INTERNET SIGURNOST I E-TRGOVINA

Pereža, Dino

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

INTERNET SIGURNOST I E-TRGOVINA

Mentor: **Student:**

Izv.prof.dr.sc. Mario Jadrić **Dino Pereža**

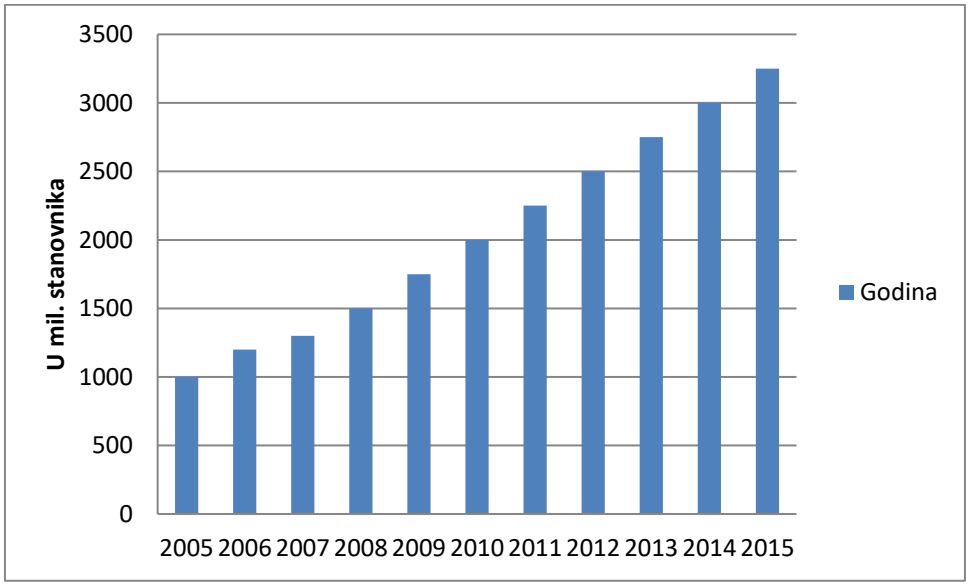
Split, kolovoz, 2017.

SADRŽAJ:

1. UVOD

1.1. Definicija problema istraživanja

Internet broji svaki dan sve više korisnika. Prema svjetskoj internet statistici[1] broj korisnika na dan 31.03.2017 bio je 3.739.698.500 (3,7 biliona korisnika). U usporedbi sa godinom 2000 to je porast od 936%. Procjena[2] je da će do 2020. godine Internet brojati 4,1 bilion korisnika. Ove brojke ukazuju na to da je Internet pogodno mjesto za ostvarivanje raznih poslovnih ideja jer ima velik broj potencijalnih klijenata. Tako se sredinom devedesetih godina 20. stoljeća počinje masovno koristit za razne poslovne pothvate.

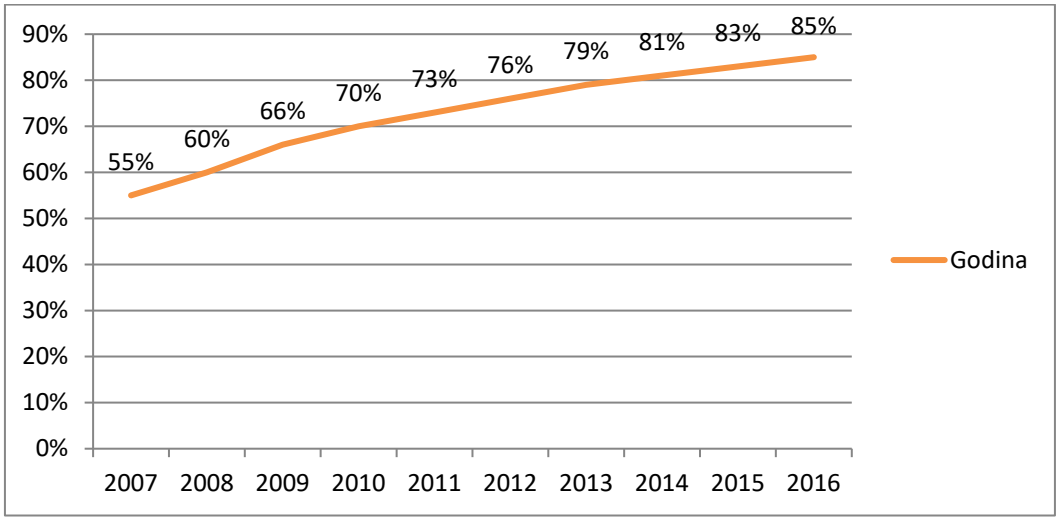


Grafikon 1 Broj korisnika Interneta
Izvor: Izrada autora prema Global Internet report 2016

Svako masovno širenje pa tako i masovno širenje interneta kao jednog novog globalnog gospodarskog prostora povlači za sobom pozitivne ali i negativne strane. Kao i u pravom svijetu i u ovom virtualnom svijetu ima prevara, krađa novaca, krađa identiteta te zlouporaba Vaših osobnih podataka. E-poslovanje i e-trgovina je nešto sa čime se gotovo sigurno susreo svaki korisnik Internet usluga a da toga možda nije ni bio svjestan.

[1] Internet world stats [Internet], raspoloživo na na http://www.internetworldstats.com/stats.htm
[2] Gemalto [Internet], raspoloživo na http://www.gemalto.com/review/Pages/infographic-the-number-of-internet-users-by-2020.aspx

U današnje vrijeme je internet nešto bez čega ne bih smo mogli, a njegovo širenje ne staje. E-trgovina postaje sve popularnija i zastupljenija na Internetu. Svaka veća i ozbiljnija tvrtka ima neki oblik web trgovine, ali sada postaju sve popularnija manja poduzeća i start-up firme koje se baziraju samo na e-trgovini. E-trgovina postaje sve raširenija a društvo, te posebice poslovno okruženje nije dovoljno upoznato sa svim rizicima takvog načina poslovanja



Grafikon 2 Postotak kućanstva koja korsite internet u EU
Izvor: Izrada autora prema http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en

1.2.Cilj rada

Cilj ovog rada je upoznavanje krajnjih korisnika sa značajem e-trgovine. Dakle obrazložit što je e-trgovina, koje su njene mogućnosti te najbitnije upoznat krajnje korisnike sa mogućim rizicima e-trgovine sa posebnim naglaskom na sigurnosti pri e-kupovini. U radu će se pokazati moguće mjere zaštite općenito na Internetu te pri e-trgovini.

1.3.Metode rada

U svrhu ostvarivanja cilja rada u radu će biti korištene različite metode i to:

1.) U teorijskom dijelu:
   1.1.Metoda analize i sinteze
   1.2.Metoda indukcije i dedukcije
   1.3.Metoda komparacije

2.) U empirijskom dijelu:

2.1. Metoda ankete – u anketi će se ispitat dob korisnika e-trgovine, njihove kupovne navike te njihovo poznavanje osnovnih pojmova pri zaštiti na Internetu te pri samo e-kupovini

1.4 Struktura rada

Rad se sastoji od uvodnog djela gdje je opisana problematika rada, cilj rada te metode korištene u izradi rada. U drugom djelu rada bit će opisan značaj e-trgovine u e-poslovanju, ponašanje korisnika na Internetu i pri e-kupovini, povijest e-trgovine i e-trgovina u Europi. Nakon toga bit će opisana kratka povijest Interneta i upoznat ćemo se sa vrstama napada na Internetu. Tu će bit uključene i vrste napad pri samoj e-kupovini te će se objasnit na koje sve načine se možemo zaštitit od istih. Empirijski dio rada sastojat će se od analize ankete koja će nam pokazati koliko krajnji korisnici znaju o zaštiti na Internetu. Na samom kraju rad će sadržavati zaključak, kratak sažetak, literaturu i popis svih priloga.

