UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

SINERGIJA ONLINE PRODAJE I CYBER SIGURNOSTI: STRATEGIJE, TEHNOLOGIJE I PRAKSA

Sarajevo, septembar 2024.godine KEMAL TUCAKOVIĆ

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se

IZJAVA O AUTENTIČNOSTI RADA

Ja, Kemal Tucaković, student drugog (II) ciklusa studija, broj index-a 75532-5333 na programu Menadžment, smjer Menadžment informacione tehnologije , izjavljujem da sam završni rad na temu:

Sinergija online prodaje i cyber sigurnosti: strategije, tehnologije i praksa

pod mentorstvom Kačapor dr. Kemal izradio samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predao/predala elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 10.09.2024.

Potpis studenta/studentice:

Kemal
Tucaković

SAŽETAK

Nove tehnologije kao i brzi razvoj ekonomije dovele su do ekspanzije online shopinga. Sa sve većom ekspanzijom online prodaje na raznim web shop stranicama/platformama kao što su eBay, Amazon, Alibaba, Aliexpress, Olx.ba, ASOS i sličnih, dolazi do izazova cyber sigurnosti. Kupci su svakodnevno izloženi raznim rizicima. Pod rizicima spada lažno predstavljanje artikala, netačne informacije o njima u vidu netačnih opisa, cijena i slika. Naravno, veliki izazov su prevare prilikom plaćanja i same dostave kupljenih stvari sa web shop stranica/platformi. Sva negativna iskustva štete imidžu web shop stranice/platforme što direktno utiče na povjerenje kupaca. Sa smanjenim povjerenjm dolazi do manjeg prometa na web shop stranicama/platformama što direktno smanjuje obim prodaje. Ovaj završni rad ima za cilj da istraži sve rizike s kojima se kupci susreću prilikom online web kupovine. Cilj rada jeste istražiti šta to utiče na povjerenje kupaca i šta utiče na odluku o kupovini na online web shop stranicama/platformama. U teoretskom okviru rad će obraditi e-commerce i rizike prilikom online kupovine kao i uticaj cyber sigurnosti na prodaju. Istraživanje je provedeno putem online ankete u kojoj je ukupno učestvovalo 436 učesnika. Na osnovu rezultata zaključeno je da na povjerenje i odluku o kupovini utiče prethodno iskustvo, izgled stranice, predstavljanje atikala, informacije o artiklima, sigurnost prilikom plaćanja kao i socijalni uticaj društva. Važno je napomenuti da istraživanje ne pokriva sve aspekte koji utiču na povjerenje te iduća istraživanja se trebaju baviti i tim aspektima.

Ključne riječi: online prodaja, cyber sigurnost, web shop stranice/platforme.

ABSTRACT

New technologies and rapid development have led to the expansion of online shopping. With the increasing expansion of online sales on various web shop sites/platforms such as eBay, Amazon, Alibaba, Aliexpress, Olx.ba, ASOS, and similar, challenges related to cyber security have arisen. Customers are exposed to various risks on a daily basis. These risks include the misrepresentation of items, inaccurate information about items in terms of incorrect descriptions, prices, and images. Naturally, major challenges include fraud during payment and the delivery of purchased items from web shop sites/platforms. All negative experiences damage the image of the web shop site/platform, which directly affects customer trust. With reduced trust, there is a decrease in traffic on web shop sites/platforms, which directly reduces sales volume. This thesis aims to explore all the risks that customers face when shopping online. The goal of the thesis is to investigate what influences customer trust and what impacts the decision to purchase on online web shop sites/platforms. In the theoretical framework, the thesis will address e-commerce and the risks associated with online shopping, as well as the impact of cyber security on sales. The research was conducted through an online survey, in which a total of 436 participants took part. Based on the results, it was concluded that trust and the decision to purchase are influenced by previous experience, the appearance of the site, the presentation of items, information about the items, payment security, as well as the social influence of the community. It is important to note that the research does not cover all aspects that influence trust, and future research should also address these aspects.

Keywords: online sales, cyber security, web shop sites/platforms.

SADRŽAJ

SAŽETAK ..... **II**

ABSTRACT ..... **II**

1. UVOD **1**

1.1 Obrazloženje teme i pregled literature **1**

1.2 Problem istraživanja **4**

1.3 Svrha istraživanja **4**

1.4 Istraživačka pitanja i hipoteze **4**

1.5 Ciljevi istraživanja **6**

1.6 Metodologija **6**

2. TEORIJSKI OKVIR **6**

2.1 E-COMMERCE **6**

2.2 RIZICI ONLINE TRGOVINE **13**

2.2.1 Privatnost podataka 15

2.2.1.1 Primjeri primjene i zaštite osobnih podataka *18*

2.2.1.2 Privatnost podataka na primjeru Fitbit *18*

2.2.2 Sigurnost korisnika 19

2.2.3 Zaštita sigurnosti 19

3. UTJECAJ IT SIGURNOSTI NA PRODAJU **20**

3.1 Uspostavljanje sigurnosti u e-commerceu **22**

3.2 Menadžment i sistemi sigurnosti **24**

3.3 Stavovi korisnika **28**

3.4 Primjer Amazon **32**

4. ISTRAŽIVANJE **32**

4.1 Metodologija **32**

4.2 Rezultati istraživanja **32**

4.3 Diskusija **41**

4.3.1 Analiza Istraživačkih pitanja 42

4.3.2 Analiza Hipoteza 49
5. ZAKLJUČAK 53
5.1 Naučni doprinos 54
5.2 Praktični doprinos 54
5.3 Ograničenja i preporuke za buduća istraživanja 55
REFERENCE 56

POPIS SLIKA:

Slika 1. - Model 1 5
Slika 2. - Model 2 5
Slika 3 - Efekat društvenog uticaja na povjerenje 45
Slika 4. - Uticaj informacijskog dizajna na povjerenje kupaca 46
Slika 5. - Uticaj vizuelnog izgleda na povjerenje kupaca 47
Slika 6. - Uticaj informacijskog dizajna na povjerenje kupaca 49
Slika 7. - Uticaj vizuelnog izgleda na povjerenje kupaca 50
Slika 8. - Uticaj prethodnog iskustva na povjerenje kupaca 50
Slika 9. - Uticaj svijesti o privatnosti na povjerenje kupaca 51
Slika 10. - Uticaj informacijskog dizajna na odluku o kupovini 51
Slika 11. - Uticaj vizuelnog izgleda na odluku o kupovini 52
Slika 12. - Uticaj prethodnog iskustva na odluku o kupovini 53

POPIS GRAFIKONA:

Grafikon 1- E-commerce prodaja 7
Grafikon 2 - Povezanost povjerenja, rizika, privatnosti i sigurnosti 11
Grafikon 3- Grafikon 3. - Ulaganje u cyber sigurnost 27
Grafikon 4. - Spol ispitanika 33
Grafikon 5 - Starosne skupine ispitanika 34
Grafikon 6. - Visina mjesečnih primanja ispitanika 35
Grafikon 7. - Nivo obrazovanja ispitanika 35
Grafikon 8. - Ranije iskustvo sa online kupovinom 36
Grafikon 9. - Web platforme koje ispitanici poznaju 37
Grafikon 10. - Buduća namjera kupovine 41

POPIS TABELA:

Tabela 1. - Opća pitanja 36

Tabela 2. - Set pitanja o Web shop stranicama/platformama 37
Tabela 3. - Povjerenje i privatne informacije 38
Tabela 4. - Prethodno iskustvo 39
Tabela 5. - Društveni uticaj 40

POPIS PRILOGA:

Prilog 1. - Anketa.....1

POPIS SKRAĆENICA:

FAQ – često postavljana pitanaj (engl. frequently asked question)

IoT - Internet of Things

SSL - Secure Socket Layer

1. UVOD

1.1 Obrazloženje teme i pregled literature

Sa sve većim porastom online tržišta, javljaju se sve veći problemi i izazovi u polju sigurnosti i samim tim postavlja se pitanje kako se sigurnost u online okruženju odražava na odluku o kupovini kod kupaca, prodaju i uspješnost kompanije.

Informacione tehnologije predstavljaju priliku za poboljšanu segmentaciju tržišta i ciljani marketing, ali se zajedno s tim javljaju i etička pitanja koja se tiču privatnosti korisnika – jer obično primjena ovih tehnologija zadire u privatnost potrošača (Foxman i Kilcoyne, 1993).

IT tehnologije imaju brojne prednosti poput pristupa velikim podacima ili poboljšanog upravljanja korisničkim iskustvom, ali one također izazivaju i zabrinutost koja se najčešće vezuje uz sigurnost informacija korisnika i potencijalne rizike u pogledu privatnosti. Ovi posredni efekti tehnologije naknadno utiču na zadovoljstvo i lojalnost kupaca, dobrobit zaposlenih, profitabilnost firme i ekosistem u kojem se provode marketinške aktivnosti firme. Na osnovu svega prethodno pomenutog, moguće je zaključiti da kompanije moraju pažljivo razvijati i implementirati korake za prikupljanje podataka među kupcima, zaposlenima i partnerima, iskoristiti prednosti tehnologije i minimizirati rizike za usmjeravanje svojih procesa donošenja odluka (Grewal *et al.*, 2019).

Brza evolucija tehnologije i informatike dovele su do procvata e-trgovine. Smanjenje troškova rada, povećanje brzine transakcija i jednostavnost postizanja globalnog dosega kupaca i dobavljača doprinijeli su razvoju e-trgovine. Mnogo je sigurnosnih problema koji se tiču izloženosti, ali i valjanosti podataka u prenosu Padmannavar (2011).

Tržište je mjesto na kojem se stranke nalaze kako bi ostvarile razmjenu dobara i usluga. Uključene strane su obično kupci i prodavci. Tržište može biti fizičko (klasično, u maloprodajnim objektima) ili virtualno (online tržište). Tržišna transakcija može uključivati robu, usluge, informacije, valutu ili bilo koju kombinaciju koja prelazi s jedne strane na drugu. Internetske prodavnice kao što su Amazon i eBay primjeri su tržišta na kojima se transakcije mogu odvijati u potpunosti online, a uključene strane se nikada fizički ne povezuju (Kenton, 2023).

Najviše pažnje se posvećuje etičkim dilemama koje se tiču privatnosti i sigurnosti podataka korisnika. Razvoj interneta i društvenih mreža dodatno su potaknuli praćenje privatnih podataka, zbog čega se javlja pitanje u kojoj mjeri je prikladno koristiti podatke o korisnicima i da li je dozvoljeno koristiti dobijene podatke kako bi se ostvario profit. Informacione tehnologije dovele su do opasnosti od ugrožavanja komunikacijske privatnosti, zbog čega se razvio concept e-privatnosti koji osigurava zaštitu ličnih podataka koji su povezani s komunikacijom putem društvenih mreža (Rauš, 2019).

Kultura, demografija, ekonomija, tehnologija i lična psihologija glavni su faktori koji određuju da li će se osoba odlučiti za online kupovinu ili ne. Glavni pokretači online kupovine su impulsivno ponašanje pri kupovini, svijest o vrijednosti, rizik, lokalna kupovina, uživanje u kupovini i uživanje u pregledavanju putem sveobuhvatnog modela ponašanja potrošača prilikom kupovine na mreži. Također, noviji trend je i naklonost prema "zelenim brendovima", što podrazumijeva zeleno percipirani kvalitet, zelena percipirana vrijednost, zeleni percipirani rizik, uštеđeni troškovi informacija i namjere kupovine prema teoriji uočenog rizika. Na ponašanje potrošača prilikom online kupovine utječe i percepcija imidža trgovine, imidž cijene robne marke trgovine, svijest o vrijednosti i stav o brendu trgovine (Wang *et al.*, 2020).

Online korisnici su gotovo uvijek zabrinuti za vlastite podatke koje ostavljaju na internetu. Mediji su dali brojne razloge za zabrinutost, kao što je naprimjer curenje privatnosti i sigurnosti, postojanje mogućnosti za prijevarne radnje kako bi se stvorile prepreke i poteškoće za potrošače prilikom kupovine putem interneta i slično. Povjerenje potrošača u online trgovinu najvjerovatnije će biti pojačano percepcijom privatnosti i sigurnosti, a ranije studije su već potvrdile da na povjerenje potrošača u online trgovinu povoljno utječe percipirani nivo privatnosti. Autori smatraju da je percepcija rizika potrošača povezana s izlaganjem ličnih podataka na mreži, te da se percipirani rizik smanjuje ukoliko je omogućena zaštita privatnosti na web stranici, koja podstiče online transakcije povećavanjem percipirane pouzdanosti web stranice. Osim toga, zaštita privatnosti potrošača povezana je sa mogućnošću kontrole da li će informacije biti otkrivene u tržišnim transakcijama i garantuje korisnicima da neće doći do nezakonitog dostavljanja informacija trećim stranama (Tran i Nguyen, 2022).

Herley (2008) navodi da su korisnici često nemotivirani u pogledu sigurnosnih pitanja, te da odabiru slabe lozinke, zanemaruju sigurnosna upozorenja i nisu svjesni grešaka u certifikatima. Autor navodi da stranice savjetuju korisnicima da se zaštite od direktnih troškova napada, ali ih opterećuje u smislu napora koji je potrebno uložiti kako bi se ta sigurnost uspostavila. Većina sigurnosnih savjeta korisnicima jednostavno nudi loš kompromis između troškova i koristi, stoga ih korisnici odbijaju.

Pandey i Parmar (2019) istraživali su faktore koji utječu na ponašanje potrošača prilikom online kupovine, a rezultati ukazuju na to da je ponašanje potrošača u online kupovini određeno sljedećim faktorima: demografski faktori, društveni faktori, iskustvo s online kupovinom, znanje o korištenju interneta i kompjutera, dizajn web stranice, društveni mediji, faktori situacije, uvjeti za olakšavanje, proizvod karakteristike, šema promocije prodaje, mogućnost plaćanja, isporuka robe i postprodajne usluge igraju važnu ulogu u online kupovini. Neki od pojmova koje je bitno spomenuti, a utiču na faktore ponašanja su i Vizualni dizajn web stranice. Ovo uključuje korištenje grafike, boja, slika, animacija, oblika, veličine, stila fonta i zabave (Kevin Lu, 2022.). Informacijski dizajn web stranice odnosi se na organizaciju i logičko predstavljanje informacija na web stranici. Istraživanja koja proučavaju karakteristike online prodavaca često naglašavaju značaj dizajna informacija i

kvaliteta koji se odnosi na proizvode ili usluge (Kevin Lu, 2022), kao i Dizajn navigacije web stranice odnosi se na obrasce koji se koriste da pomognu posjetiteljima web stranice da se kreću kroz stranice web stranice i dobiju povezane informacije za završetak zadatka kupovine. Ovo uključuje, na primjer, broj padajućih menija i broj podmenija na stranicama web stranice (Kevin Lu, 2022).

Praćenje prijetnji cyber sigurnosti i usklađivanje sa zakonskim regulativama nije jednostavno. Mnoge kompanije angažuju podršku savjetnika kako bi bolje razumjeli stanje cyber sigurnosti svoje kompanije i stepen usklađenosti s normama, kao i kako bi primijenili najbolje prakse i nastavili se kretati ka poslovnim ciljevima uprkos cyber rizicima. Savjetnici mogu pomoći menadžerima da predvide rizike, prilagode se na promjenjivo okruženje i napredak tehnologije i inovacije, sve u svrhu stjecanja konkurentske prednosti bez slabljenja sigurnosti na njihovim web stranicama. Vodeće organizacije traže tačnu procjenu situacije koja će im omogućiti razvijanje planova za bolje upravljanje rizikom, usklađenost i upravljanje, a te procjene uključuju: kvantifikaciju rizika, identificiranje sigurnosnog rizika treće strane, testiranje penetracije kako bi se pronašle slabosti sopstvenog sistema, te simulaciju cyber provala kojima se može testirati spremnost osoblja za takve napade. Iskustva sa cyber zaštitom mogu pomoći organizacijama da procijene nedostatke u njihovom planu odgovora na incidente, te da kritički procijene nivo sigurnosti u organizaciji. Ova vrsta sigurnosne introspekcije može biti od velike koristi. Sigurnost je stalni izazov, a savjetnici mogu obezbijediti kontinuirano praćenje bezbjednosti, upravljanje i obuku koja će uposlenicima i organizaciji pomoći da održe jaku sigurnost i držanje usklađenosti, njegovanje sigurnosne kulture, pomoć u rješavanju novih prijetnji i prilagodbu sigurnosti novim izazovima (IBM Security, 2020).

Menadžeri su svjesni da zadovoljstvo kupaca igra ključnu ulogu u uspješnoj poslovnoj strategiji. Kako bi zadovoljstvo kupaca bilo ostvareno, potrebno je znati na koji način upravljati tim zadovoljstvom i napore usmjeriti na povećanje zadovoljstva korisnika, pa tako i do povećanja prodaje u trgovini (Gómez, McLaughlin i Wittink, 2004).

Internet trgovci mogu usvojiti različite strategije kako bi uvjerili one koji oklijevaju da ipak obave kupovinu putem interneta. Online trgovine trebaju obratiti pažnju na kvalitet proizvoda, raznolikost, dizajn i brendove koje nudi. Prvenstveno je potrebno poboljšati kvalitet proizvoda kako bi stvorilo povjerenje potrošača. To je moguće ostvariti pružanjem potpunih informacija o historiji prodavača i proizvoda. Također, menadžeri mogu usvojiti marketinške strategije kao što je prilagođena i sigurna web stranica, koja može poboljšati kupovno iskustvo kupaca i pojednostaviti pretraživanje proizvoda i pravilan sistem navigacije na web stranici. Iskustvo korisnika moguće je poboljšati dodavanjem više slika, video zapisa proizvoda i trodimenzionalnih (3D) slika koje će dodatno pomoći u procesu donošenja odluka. Kupci se mogu osjećati sigurnije ukoliko online trgovci osiguraju sigurnost plaćanja nudeći brojne opcije plaćanja kao što su pouzećem, dostava nakon pregleda, Google Pay ili slično (Daroch, Nagrath i Gupta, 2021).

1.2 Problem istraživanja

Nakon obrazloženja i pregleda literature možemo reći da problem istraživanja ukazuje da kupci prilikom online kupovine na e-commerce stranicama se svakodnevno susreću sa nizom opasnosti koji prijete iskustvu kupovine i narušavanju povjerenja kupaca. Narušeno povjerenje kupaca u online kupovini dovodi do smanjenja obima kupovine putem e-commerce web shopova, a smanjenje prometa na e-commerce stranicama utiče na obim prodaje. U radu istražujemo na koji način kupci doživljavaju cyber sigurnost, kako to utiče na povjerenje i kako u krajnosti utiče na donošenje odluke o kupovini.

1.3 Svrha istraživanja

Ovo istraživanje istraživalo je sve rizike s kojima se kupci susreću na internetu sa ciljem da se analizira kako cyber sigurnost utiče na donošenje odluke o kupovini, a u krajnosti i na prodaju. Istraživanje je analiziralo direktnu vezu između cyber sigurnosti i povjerenja, tj. kako cyber sigurnost utiče na povjerenje kupaca. Istraživalo se šta utiče na ponašanje kupaca na internetu, kako oni shvataju cyber sigurnost, koliko je presudna u kupovini i kako sve to utiče na donošenje odluke o kupovini. Istraživali su se i tehnički aspekti sigurnosti na web stranicama koji podižu nivo zaštite kupaca i povećavaju njihovo povjerenje.

1.4 Istraživačka pitanja i hipoteze

Rad tretira nekoliko istraživačkih pitanja na koje će se fokusirati tokom istraživanja:

1. Sa kojim se prijetnjama suočavaju kupci kada se radi o web shopovima?
2. Koji su faktori koji sputavaju potrošače da obave online kupovinu?
3. Koje su vrste rizika e-kupovine?
4. Koji faktori na web shopovima jačaju povjerenja kupaca?
5. Na koji način društveni uticaj na kupca utiče na povjerenje?
6. Koja načela privatnosti trebaju poštovati vlasnici web shopova kako bi povećali povjerenje kupaca?
7. Na koji način izgled i struktura web stranice utiče na povjerenje kupaca?
8. Koje tehnologije web shopovi trebaju primjenjivati za zaštitu podataka?
9. S kojim metodama je moguće utjecati na poboljšanje sigurnosti i prodaje?
10. Koje tehničke karakteristike treba zadovoljiti web shop kako bi bio u skladu sa sigurnosnim standardima?

Hipoteze:

H1.a Informacijski dizajn web stranice ima uticaj na povjerenje kupaca.

H1.b Vizuelni izgled web stranice ima uticaj na povjerenje kupaca.

H1.c Prethodno iskustvo u online shopingu utiče na povjerenje kupaca

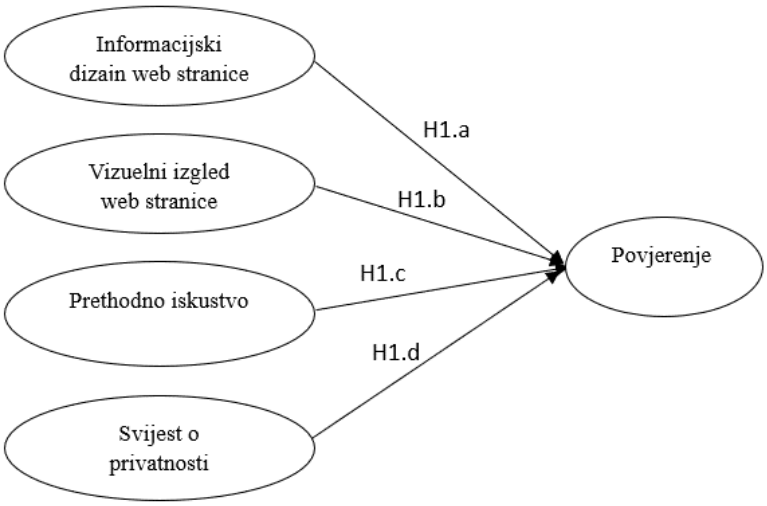
H1.d Svijest o privatnosti utiče na povjerenje kupaca.

H2.a Informacijski dizajn web stranice utiče na donošenju odluke o kupovini.

H2.b Vizuelni izgled web stranice utiče na donošenju odluke o kupovini.

