niti pomembna, niti nepomembna	1	1 %
Pomembna mi je	36	38 %
Zelo mi je pomembna	59	61 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 15: Kako močno zaupate v varnost vaših osebnih podatkov pri spletnem nakupovanju?

Odgovori	Frekvenca	Odstotek (%)
Sploh ne zaupam	1	1 %
Ne zaupam	12	13 %
Niti ne zaupam, niti zaupam	36	38 %
Zaupam	46	48 %

Povsem zaupam	1	1 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 16: Kako dobro poznate različne ukrepe za večjo varnost pri spletnem nakupovanju?

Odgovori	Frekvenca	Odstotek (%)
Sploh ne poznam	2	2 %
Ne poznam	9	9 %
Niti ne poznam, niti poznam	36	38 %
Poznam	42	44 %
Zelo dobro poznam	7	7 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 17: Poznavanje izraza "kibernetika nevarnost"

Odgovori	Frekvenca	Odstotek (%)
Da	82	85 %
Ne	14	15 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 18: Za katere izmed naslednjih vrst kibernetičnih nevarnosti ste že slišali?

Odgovori	Frekvenca	Odstotek (%)
Lažne spletne trgovine	79	82 %
Ribarjenje	66	69 %
Zlonamerna programska oprema	56	58 %
Socialni inženiring	32	33 %
Drive-by prenosi	22	23 %
Človek v sredini	14	15 %
Nič od tega	10	10 %
Drugo	0	0 %
SKUPAJ	96	290 %

Vir: lastno delo.

Tabela 19: Katere izmed ukrepov uporabljate za boljšo zaščito vaših osebnih podatkov pri spletnem nakupovanju?

Odgovori	Frekvenca	Odstotek (%)
Kupovanje le pri preverjenih spletnih straneh	90	94 %
Previdnost pri deljenju osebnih podatkov	59	61 %
Pozoren/a sem na HTTPS in URL	49	51 %
Uporaba močnih in edinstvenih gesel	45	47 %
Redno pregledovanje denarnih izpiskov	40	42 %
Dvojna avtentikacija gesel	30	31 %
Ne sprejemam nobenih posebnih podatkov	16	17 %
Pregled izjave o zasebnosti	5	5 %
Drugo	1	1 %
SKUPAJ	96	349 %

Vir: lastno delo.

Tabela 20: Pomembno je, da podjetja zagotavljajo jasno in razumljivo politiko o varstvu zasebnosti.

Odgovori	Frekvenca	Odstotek (%)
Sploh se ne strinjam	1	1 %
Se ne strinjam	0	0 %
Niti se ne strinjam niti se strinjam	7	7 %
Se strinjam	40	42 %
Popolnoma se strinjam	48	50 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 21: Kako pogosto preberete pravilnik o varstvu osebnih podatkov na spletnih straneh trgovin, preden ga sprejmete?

Odgovori	Frekvenca	Odstotek (%)
Vedno	3	3 %

Občasno	25	26 %
Redko	40	42 %
Nikoli	28	29 %
SKUPAJ	96	100 %

Vir: lastno delo.

Tabela 22: Do kakšne mere ste zaskrbljeni glede tega, kako podjetja uporabljajo vaše osebne podatke?

Odgovori	Frekvenca	Odstotek (%)
Sploh nisem zaskrbljen/a	2	2 %
Nisem zaskrbljen/a	16	17 %
Niti nisem zaskrbljen/a niti ne zaskrbljen/a	42	44 %
Sem zaskrbljen/a	31	32 %
Sem zelo zaskrbljen/a	5	5 %
SKUPAJ	96	100 %

Vir: lastno delo.

Preverjanje prve hipoteze: Porabniki so nadpovprečno zaskrbljeni glede tega, kako podjetja uporabljajo njihove osebne podatke.

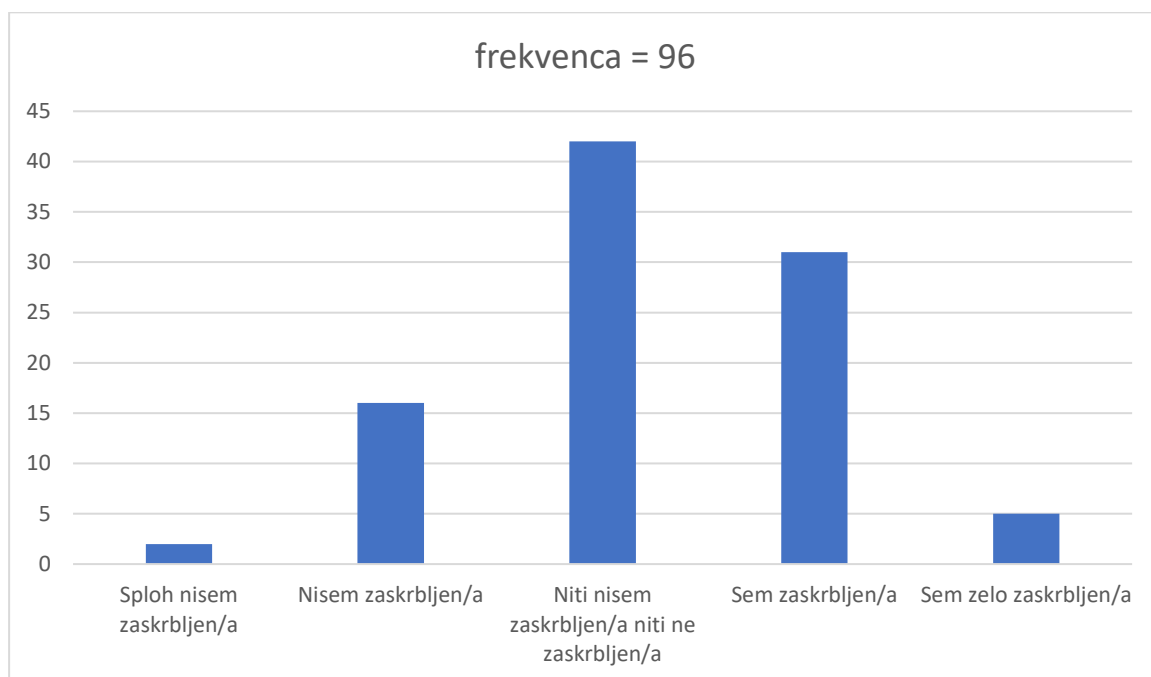
Hipoteza se nanaša na vprašanje št. 19: Do kakšne mere ste zaskrbljeni glede tega, kako podjetja uporabljajo vaše osebne podatke?