2. TEORIJSKI ASPEKTI E-TRGOVINE

2.1. Značaj e-trgovine u e-poslovanju

Prvo ćemo definirat što je to e-trgovina, a što e-poslovanje. Kao i kod mnogih drugih novijih pojmova iz područja informacijskih znanosti, definiranje e-trgovine i e-poslovanja nije jednoznačno. Panian (2000 i 2013) definira e-trgovinu kao "proces kupnje, prodaje ili razmjene proizvoda, usluga ili informacija putem javno dostupne računalne mreže, Interneta, a nudi veliko smanjenje troškova i vremena transakcija“[3]. Dok e-poslovanje definira kao suvremeni oblik organizacije poslovanja koji podrazumijeva intenzivnu primjenu informatičkih i, posebice, internetskih tehnologija u svim ključnim odnosno jezgrenim poslovnim funkcijama i procesima.[4]

Razmotrit ćemo i definiciju e-poslovanja koju nam daje Ružić et al. (2009), a ona glasi : “Proces korištenja informacijskih tehnologija (IT) da podrži punu operacionalizaciju poslovanja. To može uključivati generalno vodstvo, podržavanje potpore prodaji, integrirane partnere, i povezanosti poslovnih operacija s dobavljačima i distributerima pomoću extraneta.“[5]

Složenost pojma e-poslovanje možemo izrazit sljedećom formulom[6]:

EB = EC + BI+ CRM + SCM + ERP

EB (e-business) – e-poslovanje
EC (e-commerce) – e-trgovina
BI (Business intelligence) – poslovna inteligencija
CRM (Customer relationship management) – management odnosa sa potrošačima
SCM (Supply chain management) – efikasna isporuka proizvoda i usluga kroz veću suradnju i interakciju sa posrednicima
ERP (Enterprise resource planning) – optimizacija poslovnih procesa i snižavanje troškova kroz optimalizaciju nabave i prodaje kontrolom zaliha i fakturiranja

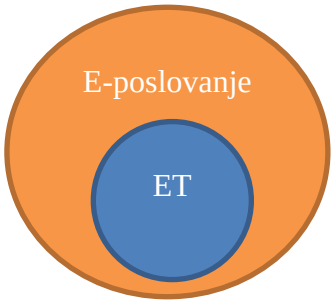
Dakle moglo bi se reći da je e-poslovanje širi pojam, tj. da je e-trgovina dio e-poslovanja. E-trgovina podrazumijeva prodaju, kupovinu, marketing, preuzimanje narudžbi, službu za

[3] Panian, Ž. (2000). Elektroničko trgovanje
[4] Panian, Ž. (2013). Elektroničko poslovanje druge generacije, str 13.
[5] Ružić, d., Biloš, A., Turkalj, D. (2009) : e-Marketing, str. 5
[6] Strauss, j., Frost, R. (2001): E-marketing, drugo izdanje str.6

korisnike, kupnju potrošnog materijala za proizvodnju itd. Kao što se vidi e-trgovina nije samo kupovina i prodaja preko Interneta već uključuje i aktivnosti koje se događaju prije ali i poslije kupovine. A e-poslovanje uz sve što podrazumijeva e-trgovina obuhvaća i interne procese kao što su proizvodnja, upravljanje zalihama, razvoj proizvoda, upravljanje rizicima, upravljanje znanjem, upravljanje ljudskim resursima, upravljanje financijama itd. Dakle e-poslovanje je više usredotočeno na interne procese i usmjereno je na uštedu troškova te poboljšanje učinkovitosti i produktivnosti.

Chaffey (2007.) ukazuje na niz različitih perspektiva e-trgovine[7]:

- Komunikacijska perspektiva – razmjena informacija, proizvoda te usluga ili plačanja elektronskim putem
- Poslovno procesna perspektiva – primjena tehnologije u automatiziranju poslovnih transakcija i tijeku rada tj. poslovanja
- Uslužna perspektiva – omogućuje rezanje troškova te u isto vrijeme povećava brzinu i kvalitetu pružanje usluga
- On-line perspektiva – kupovina i prodaja proizvoda i informacija online



Slika 1 Odnos E-poslovnja i E-trgovine (ET)
Izvor: Izrada autora

[7] Chaffey, D (2007). E-business and E-commerce management, str 8.

2.1.1. Povijest e-trgovine

Počeci e-trgovine datiraju iz 1960-te godine. Tada je razvijen „Electronic Data Interchange“ (EDI; hrv. elektronička razmjena podataka). EDI se definira kao prijenos strukturiranih podataka, prema dogovorenim standardima, od jedne računalne aplikacije do druge, elektroničkim putem uz minimalnu ljudsku intervenciju.[8] EDI je zamijenio tradicionalno dostavljanje narudžbenica, otpremnica, računa, obavijesti o plaćanju, stanje skladišta, itd. digitalnim načinom tj. prijenosom podataka sa jednog računala na drugo. U početku su samo tvrtke razmjenjivale podatke dok je odnos tvrtke direktno prema kupcu nastao kasnije kad se raširila upotreba PC-a[9] u kućanstvu te kada je nastao World Wide Web. Tada su se počele kreirati prve web stranice i prve e-trgovine.

2.1.2.Modeli e-trgovanja

Tablica 1 Modeli e-trgovine prema sudionicima

	Tvrtka	**Kupac**	**Vlada**
Tvrtka	B2B (Business to Business)	B2C (Business to Customer)	B2G (Business to Governmeent)
Kupac	C2B (Customer 2 Business)	C2C (Customer to Customer)	C2B (Customer to Government)
Vlada	G2B (Government to Business)	G2C (Governemt to Customer)	G2G (Government to Government)

Izvor: Izrada autora

Modele možemo podijelit na :

I. Business to Business (B2B) – označava trgovinu između dvije tvrtke. Ovdje ne sudjeluje krajnji potrošač već tvrtke međusobno razmjenjuju tj. kupuju proizvode i materijale te usluge

[8] OptimID (2012): EDI – što je to? [Internet], raspoloživo na http://www.optimit.hr/hr/edi/-/asset_publisher/6a93Ij7DSOHe/content/edi-sto-je-to-

[9] PC = personal computer (osobno računalo)

koje im trebaju za vlastitu proizvodnju. Panian (2000) B2B definira kao računalnu trgovinu u kojoj poslovni potrošač cilja poslovnog potrošača.

II. Business to Customer (B2C) – označava poslove između privatne tvrtke kao ponuditelja i fizičke osobe kao klijenta. Poznati primjeri za B2C su eBay.com, Amazon.com, AliExpres itd.

III. Business to Government (B2G) – označava poslove gdje je privatna tvrtka ponuditelj a država je klijent.

IV. Customer to Business – označava npr. kada kupac napravi neki projekt sa određenim budgetom te se onda tvrtke on-line prijavljuju tj. nadmeću da dobe taj projekt

V. Customer to Customer (C2C) – označava poslove između fizičkih osoba. Neki od primjera su njuškalo.hr, e-Bay, Fcebook itd.

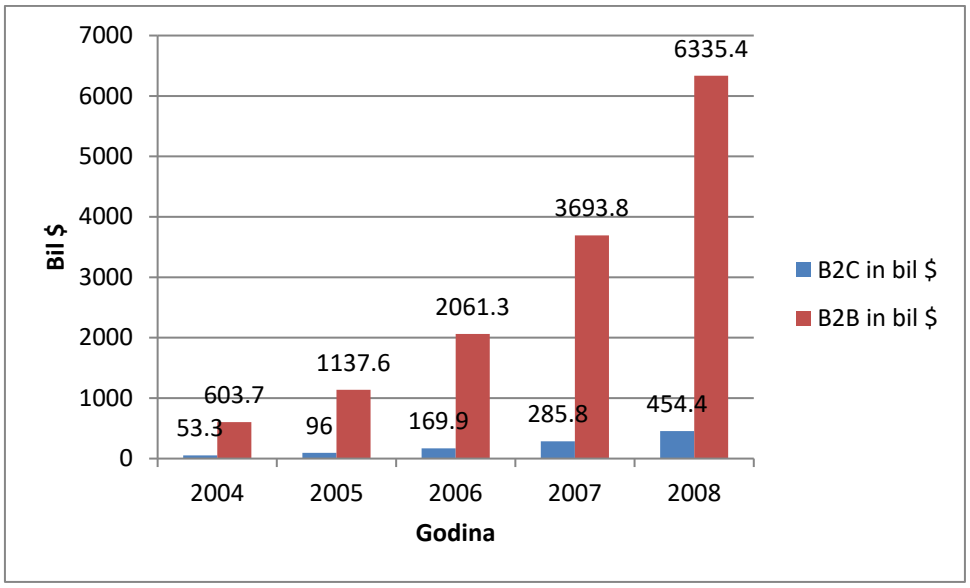
VI. Customer to Government (C2G) – označava poslove u kojima je fizička osoba ponuditelj a država klijent. Tu se uvrštavaju i povratne informacije (feedback) prema vladi kroz razne Internet stranice

VII. Government to Business (G2B) – označava poslove u kojima je država ponuditelj a privatna tvrtka je klijent (obveza plaćanja poreza, razne regulative itd)

VIII. Government to Customer (G2C) – označava aktivnosti gdje je država ponuditelj a fizička osoba kupac (npr. e-građanin, razne informacije od strane vlade, porezi)

IX. Governmnt to Government (G2G) – označava poslovanje između dvije države (razmjena informacija, roba, usluga)

Dva modela sa kojima se najčešće susrečemo te dva modela koja su najpoznatija su Business to Business (B2B) te Business to Customer (B2C). U početku je bio razvijen samo B2B dok je B2C tek zadnjih nekoliko godina doživio velik uspon. B2B i dalje ostvaruje novčano veći promet dok sa druge strane B2C ostavruje kvantitativno (prodaje se više proizvoda i usluga) veći promet.