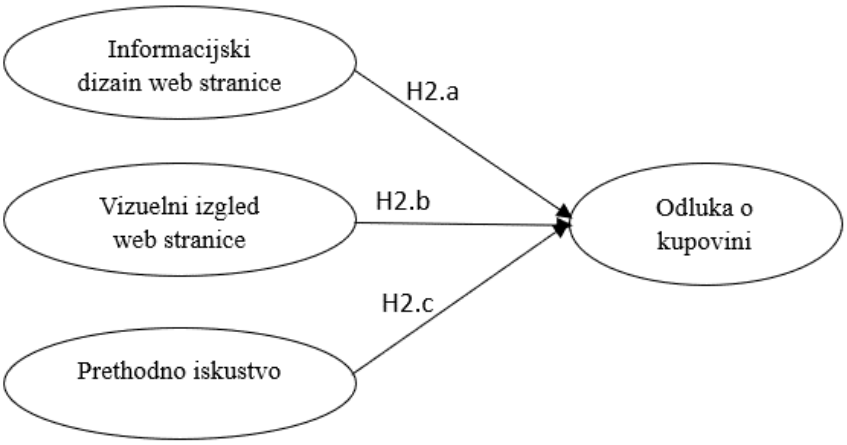
H2.c Prethodno iskustvo utiče na odluku o kupovini

Slika 1. - Model 1



Izvor: kreacija autora

Slika 2. - Model 2



Izvor: kreacija autora

1.5 Ciljevi istraživanja

Sam cilj rada je pokazati percepciju kupaca o cyber sigurnosti i na koji način, kod kupca, osjećaj sigurnosti utiče na kupovinu. Na taj način cilj je pokazati kako cyber sigurnost direktno utiče na donošenje odluke o kupovini. Cilj je pokazati percepciju kupaca u online kupovini, kako predstavljanje stranice utiče na povjerenje, kao i na donošenje odluke o kupovini. Još jedan cilj je da se pokaže koliko shvatanje i svjesnost menadžmenta na cyber sigurnost utiče na samu sigurnost kupaca, a i samim tim uspješnost prodaje sa krajnim ciljem povećanja profita za svoju kompaniju.

1.6 Metodologija

U prvom koraku vršili smo detaljni pregled literature. Literatura se preuzela iz baza podataka kojim Ekonomski fakultet Univerziteta u Sarajevu ima pristup, tj. literatura se preuzela sa Web of Sceince i Google Scholar. Na osnovu pregledanih radova, uradit će se teroetski dio koji će obraditi sve bitne aspekete teorije iz oblasti web trgovine, cyber sigurnosti i prodaje.

Nakon urađenog teoretskog pregleda literature i postavljanja hipoteza, a kako bismo ponudili odgovore na postavljena pitanja, u ovom radu proveden je elektronski anketni upitnik zbog ograničenih resursa za ispitivanje uživo i lahke dostupnosti ispitanika elektronskoj anketi. Anketa je provedena na ispitanicima (kupcima) raznih grupa potencijalnih potrošača. U prvom dijelu ankete provedenasu pitanja koja se tiču osnovnih i demografskih podataka ispitanika poput dobi, spola, obrazovanja i radnog mjesta. Drugi dio ankete bavio se iskustvima kupaca na online platformama i njihovim stavovima vezanim za osjećaj sigurnosti i kako njihovo poimanje cyber sigurnosti utiče direktno na njihovu odluku o kupovini. Za provođenja istraživanja koristi se multipla regresiona analiza te će biti predstavljeni rezultati analize iz koje smo izvesli zaključak o direktnoj vezi između cyber sigurnosti i online kupovine, samim tim i uticaja na prodaju iz ugla kupaca.

2. TEORIJSKI OKVIR

2.1 E-COMMERCE

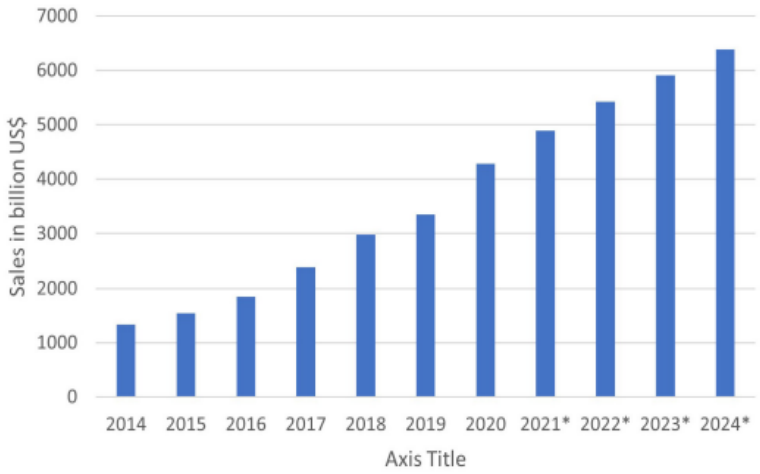
E-trgovina je trgovina koja se ostvaruje pomoću telekomunikacijskih mreža za automatizaciju poslovnih odnosa i toka rada. Može se odnositi i na razmjenu organizacijskih podataka, očuvanje poslovnih odnosa i vođenje operativnih transakcija putem za to dizajniranih telekomunikacijskih sistema (Taher, 2021).

E-commerce podrazumijeva bilo koji oblik poslovanja ili transakcije koja se provodi elektronskim putem, a Joshi i Dumbre (2017). navode sljedeće oblike e-commercea:

- Online kupovine – u kojoj prodavači stvaraju "izloge" koji su online ekvivalenti maloprodajni, mjestima, a kupci kupovinu obavljaju online.
- Elektronska plaćanja – neophodna su kada se radi o online kupovini. Ona smanjuju neučinkovitost povezanu s pisanjem i slanjem čekova, te otklanjaju mnoga sigurnosna pitanja.
- Internetske aukcije – dostupne su velikom broju kupaca i prodavača. Mnogi kupci smatraju aukcijske kupovine mnogo zanimljivijim od klasične kupovine.

E-commerce omogućava kupcima lahkoću da nešto kupe, a također je postala jedan od moćnih agenata za transformaciju poslovanja. Zbog brzog rasta, firme su unaprijedile svoje mreže, poslovanje itd., kako bi pružile bolje usluge dobavljačima i kupcima. Tehnologija e-trgovine omogućila je jučerašnje nemoguće ciljeve poslovnim firmama pružajući im mnoge mogućnosti da pronađu i osvoje nova tržišta i privuku kupce izvan granica. Iako e-trgovina ima mnoge prednosti za poslovne firme i kupce, nemoguće je bez sofisticiranog pristupa sigurnosti. Važno je napomenuti da je u 2020. godini prodaja e-trgovine iznosila 4,28 triliona dolara, a očekuje se da će dostići 5,4 triliona dolara. Slika ispod prikazuje statistiku e-trgovine od 2014. do 2024. Godine (Liu *et al.*,2022).

Grafikon 1- E-commerce prodaja



Izvor: Liu et al.,2022.

Internet i pametni telefoni postali su učinkovito sredstvo kojim različiti sektori mogu komunicirati i razmjenjivati usluge. Opskrbni lanac je tanak i inteligentan jer se digitalne mreže mogu brzo povezati s kupcima, što dovodi do porasta tržišta, koje prati tehnološki napredak. Online plaćanje omogućava e-trgovinu, a glavne varijable online transakcija su načini plaćanja koji uključuju kreditne kartice, debitne kartice, kupovinu putem internetskog bankarstva i prijenosi elektronskih sredstava. Analitika je još jedna komponenta online trgovine, a predstavlja empirijski način pretvaranja podataka u inteligenciju donošenja odluka. Ona omogućava organizacijama da jednostavnije prikupe, urede, pregledaju i odgovore na zahtjeve korisnika. Ogroman porast količine podataka primorao je organizacije

da se oslone na analitiku kako bi dobile više informacija o ponašanju kupaca. Društvene mreže služe kako bi organizacije reklamirale svoje proizvode i usluge, a društveno umrežavanje kritičnije je jer podsjeća klijente na različite ponude. Još jedan primjer e-commercea su i autonomni automobili i 3D ispis, koji predstavlja dodatnu "manufacturing" tehniku (Jain, Malivya i Arya, 2021).

Kultura, demografija, ekonomija, tehnologija i lična psihologija glavni su faktori koji određuju da li će se osoba odlučiti za online kupovinu ili ne. Glavni pokretači online kupovine su impulsivno ponašanje pri kupovini, svijest o vrijednosti, rizik, lokalna kupovina, uživanje u kupovini i uživanje u pregledavanju putem sveobuhvatnog modela ponašanja potrošača prilikom kupovine na mreži. Također, noviji trend je i naklonost prema "zelenim brendovima", što podrazumijeva zeleno percipirani kvalitet, zelena percipirana vrijednost, zeleni percipirani rizik, uštađeni troškovi informacija i namjere kupovine prema teoriji uočenog rizika. Na ponašanje potrošača prilikom online kupovine utječe i percepcija imidža trgovine, imidž cijene robne marke trgovine, svijest o vrijednosti i stav o brendu trgovine (Wang *et al.*, 2020).

Svrha istraživanja koje su radili Baubonienė i Gulevičiūtė (2015) bila je sagledati faktore koji pokreću kupovinu putem interneta, kako bi se poboljšalo razumijevanje faktora koji utječu na ponašanje kupaca u online kupovini. Istraživači su analizirali prednosti kao što su sigurnost, brza dostava, usporediva cijena, praktičnost, povoljnije cijene i veći izbor, koristi koje kupci imaju od online kupovine, ali i rizike koji se javljaju na platformama za prodaju. Istraživanje je bilo usmjereno na to na koji način na online kupovinu utječu faktori kao što su dob, spol ili zanimanje. Na kraju, autori su izdvojili sljedeće faktore koji utječu na ponašanje kupaca kod online kupovine:

- Tehnološki faktori: usklađenost s najnovijim trendovima u informacijskim tehnologijama, korištenje nalaza za istraživanje znanja, sposobnost procjene ponašanja programa, učinkovit krajnji korisnik i poznavanje hardvera.
- Faktori povezani s potrošačima: stavovi prema online kupovini, promjena stavova kupaca, kultura, lojalnost, percipirani rizici, zabrinutost potrošača, jednostavnost korištenja, obrazovanje potrošača i prihod; korisnost, povjerenje, preporuke dobavljača i recenzije potrošača, dob i kupovno iskustvo potrošača.
- Faktori određivanja cijena u online trgovini
- Faktori proizvoda/usluge: dostupnost informacija o proizvodu, web stranica.

Istraživanjem je utvrđeno da se u većini slučajeva korisnici odlučuju za online kupovinu zbog praktičnosti i jednostavnosti (72%). Na takav odabir utječe povoljno plaćanje, mogućnost dobivanja tražene usluge ili proizvoda bez obzira na lokaciju, racionalno procijenjene cijene, te jednostavna mogućnost usporedbe cijene s cijenama u drugim trgovinama. Drugi faktor (59%) zbog kojeg se korisnici odlučuju za online kupovinu je atraktivna cijena, a analiza sociodemografskih obilježja ukazuje na to da je ovaj faktor važniji kod ženskog spola nego kod muškog spola (Baubonienė i Gulevičiūtė, 2015).

Prema rezultatima studije koje su sproveli Daroch, Nagrath i Gupta (2021) ukupno je šest faktora koji sputavaju potrošače da obave online kupovinu, a to su:

1. Strah od bankovnih online transakcija
2. Tradicionalna kupovina pogodnija je od kupovine putem interneta
3. Reputacija i pružene usluge
4. Iskustvo
5. Nesigurnost i nedovoljne informacije o proizvodima
6. Nedostatak povjerenja.

Istraživanjem su utvrdili da 50,5% ljudi koji imaju prihod ispod 15.000 INR (o.p. indiski rupi = 164€) mjesečno koriste web stranice za online kupovinu. Također, utvrđeno je da 30,9% ispitanika provodi manje od 5 sati sedmično na internetu, te da 30,3% provede 6-10 sati sedmično u online kupovini ili na društvenim mrežama. Većina ispitanika (97,5%) ima i pozitivna i negativna iskustva s online kupovine. Što se tiče učestalosti kupovine – utvrđeno je da je 38% ljudi obavljalo online kupovinu 2-5 puta sedmično, a 36,7% više od deset puta sedmično, a mali broj ispitanika (12%) kupovalo je samo jednom. Većina ispitanika potrošila je između 1.000 i 5.000 INR na online kupovinu, a nekolicina troši i više od 5.000 INR. Rezultati također ukazuju i na to da su ispitanici najčešće kupovali sa sljedećih stranica: amazon.com (71,5%), flipkart.com (53,2%), a manjina kupovinu obavlja preko eBaya, , makemytrip.com i myntra.com. Najčešće ljudi kupuju odjeću (46,2%), a zatim elektroniku i stvari koje su im dnevne potrebe sa platformi za online kupovinu. Ponekad kupuju knjige i kozmetiku, ili se odlučuju kupiti putne karte, kino karte, rezervacije hotela i slično.

Nalazi studije koju su proveli Al Hamli i Sobaih (2023) zasnovani su na odgovorima potrošača putem internetskih anketa u vrijeme pandemije COVID-19. Rezultati predstavljaju stavove ispitanika prema online kupovini u Saudijskoj Arabiji u vrijeme pandemije COVID-19 i ukazuju na sljedeće:

- 55,0% ispitanika obavljala je e-trgovinu jednom ili dva puta mjesečno, 20,9% više od pet puta mjesečno, dok 13,2% ispitanika nikada nije samostalno koristilo e-trgovinu,.
- Većina ispitanika bili su povremeni korisnici e-trgovine tokom pandemije.
- 47,7% ispitanika potrošilo više od 700 SAR, 20,0% onih koji su potrošili između 300 i 499 SAR (Saudiski Rial), 17,7% je potrošilo između 500 i 700 SAR , a 14,5% trošilo je manje od 300 SAR.
- Najvažniji faktori zbog kojih su se korisnici opredjeljivali za online kupovinu su sljedeći: kvalitet proizvoda (39,5%), cijena (24,5%), promocija (22,3%), povjerenje (9,1%) i vrijeme isporuke (4,5%).

Ispitivanjem je primijećena pozitivna korelacija između faktora raznolikosti proizvoda i kupovine putem interneta, te da faktor raznolikosti proizvoda ima značajan pozitivan utjecaj na online kupovno ponašanje kupaca. Dakle, veća raznovrsnost proizvoda povećava vjerovatnoću potrošača da pronađu ono što će odgovarati njihovim potrebama i

preferencijama. Sljedeći promatrani faktor bila je povoljna cijena i utvrđeno je da postoji umjerena pozitivna korelacija između povoljne cijene i online kupovine. Još neki od faktora za koje je ranije utvrđeno da su u pozitivnoj korelaciji s online kupovinom su kvaliteta dizajna web stranice, povjerenje, pogodnosti i promocija. Međutim, istraživanjem se ispostavilo da pogodnost, povjerenje i promocija nemaju utjecaja na odabir online kupovine saudijskih kupaca. Na online kupovno ponašanje kupaca utječu i rizici koji se mogu javiti u online kupovini, a ti rizici se često tiču načina plaćanja. Naposljetku, istraživanjem je utvrđeno da način plaćanja ima umjerenu pozitivnu korelaciju s online kupovinom, apreferirane opcije plaćanja su plaćanje pouzećem (Al Hamli i Sobaih, 2023).

Pandey i Parmar (2019) istraživali su faktore koji utječu na ponašanje potrošača prilikom online kupovine, a rezultati ukazuju na to da je ponašanje potrošača u online kupovini određeno sljedećim faktorima: demografski faktori, društveni faktori, iskustvo s online kupovinom, znanje o korištenju interneta i kompjutera, dizajn web stranice, društveni mediji, faktori situacije, uvjeti za olakšavanje, proizvod karakteristike, šema promocije prodaje, mogućnost plaćanja, isporuka robe i postprodajne usluge igraju važnu ulogu u online kupovini. U odnosu na ranija istraživanja, autori ovog istraživanja navode da su finansijska sigurnost, pogodnost transakcija i dizajn sajta najvažniji faktori koji utječu na zadovoljstvo korisnika.

Iako je online poslovanje veoma zastupljeno, online trgovci se još uvijek suočavaju s brojnim problemima koji se tiču ove vrste prodaje. Malo je istraživanja koja se tiču faktora koji utječu na online prodaju, a Ranganathan i Grandon (2016) su na osnovu dostupne literature i vlastitog ispitivanja sadržaja, dizajna, sigurnosti i privatnosti 487 web stranica, identificirali sljedeće faktore koji značajno utiču na online prodaju:

- Često ažuriranje web sadržaja
- Prisustvo pomagala za odlučivanje
- Pružanje informacija o firmi
- Prisustvo sekcije FAQ
- Korištenje multimedije
- Obezbjeđivanje individualnih korisničkih naloga
- Bezbjedni načini prenosa podataka
- Mogućnost obavljanja offline i online finansijskih transakcija i izjava o privatnosti.

Povjerenje, rizik, privatnost i sigurnost pojmovi su koji se proučavaju u raznim studijama koje imaju za cilj razjasniti koncepte s gledišta potrošača u e-trgovini. Pennanen, Kaapu i Paakki (2006) svojom kvalitativnom studijom predlažu koncept odnosa između prethodno pomenutih pojmova, koji može poslužiti kao osnova za dalja istraživanja:

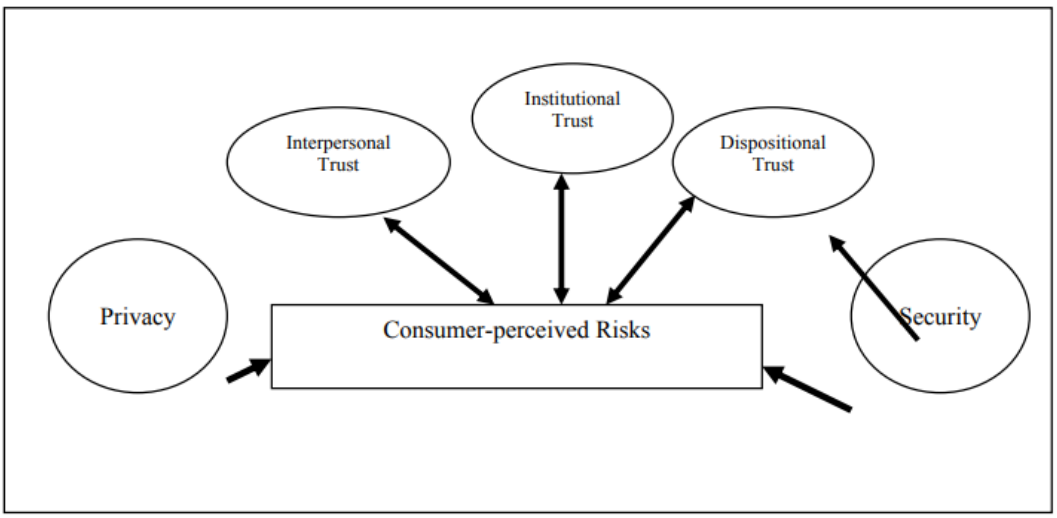
1. Povjerenje – višedimenzionalna konstrukcija koja uključuje tri elementa;
    a. institucionalno,
    b. interpersonalno i

c. dispozicijsko povjerenje.

Institucionalno povjerenje odnosi se na povjerenje pojedinca u instituciju, čemu doprinose zakoni ili tehnologija u slučaju e-trgovine.

2. Privatnost – zahtjev pojedinaca, grupa ili institucija da same određuju kada, kako, i u kojoj se mjeri informacije o njima mogu priopćiti drugima. Sa stajališta privatnosti, povjerenje se može promatrati kao očekivanja korisnika da će internetsko poslovanje pošteno postupati s njihovim informacijama i da ih neće zloupotrijebiti.
3. Rizici – brojne su prijetnje u e-trgovini, poput transakcijskih napada i zloupotrebe finansijskih i osobnih podataka.
4. Sigurnost – zaštita od prethodno pomenutih rizika i prijetnji, a treba da ispunjava sljedeća tri uslova: povjerljivost, cjelovitost i dostupnost. Na sigurnost mogu utjecati tehnički problemi, prirodne pojave, slučajne ili namjerne ljudske aktivnosti.

Grafikon 2 - Povezanost povjerenja, rizika, privatnosti i sigurnosti



Izvor: Pennanen, 2006.

Na osnovu grafika iznad možemo zaključiti da su prethodno pomenuti pojmovi povezani u koncept rizika percipiranog od strane korisnika. Autori su svojim istraživanjem ustanovili da je percepcija potrošača o pouzdanost e-prodavača povezana s percipiranim rizikom. Također je utvrđeno da percipirana sigurnost i privatnost također utječu na percepciju rizika, a tako i povjerenja. Sigurnost također može imati izravan utjecaj na povjerenje. Kako bi pomenuti koncepti bili dobro organizovani potrebno ih je dobro poznavati i to iz različitih aspekata, pogotovo u današnje vrijeme kada je tehnološka dimenzija veoma zastupljena i utječe na percipirane rizike. Koncept rizika u e-trgovini uključuje finansijsku, društvenu, psihološku, tehnološku i fizičku komponentu. Način na koji su pomenute komponente povezane s prethodno povezanim dimenzijama povjerenja, ogleda se primjerice kroz to što se privatnost smatra dimenzijom psihološkog rizika, a sigurnosti dimenzijom finansijskog

rizika. Percipirani rizici su preduvjet za uspostavljanje povjerenja, a privatnost i sigurnost su faktori koji utječu na percepciju rizika. Privatnost i sigurnost imaju neizravan učinak o povjerenju potrošača u e-trgovinu, jer potrošači percipiraju rizike povezane s tehnologijom (institucionalni aspekt) i e-prodavač (međuljudski aspekt). Model koji su ponudili Pennanen, Kaapu i Paakki (2006) sugeriše da povjerenje i rizik imaju dupleks odnosa, a da povjerenje treba posmatrati kao dinamičku konstrukciju, jer potrošač može vjerovati e-prodavatelju, ali ako nešto štetno dogodi u vezi, povjerenje bi se moglo smanjiti, a percipirani nivo rizika povećati.