Tabela 23: Preverjanje prve hipoteze

Frekvenca veljavnih	96
Frekvenca manjkajočih	25
Mediana	3,00
Testna/hipotetična mediana	3,00
Povprečje	3,22
Wilcoxonov test	999,000
Z-vrednost	2,411
P-vrednost	,016

Vir: lastno delo.

Slika 1: Zaskrbljenost za osebne podatke



Vir: lastno delo.

Preverjanje druge hipoteze: Glavni razlog za spletni nakup pri porabnikih je časovni prihranek.

Hipoteza se nanaša na vprašanje št. 8: Zaradi katerih dejavnikov se po navadi raje odločite za izbiro spletnega nakupa namesto fizičnega nakupa?

Tabela 24: Preverjanje druge hipoteze

		Frekvenca	Delež (%)
Časovni prihranek	Ni izbran	31	32,3
	Izbran	65	67,7
	Skupaj	96	100,00
Finančni prihranek	Ni izbran	62	64,6
	Izbran	34	35,4
	Skupaj	96	100,00
Širši izbor izdelkov	Ni izbran	41	42,7
	Izbran	55	57,3
	Skupaj	96	100,00
Udobje	Ni izbran	49	51,0
	Izbran	47	49,0
	Skupaj	96	100,00
Izogib gneči	Ni izbran	45	46,9
	Izbran	51	53,1
	Skupaj	96	100,00

Lažja cenovna primerjava	Ni izbran	61	63,5
	Izbran	35	36,5
	Skupaj	96	100,00
Spletne ocene in mnenja kupcev	Ni izbran	71	74
	Izbran	25	26
	Skupaj	96	100,00
Drugo	Ni izbran	90	93,8
	Izbran	6	6,3
	Skupaj	96	100,00

Vir: lastno delo.

Tabela 25: Hi-kvadrat test

	Izbire
Hi-kvadrat	61,925 ^a
df	7
P-vrednost	,000

Vir: lastno delo.

Preverjanje tretje hipoteze: Večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov.

Hipoteza se nanaša na vprašanje št. 16: Katere izmed ukrepov uporabljate za boljšo zaščito vaših osebnih podatkov pri spletnem nakupovanju?

Tabela 26: Preverjanje tretje hipoteze

	Frekvenca	Delež (%)
Ne	1	1,0
Da	95	99,0
SKUPAJ	96	100,0

Vir: lastno delo.

Tabela 27: Hi-kvadrat test

	Proaktivni ukrepi
Hi-kvadrat	92,042 ^a
df	1
P-vrednost	,000

Vir: lastno delo.

Preverjanje četrte hipoteze: Večina porabnikov vseh starosti pri spletnem nakupovanju sprejema proaktivne ukrepe za zaščito svojih podatkov.

Hipoteza se nanaša na vprašanje št. 1: Kako pogosto kupujete prek spleta?

Tabela 28: Preverjanje četrte hipoteze

	Frekvenca	Delež (%)
Več kot enkrat mesečno	57	47,1
Nekajkrat letno	46	38,0
Manj kot nekajkrat letno	9	7,4
Nikoli	8	6,6
Drugo	1	0,8
SKUPAJ	121	100,00

Vir: lastno delo.

Tabela 29: Hi-kvadrat test

	Pogostost
Hi-kvadrat	106,727 ^a
df	4
P-vrednost	,000

Vir: lastno delo.

Preverjanje pete hipoteze: Največ porabnikov plačilo spletnega nakupa opravi z debetno ali kreditno kartico.

Hipoteza se nanaša na vprašanje št. 3: Prosim, da za spodnje kriterije opredelite, kako pomembni so vam pri spletnem nakupovanju.

Tabela 30: Hi-kvadrat test

	Katero vrsto plačila izberete pri spletnih nakupih?
Hi-kvadrat	90,146 ^a
df	4
P-vrednost	,000

Vir: lastno delo.