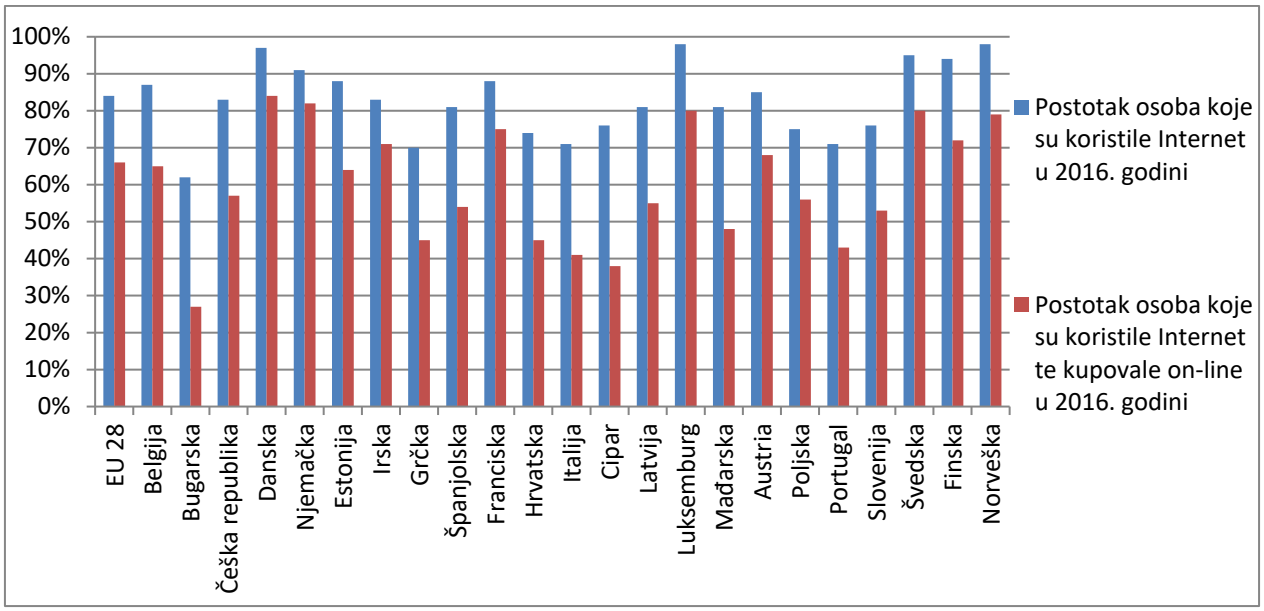
Grafikon 3 Usporedba prihoda B2B i B2C prihoda
Izvor: Izrada autora prema Grbavac (2002)

Na grafikonu 3 je vidljivo kolika je to razlika u prihodima između B2B trgovine te B2C trgovine. Prihodi jedne i druge trgovine rastu no B2B raste mnogo brže. Kako postoje stranice za B2C trgovinu kao na primjer eBay ili Amazon tako postoje i e-tržišta za B2B trgovinu. Jedno takvo tržište je ECeurope[10] gdje se nalazi preko 100 trgovinskih mrežnih stranica.

2.2. E-trgovina u Europi

U ovom poglavlju ćemo prikazat statistiku korištenja Interneta te e-trgovine u državama članicama EU.

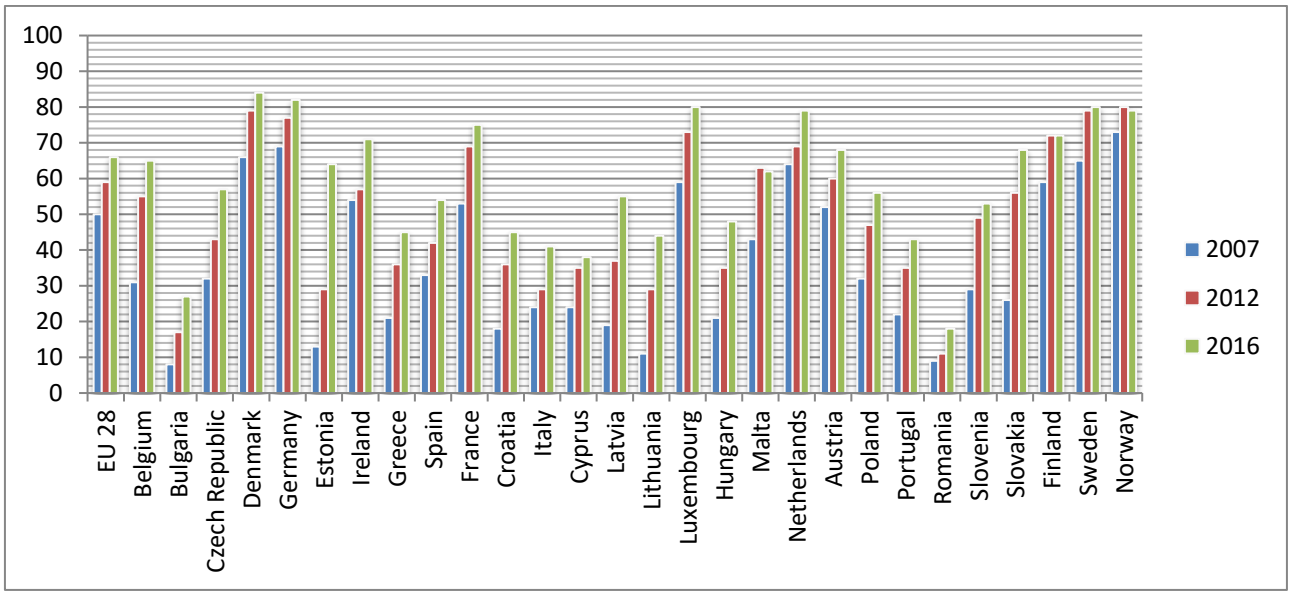
10 ECeurope [Internet],raspoloživo na http://www.eceurope.com/



Grafikon 4 Korištenje interneta te e-kupovina u 2016.
Izvor: Izrada autora prema Eurostatu[11]

Grafikon 4 uspoređuje koliko posto od ukupnog broja stanovnika neke države je koristilo Internet u 2016. godini te koliki postotak tih istih je obavilo on-line kupnju. Prema grafikonu je vidljivo da skoro u svakoj državi 2/3 korisnika koji koriste Internet obavljaju i on-line kupovinu, u nekim država je taj omjer i veći. Isto tako je na razini cijele EU 28. Od 84% osoba koje koriste Internet njih 66% je obavilo neku vrstu e-trgovine u 2016. godini. Prema podacima Eurostata europljani on-line najviše kupuju odjeću te sportsku opremu (njih 61%), iza toga slijede putovanja te bookiranje smještaja za odmor (52% kupaca).

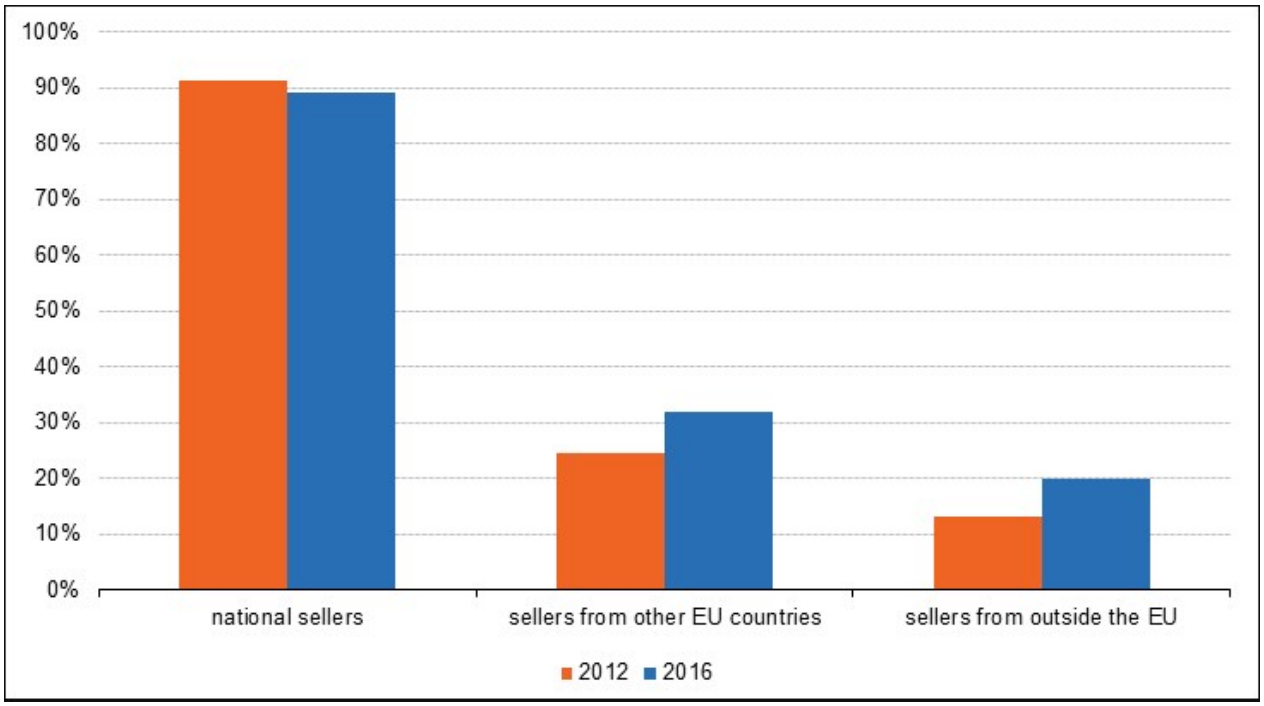
11 Eurostat: E-commerce statistics for individuals [Internet], raspoloživo na http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals



Grafikon 5 Porast e-trgovine u Europi
Izvor: Izrada autora prema Eurostatu[12]

Grafikon 5 prikazuje usporedno porast e-trgovine prema državama za godine 2007., 2012. te 2016. Svaki stupac označava koliko posto korisnika Interneta je te godine obavilo on-line kupnju. Vidi sa da e-trgovina osjetno raste svake godine, a njen daljnji rast se i dalje predviđa. Gledajući na razini članica EU 28 u 2007. godini je 50% ukupnog broja Internet korisnika obavilo neki oblik on-line kupnje dok je 2016. to obavilo 66% korisnika. Gledajući prema godinama, najviše on-line kupnje obavlja mlada populacija između 16-24 godine. Slika2 nam prikazuje da kupuju najviše na tržištu države iz koje dolaze. Samo manji dio je kupovao iz država ostalih članica EU dok je najmanji postotak onih koji su kupovali robu iz država koje nisu članice EU (uključujući i države van Europe). Isti takav trend je bio i 2012. godine. Sve više Internet korisnika se upušta u e-trgovinu no vrlo malo njih zna kako se pravilno zaštiti tj. kako se ponašat pri e-kupovini.

[12] Eurostat:Internet purchases by individuals [Internet], raspoloživo na http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_ibuy&lang=en



Slika 2Nacionalna i internacionalna e-kupovina u postocima
Izvor: Eurostat[13] National and cross-border purchases by e-shoppers

Ova slika nam pokazuje da su ljudi i dalje zabrinuti kod kupovine van svoje države jer nisu sigurni u pouzdanost tih trgovaca. No vidi se blagi trend opadanja domaće kupovine dok inozemna e-kupovina raste. U ovom radu se želi ljude upoznat sa mogućim rizicima općenito pri korištenju Interneta i pri e-kupovoni. Rizici i prijetnje postoje neovisno da li se radi o inozemnoj ili tuzemnoj e-kupovini.

[13] Eurostat: National and cross-border purchases by e-shoppers [Internet], raspoloživo na https://goo.gl/2uWxXs

3. SIGURNOST NA INTERNETU

3.1.Što je Internet?

Kako kod svih informatičkih pojmova, tako i za pojam Internet postoji mnogo različitih definicija. Za početak pokušat ćemo objasnit što je Internet riječima Tim Bernersa, osnivača WWW konzorcija. On objašnjava Internet na sljedeći način: "Internet je sličan razglednici s adresom. Ako stavite ispravnu adresu na paket te ga predate bilo kojem računalu koje je spojeno na mrežu, svako će računalo naći liniju kojim će poslati paket kako bi stigao na svoje odredište. To je što nam Internet pruža. Dostavlja pakete − u sekundi bilo gdje na svijetu"[14]

Općenita definicija Interneta na koju se često nailazi glasi: "Internet je javno dostupna globalna paketna podatkovna mreža koja zajedno povezuje računala i računalne mreže korištenjem istoimenog protokola (internetski protokol = IP). To je "mreža svih mreža" koja se sastoji od milijuna kućnih, akademskih, poslovnih i vladinih mreža koje međusobno razmjenjuju informacije i usluge kao što su elektronička pošta, chat i prijenos datoteka te povezane stranice i dokumente World Wide Weba."[15]

Internet je nastao početkom 60-tih godina 20. stoljeća. Tada su američki znanstvenici koji su radili za Američko ministarstvo obrane osmislili kako povezati dva računala sa udaljenih sveučilišta. Povezali su ih dial-up vezom preko telefonske linije. Tim koji je to izumio zvao se ARPA (engl. Advanced Research Projects Agency) te se s toga prva računalna mreža zvala ARPANET. Mrežna su računala bila 16-bitna s 12 KB memorije, a međusobno su bila povezana mrežnim linijama od 56 kbps (engl. kbps = kilobits per second). Do godine 1971. u ARPANETU je sudjelovalo oko 30 sveučilišta. Prva javna objava bila je 1972. godine na konferenciji zvanoj " International Computer Communication Conference". Od tada se mreža samo širila i razvijao se Internet kakav je danas nama poznat.

[14] The history of the Internet [Internet], raspoloživo na https://www.infoplease.com/history-internet-0
[15] Internet [Internet], raspoloživo na https://hr.wikipedia.org/wiki/Internet

3.2.Internet napadi

3.2.1. Vrste Internet napada

Svaki PC korisnik bi morao imati instaliran antivirusni program na svom računalu. On bi se trebao nalazit na svakom računali bez obzira da li to računali pristupa Internetu ili ne. Antivirusni programi su sve napredniji ali isto tako napreduju i razni zlonamjerni softveri. To je jedna vječna borba između antivirusnih programa te zlonamjernih softvera. Čest naziv za zlonamjere softvere koji se koristi i kod nas je Maleware. To je složenica od engleski riječi malicious i software.

Prema autorima Bott i Siechert (2003) najčešći tipovi malware-a na koje se može naići tj. koji nas mogu napasti su:[16]

- Virus – on je dio koda koji se replicira povezivanjem s drugim objektom, obično bez znanja ili dozvole korisnika. Virusi mogu zaraziti programske datoteke, dokumente (u obliku makro virusa), ili strukture diska i datotečnih sustava niske razine kao što su sektor za podizanje sustava (boot sector) ili particijska tablica. Virusi se pokrenu kada se pokrene zaražena programska datoteka. Oni također mogu boraviti u memoriji i zarazit datoteke kada ih korisnik otvori, spremi ili napravi datoteku. Kada virus inficira računalo koji pokreće operativni sustav Windows, on može mijenjat vrijednosti u registru (eng. registry), zamijenit neke sistemske datoteke i preuzeti e-mail program u pokušaju da sam sebe replicira (u tom trenutku postaje crv). Virusi ne moraju biti zasebni programi niti su nužno destruktivni, ali većina ih je.
- Crvi (eng. Worms) – su nezavisni programi koji se repliciraju kopiranjem s jednog računala na drugo, pretežito preko mreže ili preko e-mail privitaka. Najvirulentnija izbijanja zloćudnih softvera posljednjih godina se baziraju na crvu. Mnoge od tih prijetnji sadrže kod dizajniran za uništavanje datoteka ili za pokretanje denial-of-service (DoS) napada (on preoptereti računalo tako da ga više nitko ne može koristit; postane prespor).
- Trojanski konji – su programi koji se izvode bez znanja ili pristanka žrtve; iako mogu biti bezopasni, većina trojanskih konja u cirkulaciji danas obavljaju funkcije koje ugrožavaju sigurnost računala tako što iskorištavaju korisnička pristupna prava i privilegije. Trojanski

[16] Bott, E., Siechert, C. (2003); Microsoft Windows Security Inside Out for Windows XP and Windows 2000 str.295

konj može doći kao e-mail privitak ili može biti skinut sa Interneta tako što bude prikriven kao neka druga vrsta softvera. Napadači se obično oslanjaju na bazu socijalnog inženjeringa kako bi navukli žrtvu da instalira program. Na primjer, napadač se može javit žrtvi preko nekog chata ili poruke i upozorit da Internetom kruži opasan virus i poslati link na Trojanskog konja koji se maskira kao antivirusni program.

Uz ove tri vrste koje navode Bott i Siechert ima još načina putem kojih napadač može doći do Vaših podataka. Neki od njih su:[17]

- Spyware - je široka kategorija malicioznog softwarea sa namjenom da presreće ili preuzima djelomično kontrolu rada na računalu bez znanja ili dozvole korisnika. Dok sam naziv sugerira da je riječ o programima koji nadgledaju rad korisnika, ovaj naziv danas označava široku paletu programa koji iskorištavaju korisničko računalo za stjecanje koristi za neku treću osobu. Spyware se razlikuje od virusa i crva u tome što se obično ne replicira. Kao mnogi novi virusi, spyware je dizajniran da iskorištava zaražena računala za komercijalnu dobit.
- Rootkit - Označava tehniku prikrivanja. Načini se nevidljivim OS-u, uključujući antivirusne programe i sistemske alate .Napadaču omogućuje neovlašteno dobivanje adiministratorskih ovlasti te prikrivanje znakova malicioznih aktivnosti na kompromitiranom računalu.