Padmannavar (2011) navodi sljedeće prijetnje kada se radi o e-commerceu:

- Klijentske prijetnje – koje su obično statične do trenutka uvođenja izvršnog web sadržaja. Aktivni sadržaj se odnosi na programe koji su transparentno ugrađeni u web-stranice i na osnovu kojih stranica funkcionira. Ovi sadržaji se koriste u e-trgovini za postavljanje artikala koje se želi ponuditi korisnicima, te za računanje ukupnog iznosa fakture i slično. Budući da su moduli aktivnog sadržaja ugrađeni na web stranicama, oni mogu biti transparentni za svakoga ko posjeti tu stranicu. Ipak, moguće je ugraditi zlonamjerni aktivni sadržaj na web stranicama koji prouzrokuje štetu posjetiocima stranice. Zlonamjerni aktivni sadržaj može otkriti kreditnu karticu brojeva, korisničkih imena i lozinki koje su često pohranjeni u posebne datoteke koje se nazivaju kolačići. Zlonamjerni aktivni sadržaj isporučen putem kolačića može otkriti sadržaj datoteka na strani klijenta ili čak uništiti datoteke pohranjene na klijentskim računarima. Osim zlonamjernog aktivnog sadržaja, još jedan rizik predstavljaju i zlonamjerni dijelovi koda, kao što je:
    - trojanski konj – program koji obavlja korisnu funkciju, ali obavlja i neočekivane radnje;
    - virus – segment koda koji replicira prilaganjem kopija postojećim izvršnim datotekama.
- Prijetnje komunikacijskim kanalom – jer poruke na internetu putuju nasumičnim putem od izvornog čvora do odredišta, kroz niz posrednih računara na mreži, pri čemu je nemoguće garantovati da će svaki uključeni računar biti zaštićen i ne-neprijateljski nastrojen.
- Prijetnje povjerljivosti – prijetnje od neovlaštenog otkrivanja informacija.
- Prijetnje integritetu – postoje kada neovlaštena strana može promijeniti tok protoka informacija.
- Prijetnje dostupnosti ili prijetnja odgodom – ometanje normalne računarske obrade ili potpuno uskraćivanje iste.
- Prijetnje bazi podataka – sistemi e-trgovine pohranjuju korisničke podatke i prikupljene informacije o proizvodu iz baza podataka povezanih s web-pretraživačem. Neke baze podataka pohranjuju parove korisničko ime/lozinkama na nesiguran način, a ukoliko neko dobije autentifikaciju, onda dobivaju pristup korisnikovim informacijama.
- Hakiranje lozinki – najjednostavniji napad na sistem.

2.2 RIZICI ONLINE TRGOVINE

Brza evolucija tehnologije i informatike dovele su do procvata e-trgovine. Smanjenje troškova rada, povećanje brzine transakcija i jednostavnost postizanja globalnog dosega kupaca i dobavljača doprinijeli su razvoju e-trgovine. Mnogo je sigurnosnih problema koji se tiču izloženosti, ali i valjanosti podataka u prenosu. Padmannavar (2011) analizira načine na koje se moguće zaštiti od rizika na internet, te navodi da sigurne transakcije e-trgovine zahtijevaju web poslužitelje i preglednike koji ispunjavaju sljedeće uvjete:

1. Digitalni certifikati koje je potvrdila treća strana i kojima se potvrđuje identitet stranice.
2. Secure Socket Layer (SSL) protokol koji omogućuje enkripciju podataka. Kada se pozove SSL protokol korisnik je obaviješten i slika zatvorene brave može se pojaviti na zaslonu preglednika.

U suštini, web stranice bi trebale ispunjavati sljedeće uvjete:

1. Privatnost – čuvanje informacija od neovlaštenog pristupa.
2. Integritet – poruke se ne smiju mijenjati
3. Autentifikacija – pošiljalac i primatelj moraju dokazati svoj identitet.
4. Neporicanje – dokaz da je poruka zaista primljena.

Kaushik, Gupta i Gupta (2020) u svom radu analiziraju izazove koji se tiču online trgovine i pružaju uvid u novi model e-trgovine. Oni navode kako je korištenje interneta u porastu za prodaju, kupnju i plaćanja, što sa sobom također nosi i nove izazove u smislu definisanja zakona, ali i pravila koja se tiču sigurnosnih problema korisnika. Kada se radi o sigurnosti korisnika, predlaže se da korisnici odaberu pravilnu platformu za e-trgovinu, pri čemu je bitno držati svoju administratorsku ploču hermetički zatvorenom i imati sigurnosnu kopiju osjetljivih informacija. Autori navode sljedeće vrste rizika e-trgovine:

1. Sigurnost korisnika – potrebno je uspostaviti sigurnost na web stranici, a u tu svrhu je potreban firewall na strani poslužitelja. Pristup stanice treba biti takav da ne forsira korisnike da dijele platformu zajedno s drugim web stranicama.
2. Botovi – razlikuju se dvije vrste botova – dobri koji pomažu korisnicima stranice i loši koji pretražuju web-mjesta na cijene kao i na podatke o zalihama, nakon čega te podatke koriste kako bi promijenili cijenu, što dalje vodi padu prodaje i prihoda.
3. DdoS napadači – napadaju stranicu na način da je čine offline (neaktivnom).
4. SQL injekcija – vrsta napada u kojoj stranica traži od korisnika da prihvati zaraženi sadržaj, a nakon klika hakeri mogu ukrasti korisne informacije kupaca i tako oštetiti bazu podataka web stranice.
5. Prevara s kreditnom karticom – realna prijetnja korisnicima koji obavljaju transakcije na internetu. Kako bi dobili dobili detalje kartice, hakeri se infiltriraju u bazu podataka vezanu uz web stranicu e-trgovine koristeći se različitim softverskim programima.

Internet stvari (Internet of Things-IoT) su skup digitalnih uređaja koji su međusobno povezani i koji pružaju niz mogućnosti kompanijama koje se za njih odluče – kao naprimjer mogućnost osluškivanja potreba potrošača kako što adekvatnije zadovoljili njihove potrebe i želje. Osnovni problem kod primjene IoT-a je narušavanje sigurnosti i privatnosti potrošača (Šestak i Dobrinić, 2019).

Internet stvari omogućuju sveprisutno prikupljanje podataka ili praćenje, ali sa sobom također nosi i prijetnje privatnosti koje već sada ograničavaju uspjeh vizije Internet stvari. Prijetnje privatnosti tiču se upravljanja osobnim podacima, metoda kontrole, izbjegavanja sveprisutnog praćenja i profiliranja. Ziegeldorf, Morchon i Wehrle (2013) pručavali su problem privatnosti na internetu. Moguće je govoriti o medijskoj, teritorijalnoj, komunikacijskoj i tjelesnoj privatnosti. Uz sve veću upotrebu i elektronsku obradu ličnih podataka, privatnost informacija postala je veoma bitna u današnjem poslovanju. Privatnost u Internetu stvari je trostruko jamstvo subjektu u pogledu sljedećeg:

- svijest o rizicima privatnosti koje nameću pametne stvari i usluge koje okružuju nositelja podataka
- individualni nadzor nad prikupljanjem i obradom osobnih podataka od strane okoline Internet stvari
- svijest i kontrola naknadne upotrebe i širenja osobnih podataka

Prijetnja identifikacije trenutno je najdominantnija u fazi obrade informacija, gdje su ogromne količine informacije koncentrirane na središnjem mjestu izvan kontrole subjekta. Autori ističu sljedeće utjecaje tehnologije na privatnost:

- Tehnologija nadzornih kamera je sve više integrirana i korištena u kontekstima koji nisu povezani sa sigurnošću, npr. za analitiku i marketing. Baze podataka lica (npr. s Facebooka) postaju dostupne i za nevladine stranke poput marketinških platformi – automatska identifikacija pojedinaca sa snimaka kamere.
- Sve veća bežična povezanost i vertikalna komunikacija otvaraju mogućnosti za identifikaciju uređaja kroz uzimanje otisaka prstiju i ostalih biometrijskih uzoraka.
- Prepoznavanje govora je široko zastupljeno u mobilnim aplikacijama i već su se počele kreirati baze podataka govornih uzoraka. Ti podaci bi se mogli potencijalno koristiti za prepoznavanje i identificiranje pojedinaca, npr. od strane vlada koje traže pristup tim podacima.
- Praćenje zahtijeva identifikaciju neke vrste za vezanje kontinuirane lokalizacije na jednu osobu, što se ostvaruje putem GPS-a, internetskog prometa ili lokacije mobitela. Mnoge stvari u vezi s ovakvim praćenjem identificirane su kao kršenje privatnosti, kao npr. GPS praćenje, uhođenje, otkrivanje privatnih informacija ili općenito osjećaj nelagode zbog promatranja.
- Profiliranje predstavlja prijetnju prikupljanja informacija u svrhu kreiranja dosjea o pojedincima kako bi se zaključili interesi i povezanost s drugim profilima i podacima. Metode profiliranja uglavnom se koriste za personalizaciju u e-trgovini (npr.u

sistemima preporuka, biltenima i oglasima) ali i za internu optimizaciju na temelju demografije kupaca i interesa. Profiliranje narušava privatnost kroz neželjene oglase, društveni inžinjering, pogrešne automatske odluke i slično.

Kako bi ublažile zabrinutost zbog privatnosti, online prodavači nastoje primjenjivati intervencije kako bi ohrabrile korisnike da kupuju više na mreži. Rezultati istraživanja ukazuju na mješovite efekate preporuka i popusta na namjeru kupovine. Iako preporuke nisu pojačale efekte inhibitora rizika, one su pojačale efekte pokretača na namjeru kupovine putem interneta. Najčešće se radi o sljedećim intervencijama (Venkatesh *et al.*, 2021).:

- preporuke koje pomažu kupcima da odaberu pravi proizvod, bilo na osnovu historijskih korelacija kupovine ili na osnovu recenzija
- popusti koji povećavaju vrijednost proizvoda.

Fortes i Rita (2016) sproveli su istraživanje koje je imalo za cilj analizirati kako zabrinutost za online privatnost utječe na namjeru potrošača da kupuje putem interneta. Istraživanje predlaže da se utjecaj zabrinutosti za privatnost može povezati s teorijama povjerenja i rizika, teorijom planiranog ponašanja i modelom prihvatanja tehnologije. Istraživanje je sprovedeno online anketiranjem 900 ispitanika, a rezultati ukazuju na sljedeće:

- Zaštita privatnosti informacija u online kupovini privukla je pažnju i vlasti, tačnije Federalne trgovinske komisije (FTC) u Sjedinjenim Američkim Državama. Ova je organizacija razvila set smjernica pod nazivom Fair Information Practices, koji uključuje pravila o prikupljanju informacija od strane prodavača, ispravljanju grešaka u prikupljenim informacijama, komuniciranju potrošača o korištenju njihovih informacija u druge svrhe osim početne i sprječavanju neovlaštenih pristup informacijama.
- Utvrđeno je da prodavci moraju potrošačima pružiti kontrolu nad svim aspektima koji se odnose na prikupljanje i korištenje informacija.
- Tri su dimenzije zabrinutosti za privatnost na mreži: zabrinutost za kontrolu, kratkoročnu vezu i dugoročnu vezu. Kontrola se odnosi na stepen kontrole korisnika nad prikupljanjem i upotrebom ličnih podataka. Dimenzija kratkoročnog odnosa tiče se brige pojedinca za vrstu informacija koje se pružaju na mreži, kao i za pandan koji se prima u razmjenu tih informacija, a dugoročni odnos sugerira da potrošač i organizacija već imaju uspostavljen odnos, ukazujući na nivo zabrinutosti pojedinca koji proizilazi iz online komunikacije i interakcije s organizacijom.

2.2.1 Privatnost podataka

Vlade i korporacije prikupljaju, pohranjuju i analiziraju ogromnu količinu podataka koja se kreće na digitalnim platformama, često je to bez znanja i pristanka korisnika. Na temelju tih podataka donose zaključke o korisnicima – sa kojim prijedlozima bi se mogli slagati ili ne. Edward Snowden govorio je o načinima na koji agencije koriste podatke o klijentima. Prema

njegovim izvještajima, NSA je prikupljala mobilne pozive Amerikanaca, posjedujući izgovorene riječi, brojeve dviju strana, datum, vrijeme i trajanje poziva. Prikupljeni podaci zalazili su u intimu korisnika – njihove odnose s drugima, stavove i vrijednosti, kao i svakodnevna dešavanja u njihovom dešavanju. Na osnovu prethodno pomenutog, Sveučilište Stanford sprovelo je istraživanje s volonterima, prisluškujući njihove razgovore. Neke od informacija koje su prikupljene u tom istraživanju su primjerice (Schneier, 2017).:

- Sudionik A – komunicirao je s više lokalnih neuroloških grupa, specijaliziranom ljekarnom, rijetkim stanjem usluga za liječenje recidiva multiple skleroze.
- Sudionik B – dugo je razgovarao s kardiolozima u velikom medicinskom centru, kratko je razgovarao s medicinskim laboratorijem, primao pozive iz ljekarne i upućivao kratke pozive na kućnu telefonsku liniju za prijavu medicinskog uređaja koji se koristi pratiti srčane aritmije.
- Sudionik C – nekoliko puta je nazvao trgovinu vatrenim oružjem, a također je dugo razgovarao sa korisničkom službom za proizvođača vatrenog oružja koji proizvodi liniju AR.
- Sudionik D – je u rasponu od tri sedmice kontaktirao trgovinu za kućne popravke, bravare, trgovca hidroponima.
- Sudionica E – većinom je razgovarala sa svojom sestrom.

Samo na osnovu toka razgovora, naučnici su ustanovili da se radi o osobi oboljeloj od multiple skleroze, žrtvi srčanog udara, vlasniku poluautomatskog oružja, kućnom uzgajivaču marihuane i osobi koja je imala pobačaj. Pomenuto istraživanje je sprovedeno kako bi se pojasnilo koliko informacija o samom sebi ljudi ostavljaju online. Podaci pretraživanja weba izvor su intimnih informacija koje se mogu koristiti za nadziranje korisnika. Web pretraživači uvijek znaju ono o čemu korisnik razmišlja, šta ga muči i šta želi, jer ljudi uvijek jasno navode svoje misli pretraživačima koji pamte te pretrage.

O pravu na privatnost govorilo se još krajem osamnaestog stoljeća kao „pravu da se ljudi puste na miru“. Razvoj tehnologije doprinosi i nešto složenijem pristupu ovom problemu, pogotovo zbog toga što su nove tehnologije doprinijele ekonomskim promjenama i transformaciji društvenih institucija. Propisi o zaštiti podataka u EU postavljaju glavna načela privatnosti, a to su (Guarda, 2008).:

- Poštena i zakonita obrada – prikupljanje i obrada osobnih podataka neće bezrazložno zadirati u privatnost ispitanika niti neopravdano ometati njihovu autonomiju i integritet, te će biti usaglašena s cjelokupnim pravnim okvirom.
- Saglasnost – osobni podaci će se prikupljati i obrađivati samo ako je nositelj podataka dao izričitu saglasnost za njihovu obradu.
- Specifikacija svrhe – osobni podaci će se prikupljati za određene, zakonite i legitimne svrhe i na načine koji su u skladu sa svrhom prikupljanja podataka.
- Minimalnost – prikupljanje i obrada osobnih podataka bit će ograničena na minimum potreban za postizanje određene svrhe. Osim toga, minimalnost se odnosi na to da

podaci budu čuvani samo izvjestan vremenski period, onoliko koliko je potrebno za postizanje određenog cilja.

- Minimalno otkrivanje osobnih podataka trećim stranama, koje će biti ograničeno i primjenjivati se samo pod određenim uvjetima.
- Kvaliteta informacija – osobni podaci moraju biti tačni, relevantni i potpuni s obzirom na svrhe za koje se prikupljaju i obrađuju.
- Kontrola subjekta podataka – subjekat će moći provjeriti i utjecati na obradu njegovih osobnih podataka.
- Osjetljivost – budući da se radi o podacima koji su izuzetno osjetljivi za nositelja podataka, potrebno je primijeniti stroge mjere zaštite podataka.
- Sigurnost informacija – osobni podaci obrađuju se na način koji jamči odgovarajuću razinu sigurnosti primjerenu rizicima koje predstavlja obrada i prirodu podataka

Načelo zakonitosti, pravičnosti i transparentnosti načelo ograničenja namjene, načelo minimizacije, načelo tačnosti, načelo integriteta i povjerljivosti i načelo odgovornosti predstavljaju osnovne principe zaštite korisničkih podataka. Prvo načelo, načelo zakonitosti, pravičnosti i transparentnosti nalaže da osobni podaci budu obrađivani zakonito, pošteno i na transparentan način. Načelo ograničene namjene odnosi se na to da osobni podaci budu prikupljani samo u određene, izričite i legitimne svrhe i ne da budu obrađeni u skladu s tim svrhama. Minimizacija podrazumijeva obradu podataka koja će biti ograničena samo da ono što je apsolutno neophodno za svrhe za koje se podaci obrađuju. U tom kontekstu potrebno je odrediti minimalnu količinu podataka koja je kompatibilna i razmjerna, a svako prikupljanje podataka iznad propisanog minimuma je pretjerano i nerazmjerno. Načelo tačnosti zasniva se na tačnosti i ažuriranju podataka, a kako bi se to ostvarilo kontrolor treba provjeriti pouzdanost izvora informacija. Načelo integriteta i povjerljivosti zapravo predstavlja obavezu voditelja obrade osobnih podataka da podatke obrađuje na način koji jamči odgovarajući stepen sigurnosti. Posljednje načelo, načelo odgovornosti, nalaže da se kontrolor pridržava svih prethodno pomenutih načela i da može dokazati da postupa u skladu s njima (Mateeva Stoyanova, 2020).

Online korisnici su gotovo uvijek zabrinuti za vlastite podatke koje ostavljaju na internetu. Mediji su dali brojne razloge za zabrinutost, kao što je naprimjer curenje privatnosti i sigurnosti, postojanje mogućnosti za prijevarne radnje kako bi se stvorile prepreke i poteškoće za potrošače prilikom kupovine putem interneta i slično. Povjerenje potrošača u online trgovinu najvjerovatnije će biti pojačano percepcijom privatnosti i sigurnosti, a ranije studije su već potvrdile da na povjerenje potrošača u online trgovinu povoljno utječe percipirani nivo privatnosti. Autori smatraju da je percepcija rizika potrošača povezana s izlaganjem ličnih podataka na mreži, te da se percipirani rizik smanjuje ukoliko je omogućena zaštita privatnosti na web stranici, koja podstiče online transakcije povećavanjem percipirane pouzdanosti web stranice. Osim toga, zaštita privatnosti potrošača povezana je sa mogućnošću kontrole da li će informacije biti otkrivene u tržišnim transakcijama i garantuje korisnicima da neće doći do nezakonitog dostavljanja informacija trećim stranama (Tran i Nguyen, 2022).

2.2.1.1 Primjeri primjene i zaštite osobnih podataka

Choi, Jeon i Kim (2019) navode još neke primjere primjene osobnih podataka korisnika:

- Aplikacija Google Trips – "personalizirani turistički vodič“, razvijena je od strane Google-a. Aplikacija koristi ono što već zna o vama na temelju podataka koji su prikupljeni s vašeg gmail računa i kombinira ih s utvrđenim obilježjima iz svoje druge ponude, poput Odredišta, i svojom velikom bazom podataka recenzija prikupljenih iz gomile“. Recenzenti ove aplikacije navode da je pomenuto bilo pomalo jezivo.
- Genetski testovi – utvrđeno je da se genetski podaci nekih subjekata mogu koristiti za predviđanje genetske dispozicije drugih među istom rasnom ili etničkom skupinom. Zbog praktične brige o privatnosti i/ili mogućnosti za diskriminacijom na osnovu genetskih informacija, savezna vlada SAD-a zabranila je osiguravajućim društvima i poslodavcima bilo kakvu zloupotrebu podataka iz genetskih testova, prema Zakonu o nediskriminaciji genetskih informacija (GINA).

2.2.1.2 Privatnost podataka na primjeru Fitbit

Kao primjer primjene osobnih podataka može se navesti i Fitbit, aplikacija kojoj su potrebni podaci o korisniku kako bi mu bila od koristi, međutim Fitbit se i dalje suočava s brojnim preprekama. Neke od tih prepreka su upravo problemi s privatnošću i novom tehnologijom koja stvara nove načine prikupljanja i dijeljenja informacija. Na početku su informacija na Fitbitu bile javne, odnosno informacije o korisnicima bile su vidljive na društvenim mrežama – njihova kondicija, prehrana, spavanje i slično. Nakon nekog vremena, te informacije su se mogle objavljivati privatno i ostati dostupne samo korisniku i aplikaciji. Zabrinutost je postojala zbog neizvjesnosti šta se događa s unesenim podacima – da li ih Fitbit dalje analizira, prodaje ili dijeli. Praćenje fitnessa i podaci koje generiraju nisu bili regulirani i svaka organizacija vezana za usklađenost s Zakonom o prenosivosti i odgovornosti zdravstvenog osiguranja SAD-a (HIPAA) mogla je jednostavno pristupiti analizi podataka s uređaja korisnika. Zabrinutost o tome koji se podaci prikupljaju i kako se prikupljaju nisu postojali samo kod korisnika, već i kod uposlenika kompanije u situacijama kada su primjerice javili da su bolesni kada nisu, nelagoda zbog trudnoće koja bi također mogla biti jedan od praćenih parametara. Kreatori Fitbita također su imali svoje zabrinutosti – a to su lažni podaci na osnovu kojih su neki sudionici wellness programa dobili nagrade. Događalo se da sudionici wellness programa varaju svoje Fitbitove tako što primjerice svoj uređaj stave na ogrlicu psa koji će preći 13.000 do 30.000 koraka dnevno. Još jedan izazov je konkurencija, jer kako digitalne tehnologije napreduju na svim frontovima, postalo je očito da uređaj za praćenje fitnessa nije više aktuelan – npr. pojavom Apple pametnog sata, Apple Healtha i Google Fit-a. Ipak, Fitbit još uvijek postoji i nastoji uspostaviti praćenje fitnessa u svrhu prepoznavanja medicinske dijagnoze (Kotler i Armstrong, 2017).