  Dvije osnovne vrste rootkit alata:

  - Aplikacijska: metoda zamjene legitimnih datoteka s malicioznima kako bi se prikrila napadačeva prisutnost i neovlaštena aktivnost u sustavu.
  - Kernelski: na razini jezgre operacijskog sustava, integrirani u sam operacijski sustav.

- Phishing[18] - je vrsta socijalnog inženjeringa koja se odnosi na prijevare, kojima se služe zlonamjerni korisnici šaljući lažne poruke koristeći pritom postojeće Internet servise. Riječ je o kriminalnoj aktivnosti. Koristeći razne načine manipulacije, kriminalci od

[17] Što su virusi i ostali zlonamjerni programi [Internet]; raspoloživo na https://sites.google.com/site/zlonamjerniprograminainternetu/
[18] O phisingu [Internet], raspoloživo na http://www.cert.hr/phishing

korisnika pokušavaju prikupiti povjerljive podatke (korisnička imena, lozinke, podaci s kreditnih kartica i sl.) kako bi ostvarili financijsku korist. U pravilu, phishing poruke prenose se putem elektroničke pošte koja navodi korisnika da klikne na određeni link koji ga dalje vodi na stranice zloćudnog web poslužitelja. Takve zloćudne Web stranice obično se lažno predstavljaju kao Web stranice banaka, servisa za elektroničko plaćanje (PayPal i dr.) i sl. krivotvoreći, odnosno imitirajući njihov izgled. U svrhu phishing-a, osim elektroničke pošte, mogu poslužiti i drugi servisi poput foruma, servisa za izravnu komunikaciju (Skype, Google Talk, Facebook Messenger i dr.) te društvene mreže (Facebook, Twitter). Društvene mreže posebno su opasne jer podaci prikupljeni sa njih mogu poslužiti za krađu identiteta, ali i zbog činjenice da poruke dobivene od prijatelja, kojima su kompromitirani (oteti) računi, imaju određeni kredibilitet.

- Spoofing[19] – Internetski spoofing znači kreiranje lažne ili krivotvorene verzije nečega, poput Web lokacije ili adrese e-pošte. Na primjer, mnogi kradljivci identiteta postavljaju lažne Web lokacije koje izgledaju isto kao i stvarne i navode korisnike na te lokacije. Kada se jednom nađe na odredištu, korisnik se prijavljuje sa svojim korisničkim imenom i lozinkom, koje tako dolaze u ruke kriminalcima, a oni ih zlorabe za pristup stvarnoj Web lokaciji.

[19] Conry-Murray, A., Weafer, V. (2005): Sigurni na Internetu, str.12

	Spyware	Virusi	Crvi	Trojanski konji
Rezidentnost u radnoj memoriji	Ne	Da/Ne	Da	Ne
Mogućnost replikacije	Ne	Da	Da	Ne
Zapisivanje na tvrdi disk	Da	Da	Ne	Da
Razina rizika	Visoka	Srednje visoka	Visoka	Visoka
Primjetnost prisutnosti na računalu	Da	Da	Ne	Ne
Izvori zaraze	Internet	Internet, prijenosni računalni mediji (CD, DVD, USB)	Internet	Internet
Učinak na normalan rad računala	Da	Da	Da/Ne	Da/Ne
Utjecaj na pouzdanost podataka na računalu	Ne	Da	Da	Da
Otvaranje mogućnosti za drugu vrstu napada	Ne	Ne	Da	Da
Mogući napadi	-	-	DDoS, MITM	DDoS, MITM
Opasnost od uništavanja podataka	Ne	Da	Da	Ne
Opasnost od krađe podataka	Da	Ne	Da	Da
Nadgledanje aktivnosti na računalu	Da	Ne	Ne	Da

Slika 3 Usporedba zlonamjernih programa
Izvor: CARNet, CERT, LS&S: „Spyware programi“, CCERT-PUBDOC-2009-10-280, str. 9, raspoloživo na: http://sigurnost.lss.hr/documents/index.html

Kako Microsoft navodi postoji 10 nepromjenjivih zakona sigurnosti:[20]

- Ako vas negativac može uvjeriti da pokrenete program na računalu, to više nije samo vaše računalo.
- Ako negativac može mijenjati operacijski sustav na računalu, to više nije vaše računalo.
- Ako negativac ima neograničeni fizički pristup vašem računalu, to više nije vaše računalo.
- Ako dopustite negativcu pokretanje aktivnog sadržaja na vašoj web stranici, to više nije vaše web mjesto.
- Slabe lozinke kompromiraju jaku sigurnost.
- Računalo je jednako sigurno koliko je i administrator pouzdan.
- Šifrirani podaci sigurni su samo koliko i ključ za dešifriranje.
- Zastarjeli antimalware skener je samo fiktivno bolji nego da uopće nemate skener.
- Apsolutna anonimnost praktički nije ostvariva, online ili offline.
- Tehnologija nije panaceja

[20] Microsoft: 10 immutable laws of security [Internet]; raspoloživo na https://technet.microsoft.com/en-us/library/hh278941.aspx

3.2.2. Povrede sigurnosti

Gledano kroz povijest od nastanka Intraneta, broj povreda Internet sigurnosti svake godine raste. Napadaju se privatne osobe ali u većini slučajeva hakeri napadaju tvrtke kako bih se domogli podataka koje tvrtke imaju u svojim bazama.

Prema Gemaltu[21] u 2016. godini se dogodilo 1792 napada koji su doveli do ugrožavanja 1.4 biliona datoteka. Ovdje su urečunati samo napadi koji su prijavljeni od strane tvrtke koje su bile napadnute. Taj broj je sasvim sigurno podcijenjen jer jedan dio tvrtki nije prijavilo napade, a jedan dio tvrtki nije možda ni primijetio da su napadnuti tj. da je netko upao u njihov sistem te samim time nisu ništa niti prijavili. Brojevi koji su izneseni su za 86% veći nego 2015. godine. Najveći broj, čak 59% ukupnog broja povreda sigurnosti odnosi se na krađu identiteta.

3.2.3. Kako se zaštiti prije nego odemo on-line?

Kao što smo vidjeli u prethodnim poglavljima Internet je velik prostor na kojem ima mnogo korisnika te samim time i mnogo sadržaja ali i raznih prijetnji. Postoji nekoliko koraka tj. stvari koje bi trebalo napravit prije nego se povežemo on-line. One najbitnije će biti objašnjene u nastavku:

1. Pazite da vam je operacijski sustav ažuriran

Svaki softver pa tako i OS koji koristite nikada nije 100% savršen. Uvjek se tokom rada softvera primijete još pogreške koje se trebaju ispravit. Tako je i sa operacijskim sustavom. Neovisno koji OS koristite (Windows, iOS, Linux…) uvijek trebate biti siguran da imate zadnju verziju. Svi proizvođači (Microsoft, Apple…) izbacuju zakrpe i ažuriranja za svoje operacijske sustave tokom godina. Zato je vrlo važno imati legalnu verziju operativnih sustava jer ćete tako uvijek biti pravovremeno obaviješteni o novom ažuriranju i bit ćete sigurniji kada ste on-line.

[21] Gemalto [Internet]; raspoloživo na http://www.gemalto.com/

2. Instalirajte vatrozid (eng. Firewall)

Vatrozid preuzima ulogu zaštitara. Postoje dvije vrste vatrozida: softverski vatrozid i hardverski vatrozid. Softverski firewall štiti jedno računalo, osim u slučaju kada je to računalo predodređeno za zaštitu čitave mreže. Hardverski firewall omogućuje zaštitu čitave mreže ili određenog broja računala. Vatrozid je prvi korak pružanja sigurnosti računalu. On stvara prepreku između računala i bilo kojeg neovlaštenog programa koji pokušava doći putem Interneta. Ako koristite internet kod kuće, trajno uključite vatrozid. To vas čini svjesnim ima li neovlaštenih pokušaja za pristupanju Vašem računalu i kućnoj mreži.

3. Instalirajte antivirusni program

Prema TechTerms rječniku antivirusni softver je vrsta uslužnog programa koji se koristi za skeniranje i uklanjanje virusa s vašeg računala. Dok postoje mnoge vrste antivirusnih (ili "protuvirusnih") programa, njihova primarna svrha je zaštititi računala od virusa i ukloniti sve pronađene viruse.[22]

To je program koji se pali prilikom pokretanja operacijskog sustava te uvijek radi u pozadini. On pregledava i skenira sve što radimo i upozorava nas ako pronađe neki od malware-a. On ujedno skenira datoteke na računalu i web stranice na Internetu. U trenutku kada kliknemo na link koji bi potencijalno mogao sadržavat neki oblik zlonamjernog programa, antivirusni program nas upozori. Danas ima mnogo proizvođača antivirusnih programa i skoro svaki od njih nudi besplatnu verziju za preuzet. Ako bih smo željeli biti dodatno zaštićeni postoje i verzije koje se plačaju te nude neke dodatne mogućnosti i oblike zaštite.