2.2.2 Sigurnost korisnika

Herley (2008) navodi da su korisnici često nemotivirani u pogledu sigurnosnih pitanja, te da odabiru slabe lozinke, zanemaruju sigurnosna upozorenja i nisu svjesni grešaka u certifikatima. Autor navodi da stranice savjetuju korisnicima da se zaštite od direktnih troškova napada, ali ih opterećuje u smislu napora koji je potrebno uložiti kako bi se ta sigurnost uspostavila. Većina sigurnosnih savjeta korisnicima jednostavno nudi loš kompromis između troškova i koristi, stoga ih korisnici odbijaju. Teško je osmisliti sigurnosne savjete koji su uistinu korisni, pa tako na primjer nema smisla opterećivati korisnike svakodnevnim zadatkom kako bi 0,01% njih poštedjeli rizika na internetu.

Yang, Tian i Ward (2007) nastojali su proučiti utjecaj okolišnih faktora zasnovanih na Cloud i Edge računarstvu, kao što su alati koji se koriste u digitalnom forenzičkom procesu, metode za rukovanje neovlaštenim zvučnim datotekama, skrivenim datotekama, fotografijama i slično. Cloud i Edge računarstvo postali su najčešće korištene tehnologije, a njihove prednosti su niži troškovi i veća efikasnost, skladištenje podataka gdje se podaci obrađuju, omogućava bolju kontrolu podataka i kontinuirani rad. S druge strane, njihov utjecaj na kompjutersku forenziku je donekle nepoželjan.

Da bi izgradili sisteme koji štite korisnike od lažnih (ili phishing) web stranica, dizajneri web stranica moraju znati koje strategije napada funkcionišu i zašto. Dhamija, Tygar i Hearst (2006) u svom istraživanju pružili su empirijske dokaze o tome koje su zlonamjerne strategije uspješne u obmani korisnika. Prvo smo analizirali veliki skup uhvaćenih phishing napada i razvili niz hipoteza, koje su potom analizirane. Procjena je izvršena tako što je 22 učesnika pokazano 20 web stranica od kojih su oni trebali identificirati koje su lažne. Utvrđeno je da 23% učesnika nije pogledalo znakove zasnovane na pretraživaču, kao što su adresna traka, statusna traka i bezbjednosni indikatori, što je dovelo do pogrešnih izbora u 40% slučajeva. Također smo otkrili da neki napadi vizualne obmane mogu zavarati čak i najsofisticiranije korisnike. Prakash *et al.* (2021).

2.2.3 Zaštita sigurnosti

Johnson (2022) navodi sljedeće načine primjene tehnologije za zaštitu podataka:

- Firewall – početni sigurnosni sloj u sistemu, dizajniran tako da spriječi neovlaštene izvore da pristupe podacima preduzeća, tako što djeluje kao posrednik između lične ili poslovne mreže i javnog interneta.
- Autentifikaciju i autorizaciju – podrazumijeva da korisnici daju dokaz da su oni upravo ti za koje se predstavljaju. Provjera se može izvršiti pomoću šifre, PIN-a ili se može raditi o biometrijskoj autentifikaciji.
- Enkripcija – šifriranje podataka kojim se podaci pretvaraju u kodirani šifrirani tekst kako bi bili sigurni u mirovanju i dok su u tranzitu između odobrenih strana.

- Maskiranje podataka – metoda kojom se podaci prikrivaju tako da, čak i ako ih kriminalci eksfiltriraju, ne mogu shvatiti šta su to dobili. Maskiranje podataka uključuje zamjenu legitimnih podataka sličnim, ali lažnim podacima.
- Sigurnost zasnovana na hardveru – fizička zaštita uređaja, a ne oslanjanje samo na softver instaliran na hardveru (hardverski bazirani zaštitni zidovi, proxy server i hardverske sigurnosne module).
- Sigurnosna kopija podataka (backup) i zaštita – smatra se da bi organizacije trebale čuvati više kopija podataka, jer uz postavljene sigurnosne kopije podataka, kompanije mogu nastaviti s normalnim poslovnim funkcijama brže i s manje problema. Kao primjer zaštite podataka se navodi skladištenje podataka, pri čemu je preporučljivo voditi se strategijom izrade tri kopije koje će biti sačuvane na različitim lokacijama.
- Brisanje podataka – važno je da organizacije pravilno briše podatke i osigura da se ne mogu vratiti, a to često podrazumijeva pretvaranje podataka u nečitljive nakon brisanja.

3. UTJECAJ IT SIGURNOSTI NA PRODAJU

Baker (2019) navodi sljedeće metode kojima je moguće utjecati na poboljšanje sigurnosti i prodaje:

1. Zadržati samopouzdanje kojim će biti ostvareno veće samopouzdanje.

2. Uporediti uvjerenja sa drugima – da li se kompanija povezala s onima na koje želi utjecati, da li je veza rezultirala odnosom koji će omogućiti dvosmjernu komunikaciju, da li je komunikacija rezultirala povratnim informacijama.

3. Dodati vrijednosti – prije nego neki program ili politika budu implementirani, poželjno je dobiti povratne informacije od korisnika, kako bi ono što nudimo bilo u skladu s potrebama korisnika.

4. Predanost – Rad ne treba biti motivisan samo zaradom, već i unutarnjim stavovima pojedinca koji želi kreirati sigurno okruženje za korisnike.

5. Poznavati proizvod/uslugu i korisnike – kako bi proizvod bio dobro plasiran i konkurentan, potrebno je identificirati publiku kojoj će biti namijenjen i koja će za isti biti zainteresovana.

Lockett (2016) je sprovela istraživanje koje je imalo za cilj ispitati strategije kojima se menadžeri malih maloprodajnih poduzeća koriste prilikom provedbe mrežnih marketinških aktivnost kako bi ostvarili povećanje prodaje derivata. Podaci su prikupljani intervjuom s menadžerima, pregledom poslovnih dokumenata kompanije, njihove web stranice i društvenih mreža. Na osnovu prikupljenih podataka od četiri menadžera malih

maloprodajnih kompanija, autorica je izdvojila četiri ključe teme: platforme i strategije društvenih medija, strategije online marketinga i izazovi u online marketingu, strategije online sadržaja i strategije praćenja. Istraživanjem je ustanovljeno sljedeće:

- Poslovni čelnici bili su svjesni da je društveno umrežavanje novi način komunikacije s potrošačima.
- Svi sudionici studije koristili su Facebookove alate kao strategiju za komunikaciju s potrošačima.
- Mnoge tvrtke koriste tehnologiju temeljenu na webu i interaktivne pristupe kao novi marketinški kanal za poboljšanje konkurentnosti i veće vidljivosti organizacije.
- Angažman potrošača stvara potencijalne kupce, poboljšava prodaju i potiče lojalnost kupaca
- Svi sudionici koristili su online alate kao strategiju za umrežavanje, kako bi pomogli u izgradnji u zajednici i kako bi bolje upravljali odnosima s kupcima.
- Online sadržaj koji su kompanije objavljivale na svojim društvenim mrežama povećali su svijest o proizvodima i privukli nove potrošače.
- Sadržaj na online stranicama bio je personaliziran i prezentiran tako da odražava interes potrošača. Mrežna masovna personalizacija bila je strategija koju su koristili svi ispitani menadžeri kako bi dosegli više demografskih podataka.
- Menadžeri su nedovoljno koristili metodu ponovnog ciljanja, odnosno identificiranja ciljne publike koja će biti zainteresovana za njihov proizvod, a ta metoda može pomoći u ostvarenju boljih rezultata poslovanja.
- Za kontinuiran uspjeh u poslovanju, kompanije bi morale održavati pozitivan odnos sa svojim postojećim kupcima i predvidjeli njihove buduće potrebe.

Cilj studije koju je sprovela Zykova (2012) bio je istražiti procese marketinga i podrške u prodaji u postojećem distribucijskom kanalu kompanije, te na koji način se taj proces može poboljšati. Studija se temelji na akcijskom istraživanju koje započinje dijagnostikom postojeće situacije u posmatranoj kompaniji, uzimajući u obzir trenutna sigurnosna rješenja. Autorica je identificirala četiri značajna aspekta u procesu marketinga i poboljšanja prodaje, a to su: kanali distribucije, marketing odnosa, programi podrške marketingu i prodaji, te ranija istraživanja koja mogu pomoći u generiranju novih ideja i doprinijeti poslovanju kompanije. Istraživanjem je utvrđeno sljedeće:

- Povratne informacije trebaju pružiti opće informacije o tome šta motivira partnere u njihovoj suradnji s tvrtkom i konkretne informacije o tome šta treba poboljšati u načinu podrške partnerima, poboljšanju marketinške i prodajne materijale kako bi im pomogli u ostvarivanju veće prodaje.
- Distribucija na dvije i više stranica popularan je način ulaska na nova tržišta, a glavne prednosti je to što omogućava prodavaču da dopre do većeg broja ljudi.
- Cilj marketinga je privući nove kupce u savremenim uslovima – velika konkurencija i nedostatak diferencijacije između proizvoda. Tradicionalni marketinški koncept sugeriše da su sve interakcije između sudionika marketinške i prodajne aktivnosti

transakcijske prirode, ali također naglašava da su odnosi postali važan koncept u marketingu.

- Tvrtke se koncentriraju više na odnose, povezanost i interakciju kako bi zadržale postojeće kupce i povećale prihode ponudom novih proizvoda i usluga postojećim kupcima.
- Za postizanje pojedinačnih i zajedničkih ciljeva, kompanije moraju koordinirati svoje poslovanje, pri čemu je potrebno sljedeće: a) poboljšati komunikaciju o novim proizvodima i njihovu dostupnost ; b) poboljšati marketinške materijale; c) poboljšati informiranost o konkurenciji.

Studija kojom su ispitani uslovi strateške orijentacije koji doprinose sposobnosti korisnosti radikalne inovacije proizvoda. Kako bi testirali ove odnose, Boso *et al.* (2016) sproveli su višestruke ankete među međunarodnim malim i srednjim poduzećima (SME) u razvijenim ekonomijama i ekonomijama u razvoju. Svojim istraživanjem su ustanovili da, iako postoji pozitivna povezanost između radikalne inovativnosti proizvoda i prodajnog učinka u kontekstu razvijene ekonomije, ta veza nije značajna u kontekstu tržišta u razvoju. Također, kada postoji visok nivo radikalne inovativnosti proizvoda, kao i kada se poduzetnička orijentacija povećava, dolazi do odgovarajućeg povećanja prodajnih performansi. U oba slučaja, razvijene ekonomije i ekonomije u razvoju, visoki nivoi tržišne orijentacije jačaju efekat radikalne inovativnosti proizvoda na performanse prodaje.

Internet kupovina je fenomen koji u današnje vrijeme ubrzano raste, pogotovo kada se radi o generaciji Y. Povećanje interesa za online kupovinu dovelo je i do povećanog interesa prodavača za ovu oblast. Istraživanje sprovedeno na Univerzitetu Malaysia Perlis ukazuje na to da subjektivni stavovi i percipirana korisnost značajno pozitivno utječu na namjeru kupovine putem interneta, ali i da subjektivna norma ima neznatan negativan utjecaj na ponašanje pri kupovini. Stavovi o korisnosti online kupovine također neznatno utječu na ponašanje pri kupovini putem interneta, dok namjera kupovine značajno pozitivno utiče na ponašanje u online kupovini. Lim *et al.* (2016) također govore i o modelu prihvatanja tehnologije, koji je korišten za procjenu korisničkog prihvaćanja računara na osnovu stavova, percipirane korisnosti, rizika i percipiranom lakoćom korištenje prema namjeri upotrebe. Rezultati njihovog istraživanja ukazuju na to da percipirana korisnost snažno utječe na namjeru upotrebe, a da percipirana jednostavnost upotrebe ima samo trivijalan utjecaj na namjeru upotrebe. Uočena korisnost i percipirana lahkoća upotrebe determiniraju namjeru korištenja.

3.1 Uspostavljanje sigurnosti u e-commerceu

Kako bi se rizici u online trgovini izbjegli, potrebno je razviti model sigurne e-trgovine kako bi se ublažili i riješili problemi u ovoj oblasti. Takav model trebao bi zadovoljavati sljedeće karakteristike (Kaushik, Gupta i Gupta, 2020):

- Ažurirani HTTPS – HTTPS postaje standard internet sigurnosti, a njegovo onemogućavanje može sa sobom nositi negativne posljedice.
- Adekvatan odabir platforme – Većina trgovina e-trgovine koristi platforme kao što su Magento i Shopify, uglavnom zbog njihove zaštite. Glavni faktori koje trgovci uzimaju u obzir prilikom odabira platforme za e-trgovinu su: praktičnost, robusnost, funkcionalnost i sigurnost.
- Upozorenje sa sigurnosnim dodacima – predstavlja dobru opciju za trgovce e-trgovinom dok vode stranice na različitim platformama. Pomenuti dodaci sprječavaju hakiranje stranica.
- Hermetički zatvorena administratorska ploča – Postoji više uglova koje hakeri mogu koristiti kako bi ušli na stranicu, a najjednostavnije je pristupiti Admin panelu, s toga je potrebno da lozinke admina budu jake i teške za hakirati.
- Sigurnosne kopije podataka (backup) – Finansijski podaci vrlo su bitni ili povjerljivi, te je neophodno imati sigurnosnu kopiju ovih podataka na redovnoj bazi na više lokacija, po mogućnosti na cloud-u i na fizičkom (hard) disku, na više lokacija.

Danas se većina korisnika odlučuje za online bankarstvo, kupovinu, prodaju, kupovinu i mnoge druge aktivnosti. Pomenute online aktivnosti imaju brojne prednosti, ali sa sobom nose i različite izazove od kojih je najveći sigurnost korisnika. Implementacija odgovarajućih sigurnosnih mjera pri korištenju e-trgovine jedan je od ključnih zadataka online trgovine. Badotra i Sundas (2021) analizirali su sisteme sigurnosti e-trgovine u posljednjih deset godina. Autori zaključuju da bez obzira na sve izazove na internetu, korisnici trebaju biti sigurni na internetu. Zaključuje se da bi stranice trebale koristiti HTTPS umjesto HTTP-a – što omogućava zaštitu web stranice SSL certifikatima. HTTPS protokol štiti poslane podatke, a SSL je najčešći sigurnosni protokol koji stvara sigurnu vezu između dva računala na mreži. Radi se o šifriranju podataka kako bi se korisnici zaštitili od napada. Kada se radi o korisnicima, oni se mogu zaštiti na sljedeći način:

- Koristiti jedinstvenu i kompleksnu lozinku za svaku uslugu, primjenu i slično, a korištenje iste lozinke za sve račune je nepreporučljivo.
- Odabrati lozinku koja nije povezana s ličnosti
- Ne tražiti od trećeg lica da kreira lozinku i ne dijeliti lozinku s drugim osobama.
- Što prije sistemski mijenjati zadane lozinke u slučajevima kada ih sistemi sadrže.
- Često mijenjati lozinke
- Ne držati lozinku u datotekama na računaru ili telefonu.

Praćenje prijetnji cyber sigurnosti i usklađivanje sa zakonskim regulativama nije jednostavno. Mnoge kompanije angažuju podršku savjetnika kako bi bolje razumjeli stanje cyber sigurnosti svoje kompanije i stepen usklađenosti s normama, kao i kako bi primijenili najbolje prakse i nastavili se kretati ka poslovnim ciljevima uprkos cyber rizicima. Savjetnici mogu pomoći menadžerima da predvide rizike, prilagode se na promjenjivo okruženje i napredak tehnologije i inovacije, sve u svrhu stjecanja konkurentske prednosti bez slabljenja sigurnosti na njihovim web stranicama. Vodeće organizacije traže tačnu procjenu situacije

koja će im omogućiti razvijanje planova za bolje upravljanje rizikom, usklađenost i upravljanje, a te procjene uključuju: kvantifikaciju rizika, identificiranje sigurnosnog rizika treće strane, testiranje penetracije kako bi se pronašle slabosti sopstvenog sistema, te simulaciju cyber provala kojima se može testirati spremnost osoblja za takve napade. Iskustva sa cyber zaštitom mogu pomoći organizacijama da procijene nedostatke u njihovom planu odgovora na incidente, te da kritički procijene nivo sigurnosti u organizaciji. Ova vrsta sigurnosne introspekcije može biti od velike koristi. Sigurnost je stalni izazov, a savjetnici mogu obezbijediti kontinuirano praćenje bezbjednosti, upravljanje i obuku koja će uposlenicima i organizaciji pomoći da održe jaku sigurnost i držanje usklađenosti, njegovanje sigurnosne kulture, pomoć u rješavanju novih prijetnji i prilagodbu sigurnosti novim izazovima (IBM Security, 2020).

Sigurnosne organizacije su odgovorne za identifikaciju i analizu rizika, ranjivosti i posljedica rizika. One također trebaju biti u stanju i da preporuče određene mjere kako bi se organizacije mogle boriti protiv pomenutih rizika. Predstavnik agencije odgovoran je za odluku da se te preporuke implementiraju ili da se rizik prihvati kao dio strategije upravljanja rizikom. Zajedno, predstavnik sigurnosne organizacije i menadžer odgovorni su za identifikaciju i implementaciju najisplativije mjere za ublažavanje izloženosti riziku, čime se rizik smanjuje na prihvatljiv nivo. Za donošenje informirane odluke zasnovane na riziku, organizacija i organ za donošenje odluka moraju sarađivati jer za svaku preporučenu mjeru, sigurnosna organizacija mora pružiti sve informacije koje se odnose na odluku: priroda prijetnje, specifične ranjivosti koje se moraju riješiti, potpuno razumijevanje potencijalne posljedice i troškovi. Donosioci odluka moraju raspolagati pomenutim informacijama kako bi formirali ispravan odgovor. Oni također moraju imati ovlaštenja, odgovarajuću sigurnosnu provjeru i pristup stručnim resursima (npr. sigurnost, objekte i finansije) kako bi stekli dovoljno razumijevanja relevantnih pitanja i donijeli odluku koja se tiče identificiranog rizika (Interagency Security Committee, 2021).

3.2 Menadžment i sistemi sigurnosti

Menadžeri su svjesni da zadovoljstvo kupaca igra ključnu ulogu u uspješnoj poslovnoj strategiji. Kako bi zadovoljstvo kupaca bilo ostvareno, potrebno je znati na koji način upravljati tim zadovoljstvom i napore usmjeriti na povećanje zadovoljstva korisnika, pa tako i do povećanja prodaje u trgovini (Gómez, McLaughlin i Wittink, 2004).

Internet trgovci mogu usvojiti različite strategije kako bi uvjerili one koji oklijevaju da ipak obave kupovinu putem interneta. Online trgovine trebaju obratiti pažnju na kvalitet proizvoda, raznolikost, dizajn i brendove koje nudi. Prvenstveno je potrebno poboljšati kvalitet proizvoda kako bi stvorilo povjerenje potrošača. To je moguće ostvariti pružanjem potpunih informacija o historiji prodavača i proizvoda. Također, menadžeri mogu usvojiti marketinške strategije kao što je prilagođena i sigurna web stranica, koja može poboljšati kupovno iskustvo kupaca i pojednostaviti pretraživanje proizvoda i pravilan sistem navigacije na web stranici. Iskustvo korisnika moguće je poboljšati dodavanjem više slika,

video zapisa proizvoda i trodimenzionalnih (3D) slika koje će dodatno pomoći u procesu donošenja odluka. Kupci se mogu osjećati sigurnije ukoliko online trgovci osiguraju sigurnost plaćanja nudeći brojne opcije plaćanja kao što su pouzećem, dostava nakon pregleda, Google Pay ili slično (Daroch, Nagrath i Gupta, 2021).

Analizom ranijih istraživanja Lockett (2016) zaključuje sljedeće:

- Razumijevanje online marketinga prilika je za poboljšanje poslovanja i povećanje prodaje
- Poslovni lideri bi trebali koristiti digitalne marketinške alate (npr. Google Alerts i Crazy Egg) kako bi izmjerili svijest o brendu, hashtagovima kompanije i konkurenata na društvenim mrežama.
- Online marketinške strategije uključuju interakciju, komunikaciju i primjenu novih tehnologija.
- Primjenom digitalnog marketinga u strateškom planu poduzeća moguće je poboljšati poslovne i potrošačke odnose.

Chehrehpak, Pesaran Afsharian i Roshandel (2014) su nastojali ispitati implementaciju sistema upravljanja informacijskom sigurnosti (ISMS) i učinkovitost tih sistema na uspješnost marketinga i odjela prodaje u oblasti e-trgovine, odnosa s kupcima, povjerenja, učinkovitosti i djelotvornosti korištenja i dijeljenje informacija, te poboljšanju informacijske sigurnosti u odjelu marketinga i prodaje. ISMS uključuje razumijevanje ciljeva upravljanja informacijskom sigurnosti pomoću sistemskih metoda, standardiziranih postupaka i dokumentiranjem organizacijske strategije. Istraživanje je sprovedeno u iranskim organizacijama, a uzorak su činili stručnjaci u odjelima marketinga i prodaje u kojima se ISMS primjenjuju. Rezultati studije ukazuju na sljedeće:

- Glavni učinci implementacije ISMS-a u marketingu i odjelu prodaje uključuju povećanu informacijsku sigurnost i poboljšanje performansa e-trgovine i online prodaje.
- Upravljanje informacijskom sigurnošću podrazumijeva kontinuirani računalni proces koji ima za cilj uspostaviti, implementirati, koristiti, pratiti, pregledavati,održavati i poboljšati informacijsku sigurnost.
- Primjena i implementacija ISMS-a često je komplikovana i dugotrajna i može zahtijevati značajne troškove organizaciji. Ipak, doprinosi primjene ISMS-a daleko su veći od njihove cijene.
- Menadžerova svijest i znanje o tome kako organizacija funkcioniše može značajno doprinijeti učinkovitost upravljanja informacijskom sigurnošću.
- Kritična pitanja prilikom upravljanja informacijskim sistemima tiču se menadžerske strukture, opskrbe električnom energijom, sigurnosti informacija i podataka, te ljudski resursi.
- Sljedeće su prednosti primjene ISMS-a: ograničeni pristup neovlaštenih vanjskih osoba organizacijskim informacijama; ograničen pristup ljudi unutar organizacije

nepotrebnim informacijama; sačuvane informacije i njihova vrijednost; upotreba informacija samo od strane organizacije.