4. Instalirajte anti-spyware softver

Što je spayware opisano je u prethodnim poglavljima. Kako bih smo njih spriječili postoji dostupno mnogo programa. Slično je kao sa antivirusnim programima. Ima besplatnih programa, te ima programa koji nude bolji zaštitu ali se mora kupit licenca.

[22] TechTerms: Antivirus [Internet]; raspoloživo na https://techterms.com/definition/antivirus

5. Koristite složene i sigurne lozinke

U održavanju sigurnosti sustava vrlo je bitno imati snažne i složene zaporke. Upotrijebite lozinku duljine od najmanje 8 znakova i uključite kombinaciju brojeva, slova (kombinacija velikih i malih slova) te neki poseban znak (točka, zarez, dvotočka, upitnik itd.). Hakeri koriste određene alate sa kojima mogu razbiti jednostavne lozinke za par minuta. Ako koristite neke od najjednostavnijih lozinki poput "123456" ili "123456789" hakeru je potrebno 0.23 sekunde da je razbije. Postoji stranica[23] na Internetu gdje možete provjeriti jačine Vaše lozinke te vrijeme potrebno da se ona razbije.

6. Provjerite sigurnosne postavke Vašeg Internet preglednika (eng. browser)

Preglednici imaju različite postavke sigurnosti i privatnosti koje biste trebali pregledati i postaviti na željenu razinu. Novije verzije preglednika omogućuju Vam da kažete web stranicama da ne prate vaše pokrete, povećavajući vašu privatnost i sigurnost.

[23] BetterBuys: Estimating Password-Cracking Times [Internet], raspoloživo na https://www.betterbuys.com/estimating-password-cracking-times/

3.2.4. Zaštita pri e-trgovini

Kako je vrlo bitno zaštitit svoje računalo prije nego se spojimo na Internet tako je i vrlo bitno da znamo kako se ponašat tj. dodatno zaštitit prilikom e-kupnje. Kada želimo obavit neku vrstu e-kupnje tada se od nas traže naši osobni podaci uključujući i broj naše kartice kako bih se usluga ili proizvod mogli naplatit te je zato vrlo bitno da znamo kako se ponašat u tim situacijama i kako zaštiti naše podatke. U nastavku ćemo donijeti savjete, koje preporuča Europol[24], kako se pravilno ponašat pri online kupovini:

1. Kupujte od provjerenih izvora

Kao što smo rekli Internet je veliko virtualno mijesto koje broji mnogo korisnika. U današnje vrijeme nije veliki problem napravit neki prividan oblik web stranicie koji ima web shop te Vas namamit da kupite nešto što niti ne postoji. Zato je uvjek bitno da kupujete na stranicama koje su provjerene kao na primjer eBay, Amazon, AliExpres, web stranice poznatih proizvođača (zara, Nike, Adidas itd.)

Stranice poput eBay.com ili Amazon.com gdje ima mnogo ponuđača daju mogućnost svakom kupcu da ocjeni uslugu, proizvod i samog ponuđača. Možete provjeriti reputaciju ponuđača, zadovoljstvo drugih kupaca tj. jesu li dobili sve na vrijeme, jesu li dobili točno ono što su tražili i možete biti prilično sigurni da nećete biti prevareni. Dakle i to je vrlo bitno da se se pročitaju komentari i ocjene prije nego se upustimo u kupovinu. Ako ipak nemamo tu mogućnost da nešto kupimo od provjerenog ponuđača bitno je da ne platimo unaprijed i da ne kupujemo od osoba koje u oglasu nisu ostavile neki oblik kontakta (broj telefona, e-mail).

2. Provjeravajte trajna plaćanja

Ako namjeravate napravit neku trajnu uslugu (trajni nalog), prije nego što pošaljete podatke o svojoj kartici, informirajte se o tome kako možete prekinuti tu uslugu. Obavezno se informirajte na stranici preko koje želite aktivirat taku uslugu ali informirajte se i kod svoje banke.

[24] Europol: E-commerce: tips and advice to avoid becoming a fraud victim [Internet]; raspoloživo na https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim

3. Koristite kreditne kartice pri online kupovini

Pri online kupnji imamo mogućnost birati između korištenja kreditnih ili debitnih kartica

Kreditna kartica korisniku omogućuje plaćanje roba i usluga, isplatu gotovine te podmirivanje troškova sa ili bez odgode.

Debitna kartica[25] je platna kartica transakcijskih računa (tekući, devizni, žiroračun) kuje izdaje banka. Upotrebu kartice uvjetuje osigurano pokriće (novac na računu) za izvršenje transakcije u trenutku njezina njezina zadavanja.

Kada kupujete na online, plaćanje kreditnom karticom je bolji izbor. Korištenje kreditne kartice pruža dodatni sloj zaštite od prijevare i olakšava povrat novca. Kada plaćate kreditnom karticom, imate mogućnost odbiti plaćanje ili osporiti naplatu ako postoji problem s vašom kupnjom. Sa druge strane ako plaćate debitnom karticom, sredstva se odmah povlače s vašeg računa. Puno teža je mogućnost da ćete dobiti povrat novaca na debitnu karticu. Tek možda nakon sudskog spora kojeg ste podnijeli protiv trgovca koji Vas je oštetio.

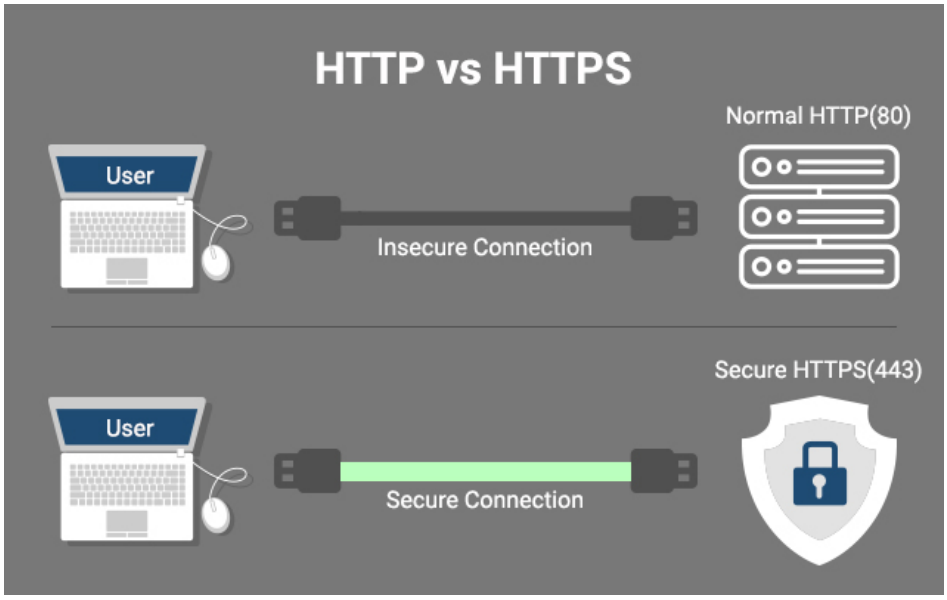
4. Provjerite da li je prijenos podataka prikladno zaštićen

Jedna od oznaka da je stranica zaštićena je ikona zaključanog lokota na URL traci. On predstavlja da je sav promet na i sa web stranice šifriran. Šifriran znači da nitko drugi osim tog web mjesta ne može pročitati detalje o kreditnoj kartici i lozinke koje unesete.

Druga stvar na koju se treba pripazit je da adresa web mjesta započinje sa https:// umjesto http://. HTTP (eng. Hyper Text Transfer Protocol) je protokl koji se koristi za prijenos web stranica između dva računala. Opisat ćemo rad HTTP protokola riječima Optima Hostinga:[26] „HTTP se zasniva na arhitekturi klijenta i poslužitelja - radi tako da računalo 'A' (klijent) uspostavlja vezu s računalom 'B' (poslužitelj) i šalje zahtjev za nekim sadržajem. Poslužitelj prima zahtjev, te traženi sadržaj šalje klijentu. Najčešće traženi sadržaji su HTML dokumenti, odnosno web stranice.“ Danas je dostupan HTTPS (Hyper Text Transfer Protocol Secure) i treba pazit da kupujemo sa

[25] Progreso Grupa: Kreditne kartice:sve što trebate zanti [Internet]; raspoloživo na https://www.progreso.hr/blog/kreditne-kartice/
[26] OptimaHosting: Što je HTTP [Internet]; raspoloživo na https://korisnik.optimahosting.hr/knowledgebase/104/Sto-je-HTTP.html

stranica koje koriste tu vrstu protokola. “S“ u HTTPS označava “Secure“ što znači da je sva komunikacija između našeg računala (web preglednika) i web stranice šifrirana.



Slika 4 Razlika između HTTP i HTTPS protokola
Izvor: https://comodosslstore.com/blog/what-is-the-difference-between-http-and-https-protocols.html

5. Uvijek spremite sve dokumente vezane uz Vaše online kupnje

Te dokumente biste mogli trebati da utvrdite uvjete prodaje ili da dokažete da ste platili robu. Što se tiče uvjeta prodaje njih je isto vrlo važno pročitat prije same kupnje kako bih smo znali koja prava kao kupac imamo vezano uz taj proizvod ili uslugu.

6. Kad god je to moguće kupujte na stranicama koje omogućuju potpunu autentifikaciju

Na takvim stranicama uvijek negdje stoji oznaka Verified by Visa/Mastercard Secure Code. To znači da je stranica odobrena od strane Vise i Mastercarda.

Slika 5 Visa/Mastercard sigurnosni znak
Izvor: https://www.polymax.in/media/wysiwyg/cc.jpg

7. Kada kupujete on-line od druge osobe, nemojte slati novac unaprijed

Ovo se odnosi na kupovinu koja nije ostvarena preko neke provjerene stranice te ako nije zaštićena nekom vrstom certifikata (Visa/Mastercard sigurnosni znak). Primjer bi bio kupovina preko naše najpoznatije stranice za oglašavanje njuškalo.hr. Tamo postoji mogućnost da vam ponuđač da njegove podatke za uplatu koju vi možete izvršit preko banke ali to nije preporučljivo. Postoji mogućnost da platite prilikom dostave kada se uvjerite u ispravnost robe koju ste kupili.

8. Nemojte slati novac nikome koga ne poznajete

Uvjek će postojat netko tko Vam se može obratit putem Interneta (e-mail, chat, društvene mreže) i tražit od Vas da mu uplatite novac. Razlozi koji će ti ljudi navest mogu biti razni kao npr. donacija, pomoć, Vaš dug koji nije podmiren itd. Nemojte takvim osobama ništa slati prije nego se uvjerite tko su i što su te da li su prevaranti ili nisu.

9. Nikad nikome nemojte slati broj kartice, PIN ili druge podatke o kartici putem e-pošte
10. Mnogi Internet trgovci će Vas tražiti da čuvaju Vaše podatke o plaćanju

Ovdje se radi o Vašim podatcima kreditne ili debitne kartice kao i o Vašim privatnim podacima (ime, prezime, adresa) te stoga pazite i dobro razmislite kojim web stranicama ćete to dopustit i zašto.

11. Ukoliko ne kupujete određeni proizvod ili uslugu, nemojte davati podatke o svojoj kreditnoj kartici

Dosta stranica će tražiti od Vas da im priložite podatke o kartici i prije same kupnje određenog proizvoda ili usluge. Za takvim postupkom nema potrebe jer stranicama ti podaci ne bi trebali biti potrebni ako vi nećete ništa kupovat s toga niti nemojte davat te podatke.

Uz prethodno navedena pravila Europola postoji još nekoliko korisnih savjeta kako se zaštitit prilikom online kupnje.

1. Prilikom online kupnje je dobro koristit token za dodatnu autentifikaciju Vas kao kupca tj. on daje dodatnu sigurnost da ste to vi te da je kartica koju koristite vaša. Token koristi

provjeru autentičnosti putem dva faktora. Prema TechTargetu[27] dvofaktorska autentifikacija pruža dodatni sloj sigurnosti i otežava napadačima pristup uređajima i online računima, jer samo poznavanje zaporke žrtve više nije dovoljno za prolaz provjere autentičnosti. Dva faktora za provjeru autentičnosti već se dugo upotrebljavaju za kontrolu pristupa osjetljivim sustavima i podacima, a mrežne usluge sve više koriste taj način autentifikacije kako bi spriječile hakerima koji su ukrali Vašu lozinku da uđu u Vaš račun.

2. Koristite složene i sigurne lozinke. Njihove benefite smo već naveli u potpoglavlju 3.2.3. Što Vam je zaporka složenija to ste sigurniji tj. manja je vjerojatnost da će je netko dešifrirat.
3. Koristite PayPal za online kupovinu.
    - The Balance nam donosi definiciju što je PayPal:[28] "PayPal je usluga koja vam omogućuje plaćanje, slanje novca i prihvaćanje uplata. Registrirajte svoju kreditnu ili debitnu karticu putem PayPal računa. Možete platiti jednostavnim odabirom PayPala prilikom plaćanja, prijavom na PayPal račun i potvrdom plaćanja. Jednostavno odaberite PayPal kad odaberete opciju plaćanja na web stranici. Sa PayPal računom možete kupovati sa milijunima trgovaca i prodavača širom svijeta gdje god vidite logotip PayPal-a. "
    - kada koristite PayPal onda ste podatke kartice dali samo njima. Nigdje više vas neće tražiti da unosite ponovo te podatke pa je samim time smanjena mogućnost da Vam netko ukrade informacije o Vama i vašoj kreditnoj kartici.

[27] TechTarget: Two-factor authentication [Internet]; raspoloživo na http://searchsecurity.techtarget.com/definition/two-factor-authentication
[28] The Balance: What is paypal and how dose it wor with eBay [Internet]; raspoloživo na https://www.thebalance.com/paypal-working-on-ebay-1140193

4. EMPIRIJSKO ISTRAŽIVANJE: KOLIKO KRAJNJI KORISNICI ZNAJU O ZAŠTITI PRI E-TRGOVINI?

U empirijskom dijelu rada korišteno je anketno istraživanje. Cilj ankete bio je dobiti sliku o tome koliko današnje društvo zna o Internet sigurnosti te sigurnosti pri e-kupovini. Anketa je provedena online putem google obrazaca te je obuhvatila uzorak od 125 ispitanika. U nastavku ćemo analizirati rezultate dobivene putem ankete.

U prvom dijelu ankete ispitanici su imali mogućnost višestrukog odabira:

Od sveukupnog broja ispitanika njih 66,4% je ženskog spola, dok je preostalih 33,6% muškog spola. Prema dobi ispitanika najviše je onih u dobi od 21-25 godina (njih 55,2%) dok najmanje ima osoba koje su ispod 18 godina starosti, a onih iznad 35 godina starosti nema. Ispitanici su se izjasnili o njihovom zanimanju. Među ispitanicama je najveći broj studenata (63,2%), zatim ima 24,8% zaposlenih, 10,4% je učenika a najmanje ima nezaposlenih (1,6%).

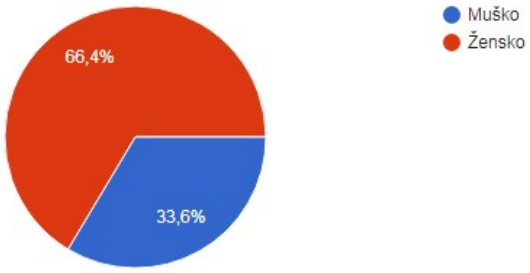
Gledajuću kupovnu naviku naših ispitanika, najviše njih kupuje on-line jednom mjesečno (36%), njh 21,6% to radi dva do tri puta mjesečno, dok njih 20,8% nema naviku on-line kupnje. Promatramo li skupinu u dobi od 21 do 25 godina (najveću skupinu u ovom istraživanju) njih 39% obavlja kupnju jednom mjesečno, 23% to radi dva di tri puta mjesečno do njih 14,5% ne kupuje on-line. Ovi rezultati nam pokazuju da ljudi još nemaju naviku kupovati preko Interneta. U prošlom poglavlju smo se upoznali sa PayPal-om i njegovim beneficijama pri e-kupnji. Autorizaciju preko PayPal-a izvršava 43,5% ispitanika.

U današnje vrijeme je vrlo popularno Internet bankarstvo te svaka banka uz intert bankarstvo nudi i dodatnu autorizaciju preko tokena. Na temelju odgovora naših ispitanika vidimo da kod nas još uvijek većina ljudi nema token. Njih 59,7% ne koristi ovu vrstu dodatne zaštite.