- ISMS također imaju pozitivan utjecaj na odjel marketinga i prodaje.
- Primjena ISMS-a promoviše informacijsku sigurnost.
- Postoji izravan značajan odnos između implementacije ISMS-a i poboljšanja e-trgovina u organizacijama.
- Korištenjem ISMS-a promiču se sigurnost i povjerenje u virtualne postavke.
- ISMS omogućuje bolju i učinkovitiju pohranu informacija i njihovo održavanje ograničava pristup informacijama o organizaciji i odjelu, te tako vodi do većeg povjerenja između članova odjela marketinga i prodaje.
- Postoji značajna korelacija između informacijske sigurnosti i poboljšanja e-trgovine u marketingu i prodaji, kao i poboljšanju odnosa s kupcima. Što je veća sigurnost informacija, veće je i povjerenje među uposlenicima, ali i povjerenje od strane klijenata.

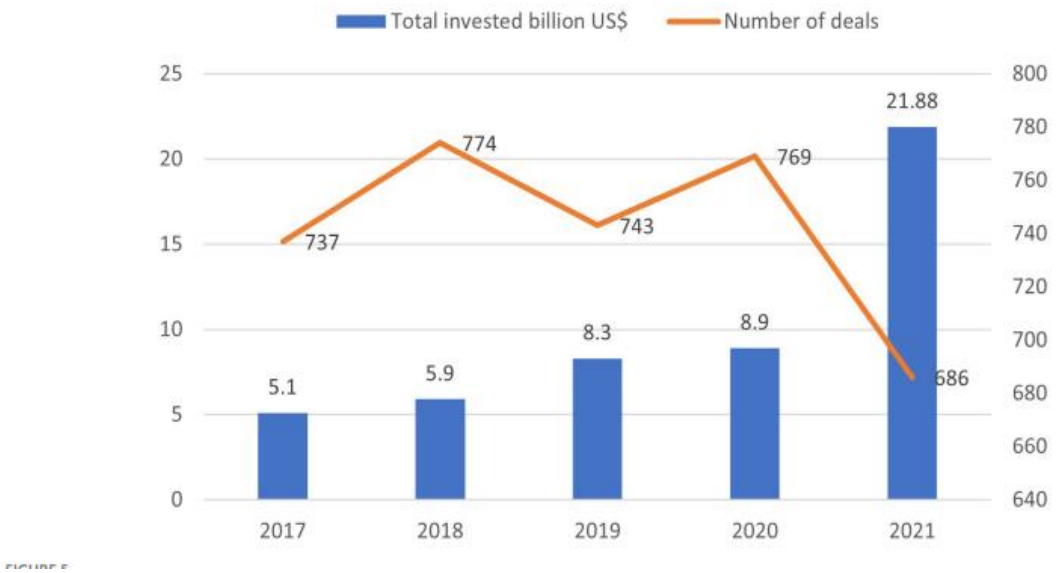
Značaj efikasnog upravljanja IT sigurnosti povećao se i iz ekonomske perspektive, zbog sve veće učestalosti kršenja sigurnosti i posljedica koje to nosi sa sobom. Svako kršenje sigurnosti uzrokuje novčanu štetu, korporativnu odgovornost i gubitak kredibiliteta. Cavusoglu, Cavusoglu i Raghunathan (2004) navode sljedeće faktore koje treba uzeti u obzir kod upravljanja sigurnosnim funkcijama:

1. Procjena sigurnosti i trošak kršenja
2. Pristup upravljanju rizikom
3. Ekonomična konfiguracija tehnologije
4. Vrijednost implementacije više tehnologija.

Smjernice komercijalnih sigurnosnih firmi i istraživačkih instituta naglašavaju potrebu za pravilnom konfiguracijom sigurnosnih implementacija, kao što je naprimjer primjena sistema za otkrivanje hakiranja firme, savjetovanje firme da ne prihvata neizvršenje obaveza, ili automatsko podešavanje odgovarajuće konfiguracije balansiranje sigurnosti i zahtjeva rada.

Drugi razlog za prijetnje cyber bezbjednosti je nepripremljenost. Zbog svoje nespremnosti, napadači iskorištavaju priliku. Ozbiljnost nepripremljenosti u prijetnjama cyber sigurnosti u modernoj elektronskoj eri evidentna je iz statistike da je samo 2021. godine u cyber sigurnost uloženo 21,8 milijardi USD u odnosu na 5,1 milijardu USD u 2017., 5,9 milijardi USD u 2018. godini, 8 milijardi USD10. , i 8,9 milijardi USD u 2020. Uz to, ako pogledamo podatke, u posljednjem kvartalu 2021. godine zabilježen je najveći iznos od 7,8 milijardi USD ulaganja u sajber sigurnost kao što je prikazano na slici . Slika iznad pokazuje da se ulaganja u cyber sigurnost povećavaju iz godine u godinu sa brzim rastom u 2021 (Liu *et al.*, 2022).

Grafikon 3- Grafikon 3. - Ulaganje u cyber sigurnost



Izvor: Liu et al.,2022

Informaciona i komunikacijska tehnologija (IKT) je osnovni element gotovo svih poslovnih procesa. Nove mogućnosti koje nude moderni IT, podjednako pokreću i provajdere i korisnike, iako se radi o osjetljivim informacijama u sve više složenim mrežnim strukturama koje oblikuju ljudi i organizacije. IT sigurnost, odnosno sigurnost informacija, predstavlja proces koji procjenjuje potrebu za zaštitom informacija, ispituje pouzdanost tehnologije, preporučuje zaštitne mjere i osigurava pouzdanost IT usluga. Web aplikacije moraju kontinuirano raditi na dostupnosti, besprijekornosti podataka i zaštiti privatnosti. Potražnja za pouzdanim IT poslovanjem također nosi rizike, koji se kreću od slučajne greške, tehničkih grešaka i grešaka više sile do namjernih grešaka i kriminalnih napada. Pomenuti rizici ukazuju na to da IT sigurnost nije izolovan proces, a sigurnosni incidenti mogu dovesti i do finansijskih gubitaka. IT sigurnost zahtijeva vrijeme, troškove novac, uzrokuje gubitak performansi, a njena financijska održivost još uvijek je nedovoljno jasna. Da bi se garantovala pouzdanost i povjerljivost informatičkog sistema, Ennen (2010) preporučuje sljedeće:

1. Ljudski resursi – adekvatan odabir osoblja, dokumentiranje očekivanja, definiranje parametara i uputstava, te redovno ažuriranje istih.
2. Organizacija – dokumentovanje odgovornosti i procedura, od dizajna faza praćenja postizanja cilja.
3. Tehnologija – implementacija jakih procesa za zaštitu pristupa, identifikaciju, autentifikaciju i izvještavanje. Enkripcija je mehanizam koji omogućava da informacije budu odgovarajuće zaštićene.
4. Infrastruktura – odnosi se na odabir pogodne prostorije za IT poslovanje, servere, serverske sobe, sastanke i arhiv.

Tijekom godina stručnjaci su razvili veliki broj standarda i najbolje prakse imajući sve prethodne faktore na umu. Certifikati i standardi se koriste za provjeru trenutnog statusa IT sigurnosti. Iskustvo pokazuje da je poželjno koristiti uspostavljene modele u tu svrhu, autori navode model PDCA (Planiraj, Uradi, Provjeri, Djeluj), koji se profilirao kao pristup oblikovanju i pružanju IT usluga. IT sigurnost, ekonomičnost i otpornost idu ruku pod ruku sa zahtjevima za funkcionalnošću, efektivnošću, efikasnošću, fleksibilnosti, usklađenosti i otpornosti.

3.3 Stavovi korisnika

U današnje vrijeme tehnologija je promijenila način na koji ljudi funkcionišu i obavljaju svakodnevne aktivnosti. Kupovina i prodaja su neke od uobičajenih ljudskih aktivnosti koje se danas odvijaju online. Na liniji kupovina i e-trgovina, potrošači mogu uživati u pristupu proizvodima iz udaljenih trgovina prema svojim željama. Iako je online kupovina dobra opcija za korisnika, kanal je osjetljiv na prijetnje koje se odnose na privatnost korisnika i ugroženost sigurnosti podataka. Zbog tih izazova, potrošači se osjećaju nesigurno na internetu i ne znaju da li da vjeruju online trgovinama. Online kupovina stekla je svoju popularnost zbog pogodnosti koje se tiču dostupnosti proizvoda na internetskoj platformi koja može biti dostupna bez obzira na lokaciju korisnika. Osim toga, online kupci ne moraju čekati u redu i mogu odabrati najjeftinije ponude bez da gube previše vremena istražujući trgovine po gradu. Aseri (2021) je analizirao prijetnje sigurnosti u online kupovini, izdvajajući faktore koji utječu na percepciju potrošača o kibernetičkim napadima prilikom online kupovine, najčešće sigurnosne prijetnje i prijetnje privatnosti u online kupovini. Autor zaključuje da na percepciju korisnika utječe njihova osobnost, sistem vrijednosti, znanje, ranija iskustva i kontekst kupovine. Korisnici najčešće navode sljedeće sigurnosne prijetnje:

- Krađa identiteta – korisnik je namamljen da da svoje važne lozinke i podatke o kreditnoj kartici ostavi na stranici koja će to zloupotrijebiti. Krađa identiteta je situacija u kojoj prevaranti šalju e-poštu koju lažno predstavljaju kao da je povezana s vrlo uglednim tvrtkama, kako bi dobili određene podatke od korisnika. Phishing koristi prikrivenu e-poštu kao svoje glavno oružje, a cilj je prevariti korisnika tako što će mu biti poslana hitna poruka kojom se zahtijevaju određene radnje – popunjavanje obrasca, uplaćivanje određenog iznosa, preuzimanje zlonamjernog softvera i slično.
- Lažne internetske trgovine – koje su prisutne na internetu i uvjeravaju kupce u kupovinu lažnih proizvoda, a nakon kupovine proizvoda, stranica više nije dostupna onima koji su s nje nešto kupili.
- Krađa podataka – problem za online trgovce koji prikupljaju važne informacije o klijentima u svojim bazama podataka. Sistemski administratori i ovlašteni radnici za pristup poslužiteljima mogu pristupiti podacima bez znanja vlasnika.

Dakle, iako ljudi vole online kupovinu, ipak se susreću s teškoćama kod čuvanja vlastitih podataka. Korisnici i online trgovci trebali zaštititi svoje podatke prilikom procesa kupovine, a Asari (2021) navodi sljedeće načine na koje je to moguće ostvariti:

- Unakrsna provjera sigurnosti stranice koju korisnik koristi. To se može učiniti gledanjem adrese web-mjesta: ako adresa web-mjesta uključuje HTTPS, a ne HTTP.
- Korištenje kreditnih kartica umjesto debitnih kartica jer kreditne kartice imaju ugrađene obrane koje su sigurnije u usporedbi s debitnim karticama.
- Korištenje različitih lozinki jer je primjena jedne lozinke za različite online stranice riskantna. Korisnici bi trebali primijeniti različite lozinke na različitim stranicama jer su one pristup nečijim računima.
- Preporučuje se korištenje vlastite Wi-Fi veze, a u slučaju da nema druge opcije osim korištenja javnog Wi-Fi-ja, onda bi pojedinac trebao šifrirati komunikaciju kako bi spriječio prisluškivanje financijskih podataka od strane lažnih trećih strana.

Zabrinutost potrošača za privatnost i sigurnost ostaje jedna od primarnih prepreka rastu e-trgovine, a razumijevanje posljedica rizika i percepcije korisnika o rizicima sigurnosti može pomoći u pronalaženju učinkovitog rješenja. Gurung i Raja (2016) su istraživali učinke privatnosti i sigurnosti na percepciju rizika i naknadne učinke na stavove i namjere koristeći teoriju planiranog ponašanja. Pomenutim modelom ispitan je odnos povjerenja, privatnosti i sigurnosti s percepcijom rizika i sudjelovanja u e-trgovini. Rezultati istraživanja ukazuju na sljedeće:

- Na namjeru potrošača da sudjeluje u e-trgovini značajno utječu stavovi, subjektivne norme i kontrola ponašanja.
- Na percepciju rizika utječu brige o privatnosti i sigurnosti, te stavovi o povjerenju.
- Zastupljena je puna medijacija stava u odnosu između percepcije rizika i namjere. Iako nema izravnog utjecaja percepcije rizika na namjeru, percepcija rizika utječe na stav, a stav utječe na namjeru.
- Ako je potrošač previše zabrinut za privatnost, to će utjecati na to kako će on/ona percipirati rizik u e-trgovini. Potrošači su ranjivi jer daju osjetljive podatke kao što su podaci o kreditnoj kartici, adrese i e-pošta kada namjeravaju sudjelovati u online transakcijama. Oni imaju ograničenu mogućnost praćenja radnji internetskih tvrtki u vezi s neovlaštenim korištenjem osobnih podataka, zbog čega korisnici osjećaju nelagodu prilikom dijeljenja vlastitih informacija. Identificirane su sljedeće dimenzije zabrinutosti pojedinca u pogledu prakse zaštite privatnosti, a to su: prikupljanje informacija, neovlaštena sekundarna uporaba, neodgovarajući pristup i pogreške.
- Postoji pozitivan odnos između brige o privatnosti i rizika – korisnici s visokim stupnjem zabrinutosti za privatnost vjerovatno će imati visoku percepciju rizika.
- Percepcija rizika značajna je za spremnost potrošača da kupuje s drugih web stranica, a također doprinos i namjeri ponovne kupovine.

- Samo 25% potrošača prepoznaje osobine privatnosti i sigurnosnog pečata na web stranicama.
- Razvijanje uvjerenja o povjerenju nužan je uvjet za sudjelovanje potrošača u e-trgovini budući da online tvrtke nemaju mogućnosti stvaranja osobnih odnosa kao u offline okruženju.

Axway je anketirao 5.074 osoba kako bi procijenio stavove i lagodnost potrošača u pogledu privatnosti i sigurnosti podataka u digitalnim iskustvima. Gotovo 60% ispitanika smatra da se isplati dati kompanijama pristup ličnim podacima ako to vodi do boljeg korisničkog iskustva. Bez obzira na to što bi se potrošači odrekli svojih podataka radi odličnog digitalnog korisničkog iskustva, oni ipak žele imati kontrolu nad tim ko ima pristup njihovim ličnim podacima i ko njima upravlja. 90% ispitanika navodi da želi znati konkretne podatke koje su kompanije prikupile o njima. Sigurnost je identificirana kao problem i mnogi su ispitanici naveli da se plaše da njihovi online podaci nisu sigurni. Analizom podataka utvrđeno je i da (Rodgers, 2022).:

- 37% ljudi širom svijeta smatra da su kompanije transparentne u pogledu načina na koji koriste podatke na mreži.
- 45% Amerikanaca smatra i smatraju da su kompanije transparentne u pogledu načina na koji koriste podatke na mreži, dok je u Ujedinjenom Kraljevstvu situacija drukčija i 74% ispitanika smatra da kompanije nisu transparentne u pogledu načina na koji koriste podatke na mreži.
- 48% ispitanika vjeruje da mobilne aplikacije koje koriste štite njihove lične podatke.
- 85% ispitanih zabrinuto je za sigurnost njihovih online podataka.

Roohparvar (2023) navodi sljedeće razloge zbog kojih je online sigurnost veoma važna:

1. Zaštita podataka o kupcima – Odeljenja za prodaju i marketing upravljaju ogromnom količinom podataka o klijentima, uključujući lične podatke, obrasce kupovine, podatke za kontakt i finansijsku evidenciju. Svi navedeni podaci su najčešća meta cyber kriminalaca. Kršenje podataka u ovim odjelima može rezultirati teškim posljedicama, kao što su oštećenje reputacije, pravne posljedice i gubitak povjerenja kupaca.
2. Osiguravanje digitalne imovine – Ova imovina sadrži vrijednu intelektualnu svojinu, poslovne tajne, marketinške strategije i baze podataka kupaca, a njenim narušavanjem ne samo da može doći do finansijskih gubitaka, već može doći i do krađe povjerljivih poslovnih informacija. Mjere sajber bezbjednosti kao što su jake lozinke, višefaktorska autentifikacija, redovna ažuriranja i enkripcija mogu umanjiti rizik od neovlaštenog pristupa i zaštititi digitalne imovine organizacije.
3. Očuvanje reputacije brenda – Odeljenja prodaje i marketinga često su u direktnoj interakciji sa kupcima, partnerima i zainteresovanim stranama, a sajber incidenti u ovim sektorima mogu narušiti povjerenje u kompaniju, dovesti do odljeva kupaca i negativnog publiciteta. Davanjem prioriteta sajber sigurnosti, organizacije mogu pokazati svoju

posvećenost zaštiti podataka o klijentima i održavanju sigurnog okruženja, čuvajući na taj način reputaciju svog brenda i održavajući pozitivne odnose sa dionicima.

4. Osiguravanje usklađenosti sa propisima – Odjeljenja za prodaju i marketing moraju se pridržavati propisa kako bi izbjegli kazne i pravne posljedice. Sprovođenje mjera kibernetičke sigurnosti (šifriranje podataka, kontrola pristupa i redovne revizije) može biti od koristi u postizanju usklađenosti s propisima.
5. Ublažavanje finansijskih gubitaka – Finansijski gubici nastali zbog sajber incidente uključuiju direktne troškove povezane s oporavkom od napada, pravne takse, regulatorne kazne i potencijalne sudske sporove. Ulaganjem u mjere sajber bezbjednosti, organizacije mogu ublažiti rizik od finansijskih gubitaka odvraćanjem sajber kriminalaca i minimiziranjem uticaja potencijalnih napada.
6. Povećanje svijesti zaposlenih – Cyber bezbjednost trebala bi biti cilj u svim odjeljenjima. Osoblje prodaje i marketinga mora biti educirano o najnovijim prijetnjama cyber sigurnosti, najboljim praksama i internim politikama. Pružajući redovne treninge i promovirajući kulturu svijesti o sigurnosti, organizacije mogu osnažiti svoje prodajne i marketinške timove da identifikuju i efikasno odgovore na potencijalne prijetnje, smanjujući rizik od uspješnih sajber napada.

Kada je riječ o kupcima, oni bi trebali tražiti znakove da je web stranica legitimna, prebaciti se na sigurnu https stranicu. Frontline menadžeri prodaje moraju biti upoznati s prijetnjama sigurnosti i na njih adekvatno reagovati. Makro-ekološki faktori, performanse i učinak menadžerskog prodajnog tima mogu utjecati na sigurnost posla u online okruženju. Studija koju je sproveo Noble (2013) bavi se pitanjem sigurnosti i varijabli koje ranije nisu razmatrane u istraživanju sigurnosti (npr. autonomija, percepcija pravednosti), te povezanost prethodno pomenutih faktora i poslovanja menadžera. Rezultati studije ukazuju na umjereni utjecaj sukoba uloga i dvosmislenosti u vezi između učinka i sigurnosti.

Tran i Nguyen (2021) u svojoj studiji su ispitivali odnos između sigurnosti, individualnosti, reputacije na kognitivnom povjerenju, percipiranog rizika, stavova potrošača i namjere obavljanja online kupovine. Sprovedeno je kvantitativno istraživanje putem ankete, a anketirano je 358 ispitanika iz Vijetnamu. Rezultati ukazuju na sljedeće:

- Sigurnost i reputacija pozitivno utiču na kognitivno povjerenje i negativno utječu na percipirani rizik.
- Privatnost negativno utječe na kognitivno povjerenje i percipirani rizik.
- Kognitivno povjerenje je imalo pozitivan utjecaj na stavove prema kupovini putem interneta, ali percipirani rizici negativno utječu na stavove prema online kupovini.
- Postoji indirektna veza između kognitivnog povjerenja, percipiranog rizika i kupovne namjere.

3.4 Primjer Amazon

Ghosal i Balaji (2022) proučavali su proces pružanja sigurnosne zaštite u Amazonovom sistemu e-trgovine. Razmatrane su različite informacije u vezi s neto prihodom i neto prodajom Amazona, kao i statistički podaci dobiveni istraživanjem tržišta. Infrastruktura Amazon Web Services (AWS) je kreirana tako da zadovoljava potrebe sigurnosti podataka. Ovaj sistem upravlja identitetima, resursima i dozvolama, te općenito upravlja pristupom web stranici. Zaštita podataka smatra se prioritetom kod e-trgovine zbog zaštite kupaca, ali i organizacija koje prodaju proizvode ili usluge. Amazon je implementirao usluge zaštite sigurnosti podataka kupaca još u vrijeme kada nije imao drugačiji i jedinstveni identitet i brend, odnosno na samom početku kada je bio kao i druge male e-trgovine diljem svijeta. Zbog činjenice da se radilo o maloj kompaniji, Amazon je u to vrijeme imao problem s razmjerom, zbog čega je kreirao konkretni interni sustav za zaštitu podataka koji je pomogao da se povećava rast prihodne marže koji je do 2016. godine porastao na 57%. Na osnovu toga se procjenjuje da će Amazon do 2025. godine zauzeti više od 30% tržišnog udjela, što će biti više u odnosu na konkurentske tvrtke IBM, Google i Microsoft. Učinkovita zaštita privatnosti i visok stepen sigurnosti usluge Amazona poboljšali su njegov rast prihoda na više od 62 milijarde američkih dolara u 2021. godini. Zaštita podataka potrošača prioritet je poslovanja Amazona i ključni pokretač ogromnog rasta prihoda Amazona u vrijeme pandemije koronavirusom. Politika sigurnosti i zaštita podataka stvorili su lojalnost i povjerenje kupaca u cijelom svijetu, koji se zbog toga opredjeljuju upravo za Amazonove online usluge.

4. ISTRAŽIVANJE

4.1 Metodologija

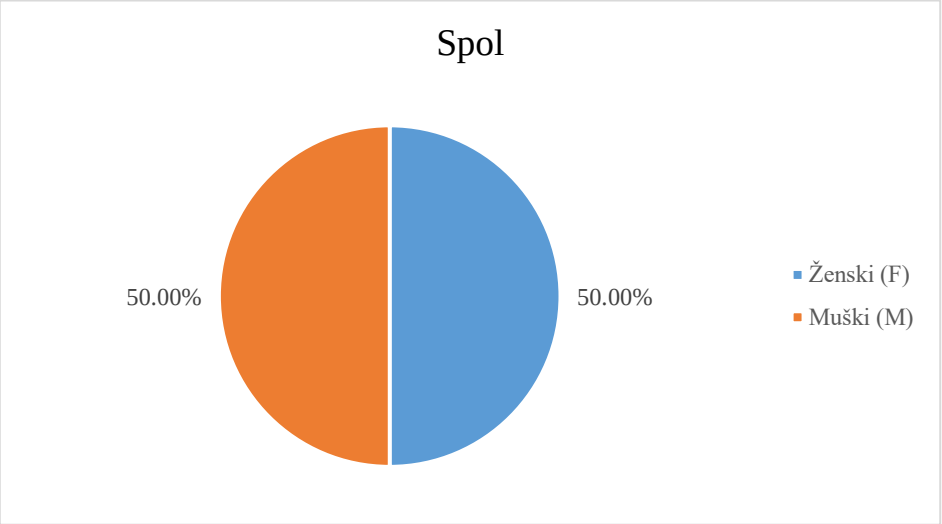
Nakon urađenog teoretskog pregleda literature i postavljanja hipoteza, a kako bismo ponudili odgovore na postavljena pitanja, u ovom radu proveden je elektronski anketni upitnik. Anketa je provedena na ispitanicima (kupcima) raznih grupa potencijalnih potrošača. U prvom dijelu ankete provedenasu pitanja koja se tiču osnovnih i demografskih podataka ispitanika poput dobi, spola, obrazovanja i radnog mjesta. Drugi dio ankete bavio se iskustvima kupaca na online platformama i njihovim stavovima vezanim za osjećaj sigurnosti i kako njihovo poimanje cyber sigurnosti utiče direktno na njihovu odluku o kupovini. Za provođenja istraživanja koristi se multipla regresiona analiza te su predstavljeni rezultati analize iz koje smo izvesli zaključak o direktnoj vezi između cyber sigurnosti i online kupovine, samim tim i uticaja na prodaju iz ugla kupaca.

4.2 Rezultati istraživanja

U dijelu istraživanja sprovedena je anketa na ukupno 436 učesnika.

Na grafikonu 4. prikazana je distribucija ispitanika prema spolu.

Grafikon 4. - Spol ispitanika

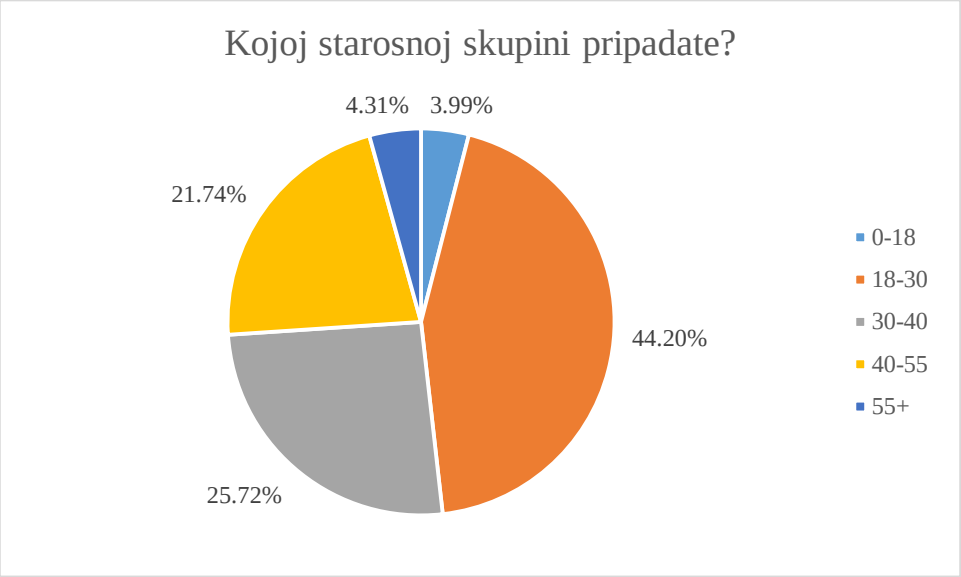


Izvor: kreacija autora

Na osnovu rezultata vidimo da je u anketi učestvovalo jednako pripadnika ženskog i muškog spola, tačnije po 50%.

Na grafikonu 5. prikazana je distribucija ispitanika prema starosnoj dobi.

Grafikon 5 - Starosne skupine ispitanika

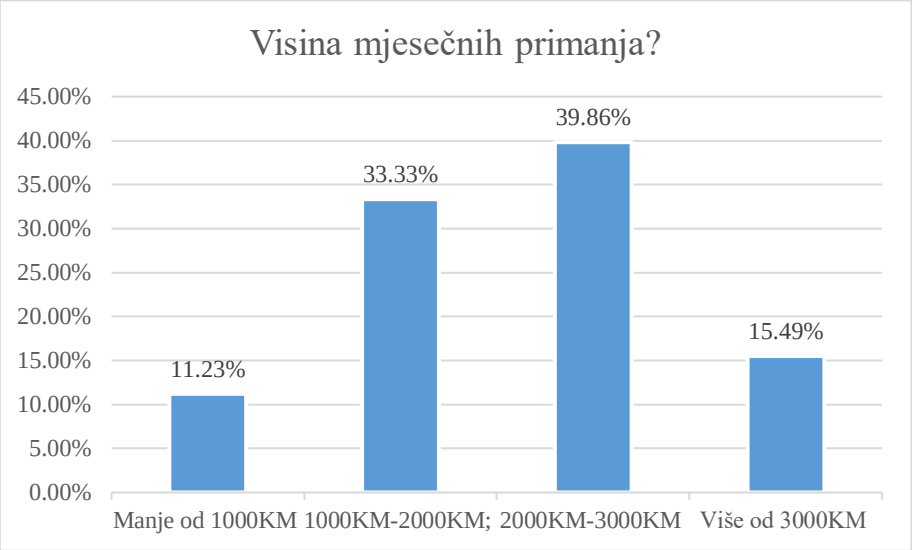


Izvor: kreacija autora

Na osnovu grafikona možemo zaključiti da je većina ispitanika od 18 godina do 30 godina što čini 44,20% ukupnih ispitanika. Druge dvije najveće grupe su grupe od 30 godina do 40 godina, tačnije 25,27% i od 40 do 55 godina, tačnije 21,74% ispitanika. Dvije najmanje grupe su osobe mlađe od 18 godina, tačnije 3,99% i osobe starije od 55 godina, tačnije 4,31%.

Na grafikonu 6. prikazana je distribucija ispitanika na osnovu mjesečnih primanja.

Grafikon 6. - Visina mjesečnih primanja ispitanika

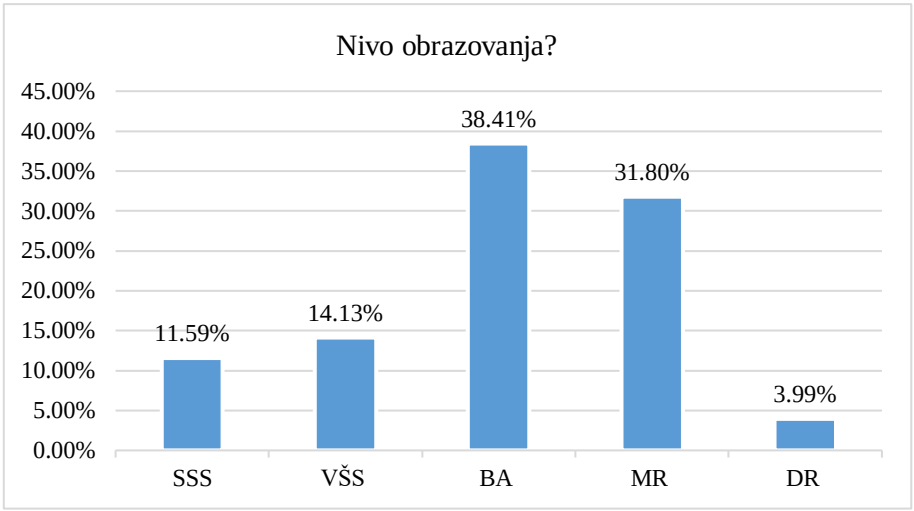


Izvor: kreacija autora

Na osnovu grafika da se zaključiti da najveći procenat ispitanika ima mjesečna primanja od 2000 do 3000KM, tačnije 39,86% ispitanika ima mjesečna primanja u tom rasponu, dok druga najveća grupa ispitanika, tačnije njih 33,33% ima mjesečna primanja između 1000KM i 2000KM. Znatno manje, to jeste, 11,23% ispitanika zarađuje mjesečno manje od 1000KM, dok njih 15,49% ima mjesečna primanja veća od 3000KM.

Na grafikonu 7. prikazana je distribucija ispitanika na osnovu nivoa obrazovanja.

Grafikon 7. - Nivo obrazovanja ispitanika



Izvor: kreacija autora

Na osnovu grafikona vidimo da je najveći procenat ispitanika visokoobrazovano, tačnije 38,41% ispitanika ima Bachelor nivo obrazovanja, 31,80% ima titulu magistra, dok 3,99% njih ima zvanje doktora. Nešto manji procenti, preciznije 11,59% ima završeno srednju školu, dok ih je 14,13% sa VŠS nivo obrazovanja.

U tabeli 1. prikazana je deskriptivna statistika za set pitanja koji se odnosi na opća pitanja koja su bitna za anketu.

Tabela 1. - Opća pitanja

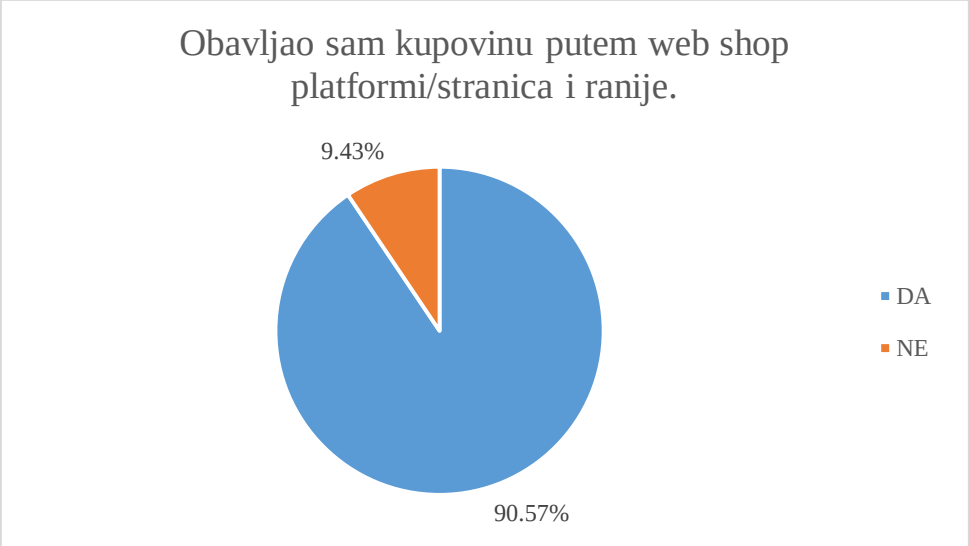
Tvrdnja	**Prosječna vrijednost**	**Standardna divijacija**	**Min**	**Max**
Ne smeta mi da dijelim privatne fotografije na internetu	3,40	1,09	1	5
Nemam ništa protiv da objavim na internetu informacije o mojoj trenutnoj lokaciji.	3,24	1,15	1	5
Nemam ništa protiv da objavim na internetu informacije o tome s kim sam u ovom trenutku	3,49	1,18	1	5

Izvor: kreacija autora

Na osnovu tabele možemo zaključiti da prosječno ispitanici imaju neutralno mišljenje o djeljenju privatnih informacija, kao što su fotografije, lokacija i s kim su, na internetu.

Na grafikonu 8. prikazana je distribucija ispitanika na osnovu ranijeg obavljanja online kupovine

Grafikon 8. - Ranije iskustvo sa online kupovinom

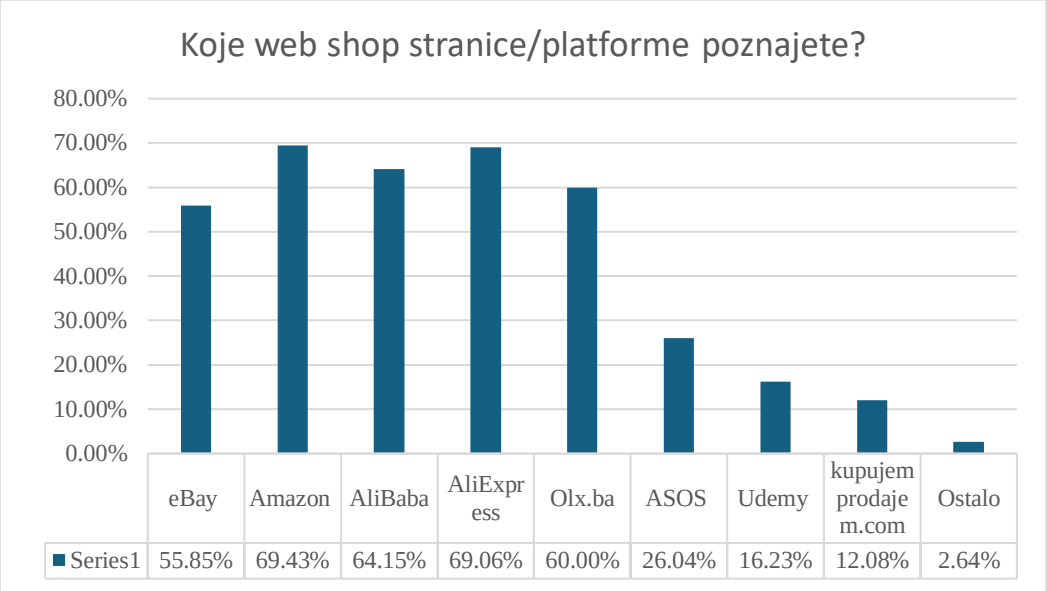


Izvor: kreacija autora

Kao što vidimo na grafikonu 90,57% ispitanika je ranije obavljala neku vrstu online kupovine, dok svega 9,43% ranije nije obavilo ni jedan vid online kupovine.

Na grafikonu 9. prikazane su web shop stranice/platforme za koje su ispitanici ranije poznavali.

Grafikon 9. - Web platforme koje ispitanici poznaju



Izvor: kreacija autora

Na grafikonu mpžemo vidjeti da većina ispitanika je čula za poznatije svjetske i lokalne web shop stranie/platforme kao što s Amazon i AliExpress sa po 69%, nešto manje za AliBaba web shop sa 64,15%. Nakon njih slijedi OLX.ba sa 60% i eBay sa 55,85%. Značajno manje ispitanicu poznaju stranice kao što su ASOS sa 26,04%, Udemy sa 16,23% i kupujemprodajem.com sa 12,08%. U ostalim odgovorima se najčešće pojavljuju stranice poput Wish.com i ZARA.

U tabeli 2. je prikazana desktriptivna statistika za set pitanja koji se odnosi na izgled, organizovanost, animacije web stranica, kao i podatke o proizvodima.

Tabela 2. - Set pitanja o Web shop stranicama/platformama

Tvrdnja	**Prosječna vrijednost**	**Standardna divijacija**	**Min**	**Max**
Smatram da su općenito informacije na web shop stranicama logično predstavljene.	3,8	0,89	1	5
Smatram da su općenito informacije na web shop stranicama dobro organizirane	3,7	0,85	1	5

Sve opcije proizvoda, atributi proizvoda i informacije o proizvodu su inače dobro i jasno predstavljene	3,5	0,95	1	5
Web shop stranice imaju općenito atraktivne boje i pozadinu ekrana	4,0	0,85	1	5
Web shop stranice imaju privlačne slike i naslove na početnoj stranici.	4,0	0,84	1	5
Animacije web shop stranica su smislene i logične.	3,9	0,87	1	5
Grafika i slike korištene na web shop stranicama dobro se uklapaju sa sadržajem.	3,9	0,89	1	5

Izvor: kreacija autora

Set pitanja prikazan u tabeli je imao za cilj da ispita stavove ispitanika o informacijama i izgledu web stranica/platformi. To jeste, da li oni smatraju da su web shop stranice/platforme privlačne, organizirane i da li informacije na njima pružaju sv potrebne detalje o proizvodu. Ono što nam prosječne vrijednosti govore jeste da ispitanici smatraju da su informacije logično predstavljene i dobro organizirane, kako o stranici, tako o proizvodima i da su grafike, slike i animacije smislene i prijatne za kupca. Standardna devijacija nam govori da nema ispitanika koji smatraju da su stranice loše vizuelno i da pruzžaju jako loše informacije o proizvodima.

U tabeli 3. prikazana je deskriptivna statistika za set pitanja koji je imao za cilj da ispita povjerenje ispitanika u online kupovini i stavove o privatnim informacijama koje ispitanici ostavljaju na već spomenutim stranicama.

Tabela 3. - Povjerenje i privatne informacije

Tvrdnja	**Prosječna vrijednost**	**Standardna divijacija**	**Min**	**Max**
Vjerujem da su web shop stranice iskrene i istinito predstavljaju podatake o proizvodima.	3,43	1,20	1	5
Platforma me uvijek upozori ako ima mogućnosti za neku vrstu prevare vezane za kvalitet proizvoda, plaćanja ili slično.	3,33	1,15	1	5

Nisam imao problema sa prevarama prilikom online plaćanja.	3,91	0,88	1	5
Nisam osjetljiv na način na koji online kompanije rukuju sa mojim personalnim informacijama.	3,42	1,23	1	5
Nisam zabrinut za moju privatnost na web shop stranicama.	3,39	1,24	1	5
Nisam zabrinut da će moji lični podaci biti prikupljeni i zloupotrebljeni.	3,26	1,25	1	5
Veoma mi je važno da sam svjestan i upućen u to kako će se moji lični podaci koristiti.	4,07	0,86	1	5
Web shop stranice koje traže informacije na mreži trebale bi otkriti način na koji se podaci prikupljaju, obrađuju i koriste.	4,25	0,79	1	5

Izvor: kreacija autora

Prosječne vrijednosti za ovaj set pitanja ukazuju na to da su ispitanici sumnjičavi kad je u pitanju upravljanje podacima od strane web shop stranica/platformi. Najnižu prosječnu vrijednost i najveću sumnju ispitanici imaju ka tome da li web shop stranice/platforme istinito prikazuju podatke o proizvodima. Kupci isto tako smatraju da uglavnom stranice ne upozoravaju na moguće prevare prilikom kupovine proizvoda. Svakako se da primjetiti da su ispitanici zabrinuti da će njihovi podaci biti prikupljeni i zloupotrebljeni. Ispitanici smatraju da bi web shop stranice/platforme trebale biti transparentnije o načinu rukovanja njihovih ličnih podataka i da im je bitno da su upućeni šta web shop stranica/platforma radi sa njihovim ličnim podacima.

U tabeli 4. prikazana je deskriptivna statistika za set pitanja koji je imao za cilj da ispita prijašenje iskustvo ispitanika u kupovini na online web shop stranicama/platformama.

Tabela 4. - Prethodno iskustvo

Tvrdnja	**Prosječna vrijednost**	**Standardna divijacija**	**Min**	**Max**
Nisam imao problema sa isporukom u prošlosti.	3,77	1,05	1	5

Zbog prethodnog iskustva sam oprezniji u online kupovini.	3,59	1,02	1	5
Veća je vjerovatnoća da ću obaviti online kupovinu ako sam ranije čuo/vidio/čitao pozitivne stvari o kompaniji.	4,05	0,82	1	5
Veća je vjerovatnoća da ću obaviti online kupovinu ako sam imao pozitivno prošlo iskustvo u komunikaciji s kompanijom (npr. služba za korisnike, račun na društvenim mrežama).	4,14	0,72	1	5
Vjerovatnije je da ću obaviti online kupovinu ako sam imao pozitivno iskustvo u prošlosti s proizvodima/uslugama kompanije.	4,22	0,67	1	5
Veća je vjerovatnoća da ću obaviti online kupovinu ako vrijednosti kompanije odgovaraju mojim etičnim i moralnim vrijednostima.	4,28	0,69	1	5

Izvor: kreacija autora

Kako možemo vidjeti i u tabeli, prosječne vrijednosti nam govore da su ispitanici uglavnom imali problema sa isporukom u prošlosti i da su uglavnom oprezniji radi prethodnih iskustava. Ispitanici većinski smatraju pozitivno prethodno iskustvo bitnim za nove kupovine. Isto tako im je bitno da su web shop stranice/platforme u skladu s njihovim moralnim i etičnim vrijednostima. Standardna devijacija nam govori da nema velikog ostupanja kod ispitanika po ovim pitanjima.

U tabeli 5. je prikazan set pitanja koji ima cilj ispitati društveni uticaj na odluku o kupovini.

Tabela 5. - Društveni uticaj

Tvrdnja	**Prosječna vrijednost**	**Standardna divijacija**	**Min**	**Max**
Većina mojih prijatelja koristi web shop-ove s toga ih koristim i ja.	3,67	1,00	1	5

Online kupovina mi olakšava kupovinu i štedi vrijeme.	3,85	0,93	1	5
Web shop stranice mi omogućava pristup online recenzijama.	3,87	0,82	1	5
Čitam online recenzije prije kupovine.	3,86	0,92	1	5
Recenzije na mreži olakšavaju mi korištenje e-trgovine.	4,00	0,78	1	5

Izvor: kreacija autora

Prosječne vrijednosti nam govore da uglavnom ispitanici koriste web shop stranice/platforme jer i njihovi prijatelji ih koriste, također većinski smatraju da im online kupovine štedi vrijeme. Ono što je zanimljivo jeste da ispitanici većinski gledaju recenzije i čitaju ih prije nego što donesu odluku o kupovini.

Na grafikonu 10. prikazan je procenat ispitanika koji planiraju u budućnosti opet obavljati kupovinu.

Grafikon 10. - Buduća namjera kupovine

Izvor: kreacija autora

Kao i što vidimo na grafikonu, 96,41% ispitanika smatra da će i u budućnosti obavljati kupovinu puetm interneta na web shop stranicama/platformama, a svega 3,59% ispitanika ne planira da u budućnosti obavi online kupovinu.

4.3 Diskusija

U ovom dijelu će biti dati odgovori na istraživačka pitanja, kao i odgovori na postavljene hipoteze rada.

4.3.1 Analiza Istraživačkih pitanja

Istraživačka pitanja koja su bila ispitivanja u istraživanju:

1. Sa kojim se prijetnjama suočavaju kupci kada se radi o web shopovima?
2. Koji su faktori koji sputavaju potrošače da obave online kupovinu?
3. Koje su vrste rizika e-kupovine?
4. Koji faktori na web shopovima jačaju povjerenja kupaca?
5. Na koji način društveni uticaj na kupca utiče na povjerenje?
6. Koja načela privatnosti trebaju poštovati vlasnici web shopova kako bi povećali povjerenje kupaca?
7. Na koji način izgled i struktura web stranice utiče na povjerenje kupaca?
8. Koje tehnologije web shopovi trebaju primjenjivati za zaštitu podataka?
9. S kojim metodama je moguće utjecati na poboljšanje sigurnosti i prodaje?
10. Koje tehničke karakteristike treba zadovoljiti web shop kako bi bio u skladu sa sigurnosnim standardima?

1. Sa kojim se prijetnjama suočavaju kupci kada se radi o web shopovima?

Padmannavar (2011) navodi sljedeće prijetnje kada se radi o e-commerceu:

- Klijentske prijetnje – koje su obično statične do trenutka uvođenja izvršnog web sadržaja. Aktivni sadržaj se odnosi na programe koji su transparentno ugrađeni u web-stranice i na osnovu kojih stranica funkcionira. Ovi sadržaji se koriste u e-trgovini za postavljanje artikala koje se želi ponuditi korisnicima, te za računanje ukupnog iznosa fakture i slično. Budući da su moduli aktivnog sadržaja ugrađeni na web stranicama, oni mogu biti transparentni za svakoga ko posjeti tu stranicu. Ipak, moguće je ugraditi zlonamjerni aktivni sadržaj na web stranicama koji prouzrokuje štetu posjetiocima stranice. Zlonamjerni aktivni sadržaj može otkriti kreditnu karticu brojeva, korisničkih imena i lozinki koje su često pohranjeni u posebne datoteke koje se nazivaju kolačići. Zlonamjerni aktivni sadržaj isporučen putem kolačića može otkriti sadržaj datoteka na strani klijenta ili čak uništiti datoteke pohranjene na klijentskim računarima. Osim zlonamjernog aktivnog sadržaja, još jedan rizik predstavljaju i zlonamjerni dijelovi koda, kao što je:
- trojanski konj – program koji obavlja korisnu funkciju, ali obavlja i neočekivane radnje;
- virus – segment koda koji replicira prilaganjem kopija postojećim izvršnim datotekama.

- Prijetnje komunikacijskim kanalom – jer poruke na internetu putuju nasumičnim putem od izvornog čvora do odredišta, kroz niz posrednih računara na mreži, pri čemu je nemoguće garantovati da će svaki uključeni računar biti zaštićen i ne-neprijateljski nastrojen.
- Prijetnje povjerljivosti – prijetnje od neovlaštenog otkrivanja informacija.
- Prijetnje integritetu – postoje kada neovlaštena strana može promijeniti tok protoka informacija.
- Prijetnje dostupnosti ili prijetnja odgodom – ometanje normalne računarske obrade ili potpuno uskraćivanje iste.
- Prijetnje bazi podataka – sistemi e-trgovine pohranjuju korisničke podatke i prikupljene informacije o proizvodu iz baza podataka povezanih s web-pretraživačem. Neke baze podataka pohranjuju parove korisničko ime/lozinkama na nesiguran način, a ukoliko neko dobije autentifikaciju, onda dobivaju pristup korisnikovim informacijama.
- Hakiranje lozinki – najjednostavniji napad na sistem.

2. Koji su faktori koji sputavaju potrošače da obave online kupovinu?

Prema rezultatima studije koje su sproveli Daroch, Nagrath i Gupta (2021) ukupno je šest faktora koji sputavaju potrošače da obave online kupovinu, a to su:

1. Strah od bankovnih online transakcija
2. Tradicionalna kupovina pogodnija je od kupovine putem interneta
3. Reputacija i pružene usluge
4. Iskustvo
5. Nesigurnost i nedovoljne informacije o proizvodima
6. Nedostatak povjerenja

3. Koje su vrste rizika e-kupovine?

Autori navode sljedeće vrste rizika e-trgovine:

1. Sigurnost korisnika – potrebno je uspostaviti sigurnost na web stranici, a u tu svrhu je potreban firewall na strani poslužitelja. Pristup stanice treba biti takav da ne forsira korisnike da dijele platformu zajedno s drugim web stranicama.
2. Botovi – razlikuju se dvije vrste botova – dobri koji pomažu korisnicima stranice i loši koji pretražuju web-mjesta na cijene kao i na podatke o zalihama, nakon čega te podatke koriste kako bi promijenili cijenu, što dalje vodi padu prodaje i prihoda.
3. DdoS napadači – napadaju stranicu na način da je čine offline (neaktivnom).
4. SQL injekcija – vrsta napada u kojoj stranica traži od korisnika da prihvati zaraženi sadržaj, a nakon klika hakeri mogu ukrasti korisne informacije kupaca i tako oštetiti bazu podataka web stranice.
5. Prevara s kreditnom karticom – realna prijetnja korisnicima koji obavljaju transakcije na internetu.

Kako bi dobili dobili detalje kartice, hakeri se infiltriraju u bazu podataka vezanu uz web stranicu e-trgovine koristeći se različitim softverskim programima.

4. Koji faktori na web shopovima jačaju povjerenja kupaca?

Svrha istraživanja koje su radili Baubonienė i Gulevičiūtė (2015) bila je sagledati faktore koji pokreću kupovinu putem interneta, kako bi se poboljšalo razumijevanje faktora koji utječu na ponašanje kupaca u online kupovini. Istraživači su analizirali prednosti kao što su sigurnost, brza dostava, usporediva cijena, praktičnost, povoljnije cijene i veći izbor, koristi koje kupci imaju od online kupovine, ali i rizike koji se javljaju na platformama za prodaju. Istraživanje je bilo usmjereno na to na koji način na online kupovinu utječu faktori kao što su dob, spol ili zanimanje. Na kraju, autori su izdvojili sljedeće faktore koji utječu na ponašanje kupaca kod online kupovine:

1. Tehnološki faktori: usklađenost s najnovijim trendovima u informacijskim tehnologijama, korištenje nalaza za istraživanje znanja, sposobnost procjene ponašanja programa, učinkovit krajnji korisnik i poznavanje hardvera.
2. Faktori povezani s potrošačima: stavovi prema online kupovini, promjena stavova kupaca, kultura, lojalnost, percipirani rizici, zabrinutost potrošača, jednostavnost korištenja, obrazovanje potrošača i prihod; korisnost, povjerenje, preporuke dobavljača i recenzije potrošača, dob i kupovno iskustvo potrošača.
3. Faktori određivanja cijena u online trgovini
4. Faktori proizvoda/usluge: dostupnost informacija o proizvodu, web stranica.

Dodatno su identificirali sljedeće faktore koji značajno utiču na online prodaju:

1. Često ažuriranje web sadržaja
2. Prisustvo pomagala za odlučivanje
3. Pružanje informacija o firmi
4. Prisustvo sekcije FAQ
5. Korištenje multimedije
6. Obezbjeđivanje individualnih korisničkih naloga
7. Bezbjedni načini prenosa podataka
8. Mogućnost obavljanja offline i online finansijskih transakcija i izjava o privatnosti.

5. Na koji način društveni uticaj na kupca utiče na povjerenje?

Na slici 3. prikazan je regresioni model za istraživačko pitanje „Na koji način društveni uticaj na kupca utiče na povjerenje“:

Slika 3 - Efekat društvenog uticaja na povjerenje

Source	SS	df	MS
Model	9.85667723	1	9.85667723
Residual	214.883623	250	.85953449
Total	224.7403	251	.895379681

Number of obs	252
F(1, 250)	11.47
Prob > F	0.0008
R-squared	0.0439
Adj R-squared	0.0400
Root MSE	.92711

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Drustveni_uticaj	.2855767	.0843314	3.39	0.001	.1194862	.4516672
_cons	2.343509	.3353116	6.99	0.000	1.683114	3.003905

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem društvenog uticaja za jednu jedinicu, dolazi do povećanja povjerenja za 0,29 jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,001 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 4,39% što znači da je 4,39% varijabiliteta u povjerenju objašnjeno varijabilitetom u društvenom uticaju.

6. Koja načela privatnosti trebaju poštovati vlasnici web shopova kako bi povećali povjerenje kupaca?

Propisi o zaštiti podataka u EU postavljaju glavna načela privatnosti, a to su (Guarda, 2008).:

- Poštena i zakonita obrada – prikupljanje i obrada osobnih podataka neće bezrazložno zadirati u privatnost ispitanika niti neopravdano ometati njihovu autonomiju i integritet, te će biti usaglašena s cjelokupnim pravnim okvirom.
- Saglasnost – osobni podaci će se prikupljati i obrađivati samo ako je nositelj podataka dao izričitu saglasnost za njihovu obradu.
- Specifikacija svrhe – osobni podaci će se prikupljati za određene, zakonite i legitimne svrhe i na načine koji su u skladu sa svrhom prikupljanja podataka.
- Minimalnost – prikupljanje i obrada osobnih podataka bit će ograničena na minimum potreban za postizanje određene svrhe. Osim toga, minimalnost se odnosi na to da podaci budu čuvani samo izvjestan vremenski period, onoliko koliko je potrebno za postizanje određenog cilja.
- Minimalno otkrivanje osobnih podataka trećim stranama, koje će biti ograničeno i primjenjivati se samo pod određenim uvjetima.
- Kvaliteta informacija – osobni podaci moraju biti tačni, relevantni i potpuni s obzirom na svrhe za koje se prikupljaju i obrađuju.

- Kontrola subjekta podataka – subjekat će moći provjeriti i utjecati na obradu njegovih osobnih podataka.
- Osjetljivost – budući da se radi o podacima koji su izuzetno osjetljivi za nositelja podataka, potrebno je primijeniti stroge mjere zaštite podataka.
- Sigurnost informacija – osobni podaci obrađuju se na način koji jamči odgovarajuću razinu sigurnosti primjerenu rizicima koje predstavlja obrada i prirodu podataka

7. Na koji način izgled i struktura web stranice utiče na povjerenje kupaca?

Vizualni dizajn web stranice uključuje korištenje grafike, boja, slika, animacija, oblika, veličine i stila fonta (Kevin Lu, 2022.). Informacijski dizajn web stranice odnosi se na organizaciju i logičko predstavljanje informacija na web stranici. Istraživanja koja proučavaju karakteristike online prodavaca često naglašavaju značaj dizajna informacija i kvaliteta koji se odnosi na proizvode ili usluge (Kevin Lu, 2022), kao i Dizajn navigacije web stranice odnosi se na obrasce koji se koriste da pomognu posjetiteljima web stranice da se kreću kroz stranice web stranice i dobiju povezane informacije za završetak zadatka kupovine. Ovo uključuje, na primjer, broj padajućih menija i broj podmenija na stranicama web stranice (Kevin Lu, 2022). Na osnovu ankete koja je provedena dolazimo do idućeg zaključka:
Na slici 4. je prikazan uticaj informacijskog dizajna na povjerenje kupaca:

Slika 4. - Uticaj informacijskog dizajna na povjerenje kupaca

Source	SS	df	MS
Model	114.355959	1	114.355959
Residual	110.38434	250	.441537362
Total	224.7403	251	.895379681

Number of obs	252
F(1, 250)	258.99
Prob > F	0.0000
R-squared	0.5088
Adj R-squared	0.5069
Root MSE	.66448

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Informacijskidizajn	.8770673	.0544988	16.09	0.000	.7697319	.9844026
_cons	.2410863	.2044483	1.18	0.239	-.1615743	.643747

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem informacijskog dizajna za jednu jedinicu, dolazi do povećanja povjerenja za 0,88 jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 50,88% što znači da je 50,88% varijabiliteta u povjerenju objašnjeno varijabilitetom u informacijskom dizajnu..

Na slici 5. prikazan je regresioni model za uticaj vizuelnog izgleda na povjerenje kupaca

Slika 5. - Uticaj vizuelnog izgleda na povjerenje kupaca

Source	SS	df	MS	Number of obs =	252
				F(1, 250) =	198.47
Model	99.4579693	1	99.4579693	Prob > F =	0.0000
Residual	125.28233	250	.501129322	R-squared =	0.4425
				Adj R-squared =	0.4403
Total	224.7403	251	.895379681	Root MSE =	.7079

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Vizuelni_izgled	.9671079	.0686483	14.09	0.000	.8319051	1.102311
_cons	-.3741709	.2759055	-1.36	0.176	-.9175663	.1692246

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem vizuelnog izgleda za jednu jedinicu, dolazi do povećanja povjerenja za 0,97 jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 44,25% što znači da je 44,25% varijabiliteta u povjerenju objašnjeno varijabilitetom u vizuelnom izgledu.
Zaključujemo da je izgled stranice koji uključuje grafike, slike, predstavljanje proizvoda, informacije o njima, padajući meniji i svi ostalih sastavni dijelovi web shop stranice/platforme utiču na povjerenje kupaca.

8. Koje tehnologije web shopovi trebaju primjenjivati za zaštitu podataka?

Johnson (2022) navodi sljedeće načine primjene tehnologije za zaštitu podataka:

- Firewall – početni sigurnosni sloj u sistemu, dizajniran tako da spriječi neovlaštene izvore da pristupe podacima preduzeća, tako što djeluje kao posrednik između lične ili poslovne mreže i javnog interneta.
- Autentifikaciju i autorizaciju – podrazumijeva da korisnici daju dokaz da su oni upravo ti za koje se predstavljaju. Provjera se može izvršiti pomoću šifre, PIN-a ili se može raditi o biometrijskoj autentifikaciji.
- Enkripcija – šifriranje podataka kojim se podaci pretvaraju u kodirani šifrirani tekst kako bi bili sigurni u mirovanju i dok su u tranzitu između odobrenih strana.
- Maskiranje podataka – metoda kojom se podaci prikrivaju tako da, čak i ako ih kriminalci eksfiltriraju, ne mogu shvatiti šta su to dobili. Maskiranje podataka uključuje zamjenu legitimnih podataka sličnim, ali lažnim podacima.
- Sigurnost zasnovana na hardveru – fizička zaštita uređaja, a ne oslanjanje samo na softver instaliran na hardveru (hardverski bazirani zaštitni zidovi, proxy server i hardverske sigurnosne module).
- Sigurnosna kopija podataka (backup) i zaštita – smatra se da bi organizacije trebale čuvati više kopija podataka, jer uz postavljene sigurnosne kopije podataka,

kompanije mogu nastaviti s normalnim poslovnim funkcijama brže i s manje problema. Kao primjer zaštite podataka se navodi skladištenje podataka, pri čemu je preporučljivo voditi se strategijom izrade tri kopije koje će biti sačuvane na različitim lokacijama.

- Brisanje podataka – važno je da organizacije pravilno briše podatke i osigura da se ne mogu vratiti, a to često podrazumijeva pretvaranje podataka u nečitljive nakon brisanja.

9. S kojim metodama je moguće utjecati na poboljšanje sigurnosti i prodaje?

Baker (2019) navodi sljedeće metode kojima je moguće utjecati na poboljšanje sigurnosti i prodaje:

1. Zadržati samopouzdanje kojim će biti ostvareno veće samopouzdanje.

2. Uporediti uvjerenja sa drugima – da li se kompanija povezala s onima na koje želi utjecati, da li je veza rezultirala odnosom koji će omogućiti dvosmjernu komunikaciju, da li je komunikacija rezultirala povratnim informacijama.

3. Dodati vrijednosti – prije nego neki program ili politika budu implementirani, poželjno je dobiti povratne informacije od korisnika, kako bi ono što nudimo bilo u skladu s potrebama korisnika.

4. Predanost – Rad ne treba biti motivisan samo zaradom, već i unutarnjim stavovima pojedinca koji želi kreirati sigurno okruženje za korisnike.

5. Poznavati proizvod/uslugu i korisnike – kako bi proizvod bio dobro plasiran i konkurentan, potrebno je identificirati publiku kojoj će biti namijenjen i koja će za isti biti zainteresovana.

10. Koje tehničke karakteristike treba zadovoljiti web shop kako bi bio u skladu sa sigurnosnim standardima?

Kako bi se rizici u online trgovini izbjegli, potrebno je razviti model sigurne e-trgovine kako bi se ublažili i riješili problemi u ovoj oblasti. Takav model trebao bi zadovoljavati sljedeće karakteristike (Kaushik, Gupta i Gupta, 2020):

- Ažurirani HTTPS – HTTPS postaje standard internet sigurnosti, a njegovo onemogućavanje može sa sobom nositi negativne posljedice.
- Adekvatan odabir platforme – Većina trgovina e-trgovine koristi platforme kao što su Magento i Shopify, uglavnom zbog njihove zaštite. Glavni faktori koje trgovci uzimaju u obzir prilikom odabira platforme za e-trgovinu su: praktičnost, robusnost, funkcionalnost i sigurnost.
- Upozorenje sa sigurnosnim dodacima – predstavlja dobru opciju za trgovce e-trgovinom dok vode stranice na različitim platformama. Pomenuti dodaci sprječavaju hakiranje stranica.

- Hermetički zatvorena administratorska ploča – Postoji više uglova koje hakeri mogu koristiti kako bi ušli na stranicu, a najjednostavnije je pristupiti Admin panelu, s toga je potrebno da lozinke admina budu jake i teške za hakirati.
- Sigurnosne kopije podataka (backup) – Finansijski podaci vrlo su bitni ili povjerljivi, te je neophodno imati sigurnosnu kopiju ovih podataka na redovnoj bazi na više lokacija, po mogućnosti na cloud-u i na fizičkom (hard) disku, na više lokacija.

4.3.2 Analiza Hipoteza

Nakon pregleda istraživačkih pitanja bit će provedena regresiona analiza sa svim navedenim varijablama kako bi se procijenio uticaj nezavisnih varijabli na zavisne varijable, povjerenje kupaca i odluku o kupovini.

Prva hipoteza glasila je: H1.a Informacijski dizajn web stranice ima uticaj na povjerenje kupaca.

Na slici 6. prikazan je regresioni model za hipotezu H1.a.

Slika 6. - Uticaj informacijskog dizajna na povjerenje kupaca

Source	SS	df	MS
Model	114.355959	1	114.355959
Residual	110.38434	250	.441537362
Total	224.7403	251	.895379681

Number of obs	= 252
F(1, 250)	= 258.99
Prob > F	= 0.0000
R-squared	= 0.5088
Adj R-squared	= 0.5069
Root MSE	= .66448

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Informacijskidizajn	.8770673	.0544988	16.09	0.000	.7697319	.9844026
_cons	.2410863	.2044483	1.18	0.239	-.1615743	.643747

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem informacijskog dizajna za jednu jedinicu, dolazi do povećanja povjerenja za 0,88 jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 50,88% što znači da je 50,88% varijabiliteta u povjerenju objašnjeno varijabilitetom u informacijskom dizajnu.

Druga hipoteza glasila je: H1.b Vizuelni izgled web stranice ima uticaj na povjerenje kupaca.

Na slici 7. prikazan je regresioni model za hipotezu H1.b.

Slika 7. - Uticaj vizuelnog izgleda na povjerenje kupaca

Source	SS	df	MS	Number of obs =	252
Model	99.4579693	1	99.4579693	F(1, 250) =	198.47
Residual	125.28233	250	.501129322	Prob > F =	0.0000
				R-squared =	0.4425
Total	224.7403	251	.895379681	Adj R-squared =	0.4403
				Root MSE =	.7079

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Vizuelni_izgled	.9671079	.0686483	14.09	0.000	.8319051	1.102311
_cons	-.3741709	.2759055	-1.36	0.176	-.9175663	.1692246

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem vizuelnog izgleda za jednu jedinicu, dolazi do povećanja povjerenja za 0,97 jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 44,25% što znači da je 44,25% varijabiliteta u povjerenju objašnjeno varijabilitetom u vizuelnom izgledu.

Treća hipoteza glasila je: H1.c Prethodno iskustvo u online shoppingu utiče na povjerenje kupaca.

Na slici 8. prikazan je regresioni model za hipotezu H1.c.

Slika 8. - Uticaj prethodnog iskustva na povjerenje kupaca

Source	SS	df	MS	Number of obs =	252
Model	169.884152	1	169.884152	F(1, 250) =	774.23
Residual	54.8561477	250	.219424591	Prob > F =	0.0000
				R-squared =	0.7559
Total	224.7403	251	.895379681	Adj R-squared =	0.7549
				Root MSE =	.46843

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Prethodno_iskustvo	1.427321	.0512965	27.82	0.000	1.326293	1.52835
_cons	-1.994024	.1982792	-10.06	0.000	-2.384535	-1.603514

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem prethodnog iskustva za jednu jedinicu, dolazi do povećanja povjerenja za 1,42 jedinice u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 75,59% što znači da je 75,59% varijabiliteta u povjerenju objašnjeno varijabilitetom u prethodnom iskustvu.

Četvrta hipoteza glasila je: H1.d Svijest o privatnosti utiče na povjerenje kupaca.

Na slici 9. prikazan je regresioni model za hipotezu H1.d.

Slika 9. - Uticaj svijesti o privatnosti na povjerenje kupaca

Source	SS	df	MS
Model	114.821352	1	114.821352
Residual	109.918948	250	.439675791
Total	224.7403	251	.895379681

Number of obs	= 252
F(1, 250)	= 261.15
Prob > F	= 0.0000
R-squared	= 0.5109
Adj R-squared	= 0.5090
Root MSE	= .66308

Povjerenje	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Svijest_o_privatnosti	.9426262	.0583303	16.16	0.000	.8277447	1.057508
_cons	-.033558	.2202817	-0.15	0.879	-.4674025	.4002864

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem svijesti o privatnosti za jednu jedinicu, dolazi do povećanja povjerenja za 0,94 jedinice u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 51,09% što znači da je 51,09% varijabiliteta u povjerenju objašnjeno varijabilitetom u svijesti o privatnosti.

Peta hipoteza glasila je: H2.a Informacijski dizajn web stranice utiče na donošenje odluke o kupovini.

Na slici 10. prikazan je regresioni model za hipotezu H2.a.

Slika 10. - Uticaj informacijskog dizajna na odluku o kupovini

Source	SS	df	MS
Model	36.5204549	1	36.5204549
Residual	100.443831	250	.401775323
Total	136.964286	251	.545674445

Number of obs	= 252
F(1, 250)	= 90.90
Prob > F	= 0.0000
R-squared	= 0.2666
Adj R-squared	= 0.2637
Root MSE	= .63386

Odluka_o_kupovini	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Informacijskidizajn	.495646	.051987	9.53	0.000	.3932576	.5980344
_cons	2.168104	.1950255	11.12	0.000	1.784002	2.552207

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem informacijskog dizajna za jednu jedinicu, dolazi do povećanja odluke o kupovini za 0,50

jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 26,66% što znači da je 26,66% varijabiliteta u odluci o kupovini objašnjeno varijabilitetom u informacijskom dizajnu.

Šesta hipoteza glasila je: H2.b Vizuelni izgled web stranice utiče na donošenje odluke o kupovini.

Na slici 11. prikazan je regresioni model za hipotezu H2.b.

Slika 11. - Uticaj vizuelnog izgleda na odluku o kupovini

Source	SS	df	MS		
Model	23.5322708	1	23.5322708	Number of obs =	252
Residual	113.432015	250	.45372806	F(1, 250) =	51.86
				Prob > F =	0.0000
Total	136.964286	251	.545674445	R-squared =	0.1718
				Adj R-squared =	0.1685
				Root MSE =	.67359

Odluka_o_kupo~i	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Vizuelni_izgled	.4704214	.065321	7.20	0.000	.3417718	.5990711
_cons	2.122277	.2625326	8.08	0.000	1.605219	2.639335

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem vizuelnog izgleda za jednu jedinicu, dolazi do povećanja odluke o kupovini za 0,47 jedinica u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 17,18% što znači da je 17,18% varijabiliteta u odluci o kupovini objašnjeno varijabilitetom u vizuelnom izgledu.

Sedma hipoteza glasila je: H2.c Prethodno iskustvo utiče na odluku o kupovini.

Na slici 12. prikazan je regresioni model za hipotezu H2.c.

Slika 12. - Uticaj prethodnog iskustva na odluku o kupovini

Source	SS	df	MS	Number of obs =	252
				F(1, 250) =	124.92
Model	45.6360616	1	45.6360616	Prob > F =	0.0000
Residual	91.3282241	250	.365312896	R-squared =	0.3332
				Adj R-squared =	0.3305
Total	136.964286	251	.545674445	Root MSE =	.60441

Odluka_o_kupovini	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
Prethodno_iskustvo	.7397745	.0661878	11.18	0.000	.6094178	.8701312
_cons	1.160448	.2558392	4.54	0.000	.6565726	1.664322

Izvor: kreacija autora

Na osnovu rezultata regresionog modela, može se zaključiti da sa povećanjem prethodnog iskustva za jednu jedinicu, dolazi do povećanja odluke o kupovini za 0,74 jedinice u prosjeku, uz ostale uslove nepromijenjene. Osim toga, ovaj efekat je statistički značajan jer p-vrijednost iznosi 0,000 što je manje od nivoa značajnosti od 5%. Koeficijent determinacije iznosi 33,32% što znači da je 33,32% varijabiliteta u odluci o kupovini objašnjeno varijabilitetom u prethodnom iskustvu.

Na osnovu prikazanih rezultata i provedene statističke regresije zaključujemo da su sve hipoteze potvrđene.

5. ZAKLJUČAK

E-commerce podrazumijeva online kupovinu, elektronska plaćanja i internetske aukcije. Brojnim istraživanjima je potvrđeno da je online kupovina postala dio svakodnevice, pogotovo od pandemije COVID-19. Na online kupovinu utječu faktori kao što su sigurnost, brza dostava, praktičnost, povoljne cijene i veći izbor u online trgovinama u odnosu na lokalne trgovine.

Uprkos tome što su svi oblici online transfera prilično zastupljeni širom svijeta, korisnici i organizacije još uvijek imaju određene poteškoće u primjeni ovih platformi. Najčešće se govori o problemima koji se tiču privatnosti podataka i etičkih dilemma u smislu primjene podataka koje organizacija ima o korisnicima, te sigurnosnih rizika kojima su svi korisnici izloženi. Obično se radi o klijentskim prijetnjama (zlonamjerni aktivni sadržaj – trojanski konj, virusi…), prijetnje komunikacijskim kanalom, prijetnje povjerljivosti, prijetnje integritetu, prijetnje dostupnosti ili prijetnja odgodom, prijetnje bazi podataka i prijetnje od hakiranja lozinki.

Ipak, organizacije i korisnici mogu poduzeti određene korake kako bi se uspjeli zaštititi prethodno pomenutih rizika. Neke od metoda su: firewall, autentifikacija I autorizacija podataka, enkripcija, maskiranje podataka, sigurnost zasnovana na hardveru, te sigurnosna

kopija podataka i brisanje podataka. Korisnici se također mogu zaštititi korištenjem jedinstvenom lozinkom za svaku uslugu, ne dijeliti lozinku s drugima, mijenjati lozinke i ne držati ih zapisane u datotekama na računaru ili telefonu.

Kada je riječ o zaštiti kompanije, vlasnici mogu angažovati savjetnike koji mogu pomoći u identificiranju rizika, problema i potencijalnih rješenja. Bitno je da menadžeri i organizacije prate tok razvoja informacijskih tehnologija i da budu spremni na promjene i rizike koji se mogu javiti zajedno s napretkom tehnologije. Kroz ovaj rad također su navedeni i primjeri kompanija koje su se koristile ličnim podacima korisnika i na koji način je to utjecalo na korisnike. Pa tako na primjer Google Trips predstavlja neobično i pomalo jezivo iskustvo za klijente, dok s druge strane stepen sigurnosti na stranicama Amazona pozitivno utječe na kupovinu i poslovanje kompanije.

Ovaj rad je imao za cilj da istraži uticaj informacijskog dizajna web stranice, vizuelni izgled web stranice, prethodno iskustvo i svijest o privatnosti na povjerenje kupaca u modelu 1, kao i prethodno iskustvo, informacijski dizajn web stranice i vizuelni izgled web stranice utiče na odluku o kupovini u modelu 2.

Nakon provedene ankete i istraživanja zaključeno je da je svaka hipoteza potvrđena, tj. da informacijski dizajn web stranice, vizuelni izgled web stranice, prethodno iskustvo i svijest o privatnosti utiču na povjerenje kupaca u modelu 1, kao i da prethodno iskustvo, informacijski dizajn web stranice i vizuelni izgled web stranice utiču na odluku o kupovini u modelu 2.

5.1 Naučni doprinos

Ovo istraživanja pruža dublje razumjevanje veze između izgleda web stranice, prethodnog iskustva, društvenog uticaja, svijesti o privatnosti i povjerenja kupaca na web shop stranicama kao i donošenju odluke o kupovini. Istraživanje pokazuje da su i izgled i prethodno iskustvo jako bitni u donošenje odluke o kupovini, kao i povjerenja ka web shop stranicama. Svakako, oni nalazi pružaju osnovu za daljnje detaljnije istraživanje o tome šta utiče na povjerenje kupaca, jer povećanim povjerenjem kupaca dolazimo do većeg prometa putem online web shop stranica, a samim tim i povećanja prihoda.

5.2 Praktični doprinos

Rezultati ovog istraživanja imaju praktičnu primjenu u tome da vlasnicima web shop stranica/platformi ukaže šta je to kupcima bitno i presudno u online kupovini na njihovim web shopovima. Jako je bitno da vlasnici shvate da svako negativno iskustvo doprinosi tome da ti kupci u budućnosti ne obavljaju kupovinu putem njihovih web shop stranica/platformi ili općenito nikako putem interneta.

5.3 Ograničenja i preporuke za buduća istraživanja

Iako je ovo istraživanje pružilo korisna saznanja, neka ograničenja treba ipak uzeti u obzir, Naprimjer, ova studija se fokusirala na kupce na teritoriji Bosne i Hercegovine, najviše u području Sarajeva. S toga buduće istraživanje bi se trebalo provesti na teritorijama drugih zemalja, kao i kod kupaca sa drugačijim zanimanjima, visinama mjesečnijh primanja, drugačijim obrazovanjem i slično. Također, bilo bi korisno uključiti vremensku dimenziju i analizirati uticaj motivacije i ličnih karakteristika na potrošački orijentisano ponašanje kroz određen duži period godina, kako bi se dobila sveobuhvatnija analiza.

REFERENCE

1. Al Hamli, S.S. i Sobaih, A.E.E. (2023). Factors Influencing Consumer Behavior towards Online Shopping in Saudi Arabia Amid COVID-19: Implications for E-Businesses Post Pandemic. *Journal of Risk and Financial Management*, Vol. 16, No. 1.
2. Aseri, A. (2021). Security Issues For Online Shoppers. *International Journal of Scientific & Technology Research* , Vol. 10, Issue 3.
3. Badotra, S. i Sundas, A. (2021). *A systematic review on security of E-commerce systems. International Journal of Applied Science and Engineering*, Vol. 18, No. 2.
4. Baker, D. (2019). *Selling safety - 5 keys to increase your sales influence*. Linkedin. Dostupno na: https://www.linkedin.com/pulse/selling-safety-5-keys-increase-your-sales-influence-denis (pristupljeno:28 Novembar 2023.)
5. Baubonien, Ž. i Gulevičiūtė, G. (2015). *E-commerce factors influencing consumers' online shopping decision. Social Technologies*, Vol. 5, No. 1.
6. Boso, N., Story, V.M., Cadogan, J.W., Annan, J., Kadić-Maglajlić, S. i Micevski, M. (2016). Enhancing the sales benefits of radical product innovativeness in internationalizing small and medium-sized enterprises. *Journal of Business Research*, Vol. 69., Issue 11.
7. Cavusoglu, H., Cavusoglu, H. i Raghunathan, S. (2004). *Economics of IT security management: Four improvements to current security practices. Communications of the Association for Information Systems*, Vol. 14, 2004.
8. Chehrehpak, M., Pesaran Afsharian, S. i Roshandel, J. (2014). Effects of implementing information security management systems on the performance of marketing and sales departments. *International Journal of Business Information Systems*, Vol. 15, No. 3.
9. Choi, JP., Jeon, DS. i Kim, BC. (2019). Privacy and Personal Data Collection with Information Externalities. *Journal of Public Economics*, Volume 173, Pages 113-124.
10. Choo, K. K. R. (2011). *Cyber Security: Analytics, Technology, and Automation. CRC Press*.
11. Daroch, B., Nagrath, G. and Gupta, A. (2021), "A study on factors limiting online shopping behaviour of consumers", *Rajagiri Management Journal*, Vol. 15 No. 1.
12. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why Phishing Works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '06).
13. Ennen, G (2010). *Shaping IT Security as a Factor for Success. Improving IT Security, BSI Annual Report 2010*.
14. Fortes, N. i Rita, P. (2016). *Privacy concerns and online purchasing behaviour: Towards an integrated model. European Research on Management and Business Economics*, Vol. 22, Issue 3.

15. Foxman, E. i Kilcoyne, P. (1993). Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing*, Volume 12, Issue 1.
16. Gefen, D., Karahanna, E., & Straub, D. W. (2003). *Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly*, 27(1), 51-90.
17. Ghasal, I. i Balaji, K. (2022). The Process of Providing Security Protection in the Amazon E-Commerce System. *Technoarete Journal on Advances in E-Commerce and E-Business*, Vol. 1, Issue 4.
18. Gómez, M.I., McLaughlin, E.W. i Wittink, D.R. (2004). Customer satisfaction and retail sales performance: an empirical investigation. *Journal of Retailing*, Vol, 80, Issue 4.
19. Grewal, D., Hulland, J., Kopalle, P. i Karahanna, E. (2019). The future of technology and marketing: a multidisciplinary perspective. *Journal of the Academy of Marketing Science* (2020) 48:1–8
20. Guarda, P. (2008). *Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks*.Versione 1.0 – December 2008.
21. Gurung, A. i Raja, M.K. (2016). *Online Privacy and Security Concerns of Consumers*. Information and Computer Security 24(4):348-371.
22. Herley, C. (2009). *So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. Proceedings of the 2009 Workshop on New Security Paradigms Workshop (NSPW '09).*
23. IBM Security (2020). *Strategies for managing cybersecurity risk – Assess and advance your security and compliance posture*. IBM Global Services, United States of America.
24. Interagency Security Committee (2021). *The Risk Management Process – An Interagency Security Committee Standard*.
25. Jain, V., Malivya, B. i Arya, S. (2021). An Overview of Electronic Commerce (e-Commerce). *Journal of Contemporary Issues in Business and Government* Vol. 27, No. 3, 2021.
26. Johnson, K. (2020). *Top 7 types of data security technology*. TechTarget. Dostupno na: https://www.techtarget.com/searchsecurity/feature/Top-7-types-of-data-security-technology (Pristupljeno: 15 Decembar 2023).
27. Joshi, J.M. i Dumbre, G.M. (2017). *Basic Concept of E-Commerce. International research journal of multidisciplinary studies*. Vol. 3, Issue 3, March, 2017
28. Kaushik, D.,Gupta, A. i Gupta, S. (2020). *E-Commerce Security Challenges: A Review. International Conference on Innovative Computing and Communication (ICICC 2020)*.
29. Kotler, P., & Armstrong, G. (2017). *Principles of Marketing*.
30. Lim, Y.J., Osman, A., Salahuddin, N.S., Romle, A.R. i Abdullah, S. (2016). *Factors Influencing Online Shopping Behavior: The Mediating Role of Purchase Intention. Procedia Economics and Finance*. Vol. 35, 2016.

31. Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J and Abbas S. (2022). *Cyber security threats: A never-ending challenge for e-commerce*
32. Locket, A.R. (2018). *Online Marketing Strategies for Increasing Sales Revenues of Small Retail Businesses*. Doctoral Study, Walden University.
33. Mateeva Stoyanova, Z. (2018). *Principles of personal data protection*. Audit 2, Vol. 28, pp. 95-104.
34. Noble, C.H. (2013). The Influence of Job Security on Field Sales Manager Satisfaction: Exploring Frontline Tensions. *Journal of Personal Selling & Sales Management*, Vol. 28., Issue 3.
35. Padmannavar, S. (2011). A Review on Ecommerce Security. *International Journal of Engineering Research and Applications*, Vol. 1, Issue 4.
36. Pandey, A, i Parmar, J. (2019). *Factors Affecting Consumer's Online Shopping Buying Behavior. Proceedings of 10th International Conference on Digital Strategies for Organizational Success*.
37. Pennanen, K., Kaapu, T. i Paakki, M-K. (2006). *Trust, Risk, Privacy and Security in e-Commerce*. ICEB 2006 Proceedings, 25.
38. Provost, F. i Fawcett, T. (2013). *Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking. O'Reilly Media*.
39. Ranganathan, C. i Grandon, S. (2016). An Exploratory Examination of Factors Affecting Online Sales. *Journal of Computer Information Systems*, Vol. 42, Issue 3.
40. Ransbotham, S., & Mitra, S. (2010). Choice and Quality of Information in Customer Relationship Management Systems: The Role of Sales Team Decision-Making. *Journal of Marketing Research*, 47(5), 857-865.
41. Rauš, T. (2019). *Etika u marketingu*. Diplomski rad. Sveučilište sjever, Poslovna ekonomija.
42. Rodgers, G. (2022). *Consumer Wants: Privacy Transparency, Online Security, Better Customer Experience*. CMSWire. . Dostupno na : https://www.cmswire.com/customer-experience/consumer-wants-privacy-transparency-online-security-better-customer-experience/ (Pristupljeno: 26 Novembar 2023).
43. Roohparvar, R. (2023). *The Importance of Cybersecurity for Sales and Marketing Departments. Infoguard Cyber Security*. Dostupno na: https://www.infoguardsecurity.com/the-importance-of-cybersecurity-for-sales-and-marketing-departments/ (Pristupljeno: 23 Novembar 2023).
44. Sarker, S., Sarker, S., & Sahaym, A. (2012). Examining the Relationship between Customer Relationship Management and Business Performance: A Study of the Banking Industry in Thailand. *Journal of Database Marketing & Customer Strategy Management*, 19(2), 95-113.
45. Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company*.

46. Šestak, P. i Dobrinić, D. (2019). Primjena novih tehnologija u marketingu s osvrtom na marketing stvari. *CroDiM: International Journal of Marketing Science*, Vol. 2 No. 1.
47. Taher, G. (2021). E-Commerce: Advantages and Limitations. *International Journal of Academic Research in Accounting Finance and Management Sciences*, 11(1), 153-165.
48. Tran, V.D. i Nguyen, T.D. (2022). *The impact of security, individuality, reputation, and consumer attitudes on purchase intention of online shopping: The evidence in Vietnam. Cogent Psychology*, Vol. 9, Issue 1.
49. Venkatesh, V., Hoehle, H., Aloysius, J.A. i Nikkhah, H.R. (2021). *Being at the cutting edge of online shopping: Role of recommendations and discounts on privacy perceptions. Computers in Human Behavior*, Vol. 121, August 2021.
50. Wang, Q., Zhu, X., Wang, M., Zhou, F. i Cheng, S. (2020). *A theoretical model of factors influencing online consumer purchasing behavior through electronic word of mouth data mining and analysis. PLoS Online*, Vol. 18, No. 5.
51. Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security. Cengage Learning*.
52. Yang, C., Tian, G. i Ward, S. (2007). Security systems of point-of-sales devices. *The International Journal of Advanced Manufacturing Technology*, Vol 34.
53. Ziegeldorf, J.H., Morchon, O.G. i Wehrle, K. (2013). *Privacy in the Internet of Things: Threats and Challenge. Security and Communication Networks, Security Comm. Networks 2013*.
54. Zykova, E. (2012). *Improving Marketing and Sales Support Processes in the Distribution Channel of an IT Security Company. Master's Thesis*, Helsinki Metropolia University of Applied Sciences.

PRILOZI

Prilog 1. - Anketa

Spol

Molimo vas da izaberete SAMO JEDAN od ponuđenih odgovora:

- Ženski
- Muški

Kojoj starosnoj skupini pripadate? *

Izaberite jedan od ponuđenih odgovora

Molimo vas da izaberete SAMO JEDAN od ponuđenih odgovora:

- 0-18
- 18-30
- 30-40
- 40-55
- 55+

Visina mjesečnih primanja? *

Izaberite jedan od ponuđenih odgovora

Molimo vas da izaberete SAMO JEDAN od ponuđenih odgovora:

- Manje od 1000KM
- 1000KM-2000KM;
- 2000KM-3000KM
- Više od 3000KM

Nivo obrazovanja? *

Izaberite jedan od ponuđenih odgovora

Molimo vas da izaberete SAMO JEDAN od ponuđenih odgovora:

- SSS
- VŠS
- BA

- MR
- DR

Odaberite odgovarajući odgovor za svaku stavku:

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
Ne smeta mi da dijelim privatne fotografije na internetu.					
Nemam ništa protiv da objavim na internetu informacije o mojoj trenutnoj lokaciji.					
Nemam ništa protiv da objavim na internetu informacije o tome s kim sam u ovom trenutku.					
Obavljao sam kupovinu putem web shop platformi/stranica i ranije.					

Koje web shop stranice/platforme poznajete?

Možete izabrati više ponuđenih opcija

Izaberite **sve** što vrijedi:

- eBay
- Amazon
- AliBaba
- AliExpress
- Olx.ba
- ASOS
- Udemy
- kupujemprodajem.com
- Ostalo: *****

Odaberite odgovarajući odgovor za svaku stavku:

	1 - Apsolutno se ne slažem	**2 - Ne slažem se**	**3 - Niti se slažem, niti se ne slažem**	**4 - Slažem se**	**5 - Apsolutno se slažem**
Smatram da su općenito informacije na web shop stranicama logično predstavljene.					
Smatram da su općenito informacije na web shop stranicama dobro organizirane.					
Sve opcije proizvoda,					

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
atributi proizvoda i informacije o proizvodu su inače dobro i jasno predstavljene.					
Web shop stranice imaju općenito atraktivne boje i pozadinu ekrana.					
Web shop stranice imaju privlačne slike i naslove na početnoj stranici.					
Animacije web shop stranica su smislene i logične.					
Grafika i slike korištene na web shop stranicama dobro se uklapaju sa sadržajem.					

Odaberite odgovarajući odgovor za svaku stavku:

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
Vjerujem da su web shop stranice iskrene i istinito predstavljaju podatake o proizvodima.					
Platforma me uvijek upozori ako ima mogućnosti za neku vrstu prevare vezane za kvalitet proizvoda, plaćanja ili slično.					
Nisam imao problema sa prevarama prilikom online plaćanja.					
Nisam osjetljiv na način na koji online kompanije rukuju sa mojim personalnim informacijama.					
Nisam zabrinut za moju privatnost na web shop stranicama.					

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
Nisam zabrinut da će moji lični podaci biti prikupljeni i zloupotrebljeni.					
Veoma mi je važno da sam svjestan i upućen u to kako će se moji lični podaci koristiti.					
Web shop stranice koje traže informacije na mreži trebale bi otkriti način na koji se podaci prikupljaju, obrađuju i koriste.					

Odaberite odgovarajući odgovor za svaku stavku:

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
Nisam imao problema sa isporukom u prošlosti.					

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
Zbog prethodnog iskustva sam oprezniji u online kupovini.					
Veća je vjerovatnoća da ću obaviti online kupovinu ako sam ranije čuo/vidio/čitao pozitivne stvari o kompaniji.					
Veća je vjerovatnoća da ću obaviti online kupovinu ako sam imao pozitivno prošlo iskustvo u komunikaciji s kompanijom (npr. služba za korisnike, račun na društvenim mrežama).					
Vjerovatnije je da ću obaviti online kupovinu ako sam imao pozitivno iskustvo u prošlosti s proizvodima/uslugama kompanije.					
Veća je vjerovatnoća da ću obaviti online kupovinu ako vrijednosti kompanije odgovaraju mojim etičnim i moralnim vrijednostima.					

Odaberite odgovarajući odgovor za svaku stavku:

	1 - Apsolutno se ne slažem	2 - Ne slažem se	3 - Niti se slažem, niti se ne slažem	4 - Slažem se	5 - Apsolutno se slažem
Većina mojih prijatelja koristi web shop-ove s toga ih koristim i ja.					
Online kupovina mi olakšava kupovinu i štedi vrijeme.					
Web shop stranice mi omogućava pristup online recenzijama.					
Čitam online recenzije prije kupovine.					
Recenzije na mreži olakšavaju mi korištenje e-trgovine.					
Vjerujem da ću u budućnosti više kupovati putem interneta.					