Rezultati prvog dijela ankete:

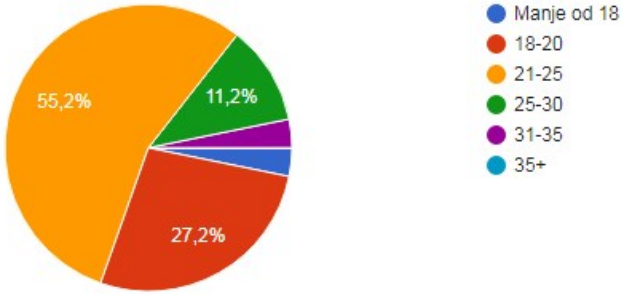
Spol:

125 odgovora



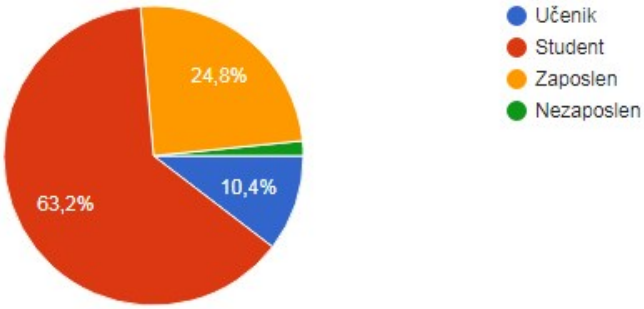
Dob:

125 odgovora



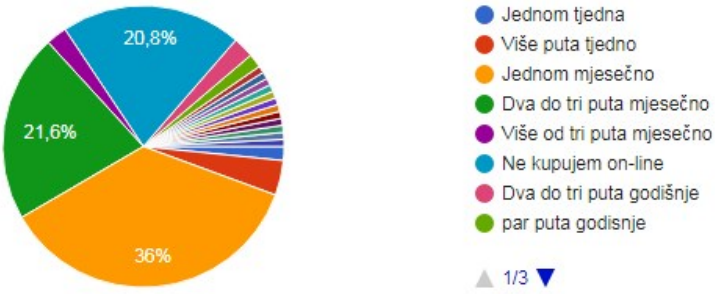
Zanimanje:

125 odgovora



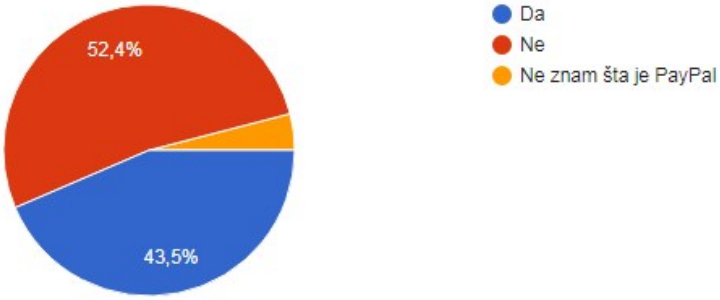
Koliko često kupujete online?

125 odgovora



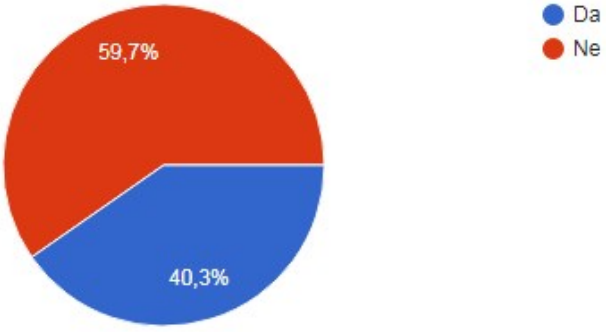
Imam PayPal račun

124 odgovora



Koristim autorizaciju kartice preko tokena.

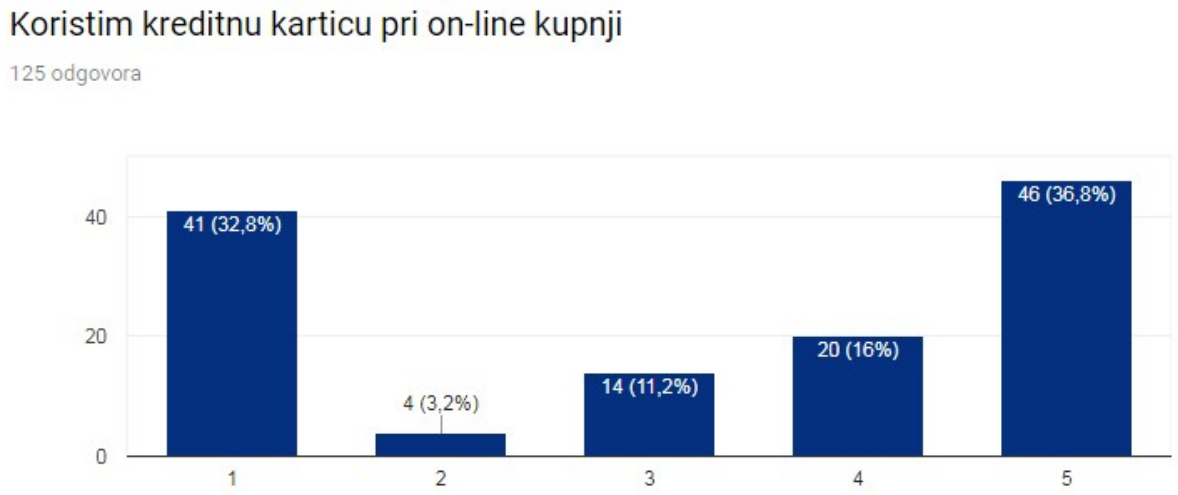
124 odgovora



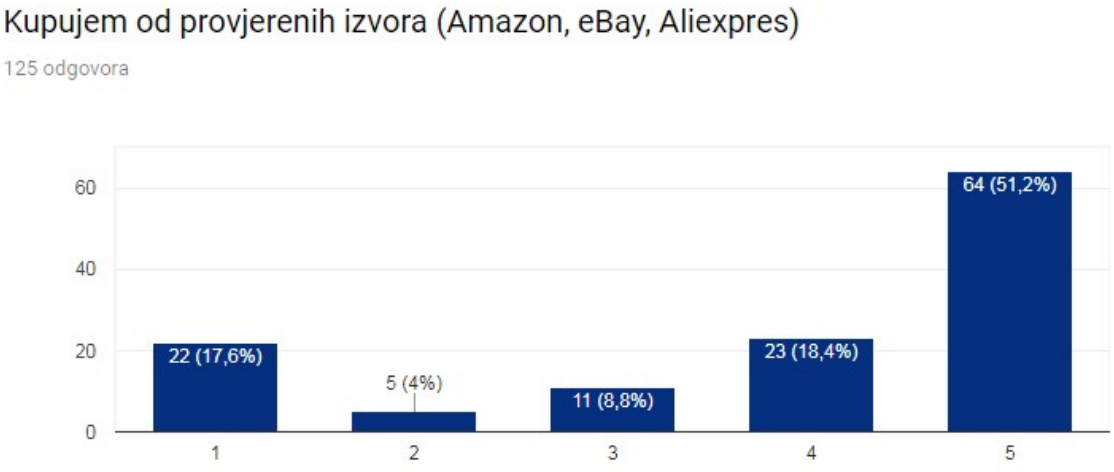
U drugom dijelu ankete ispitanici su morali ocijenit od 1 do 5 njihov stupanj slaganja sa navedenim tvrdnjama. Ocjene su označavale:

- 1 – uopće se ne slažem
- 2 – uglavnom se ne slažem
- 3 – niti se slažem, niti se ne slažem
- 4 – uglavnom se ne slažem
- 5 - potpuno se slažem

Tvrdnje te rezultati drugog djela ankete slijede u nastavku:

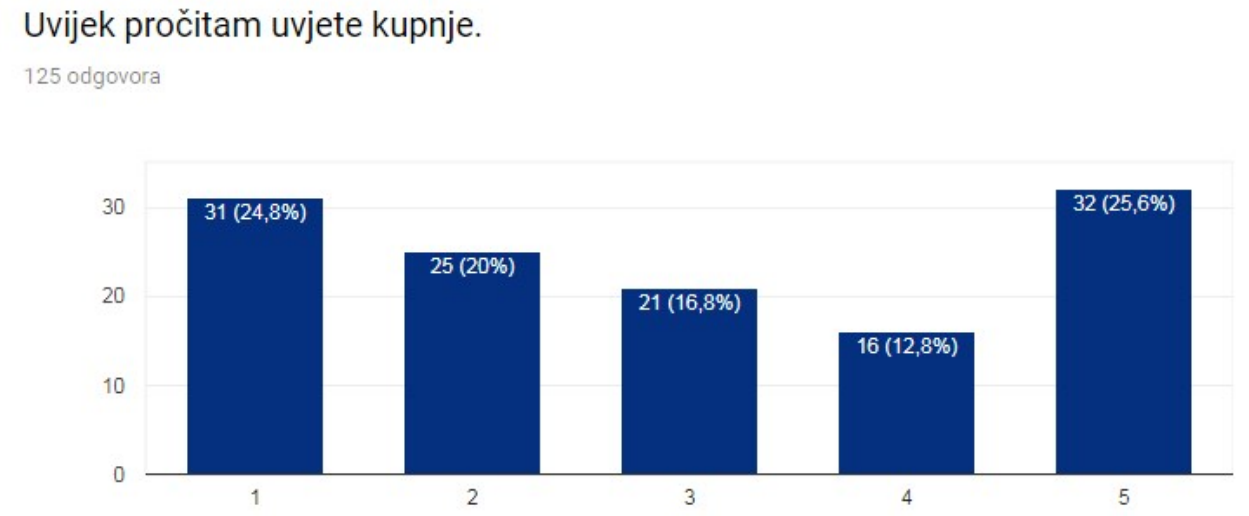


Ovdje vidimo da je podjednak broj onih koji koriste kreditnu karticu prilikom kupnje i onih koji je ne koriste dok njih 30,4 posto koristi kreditnu karticu samo povremeno.

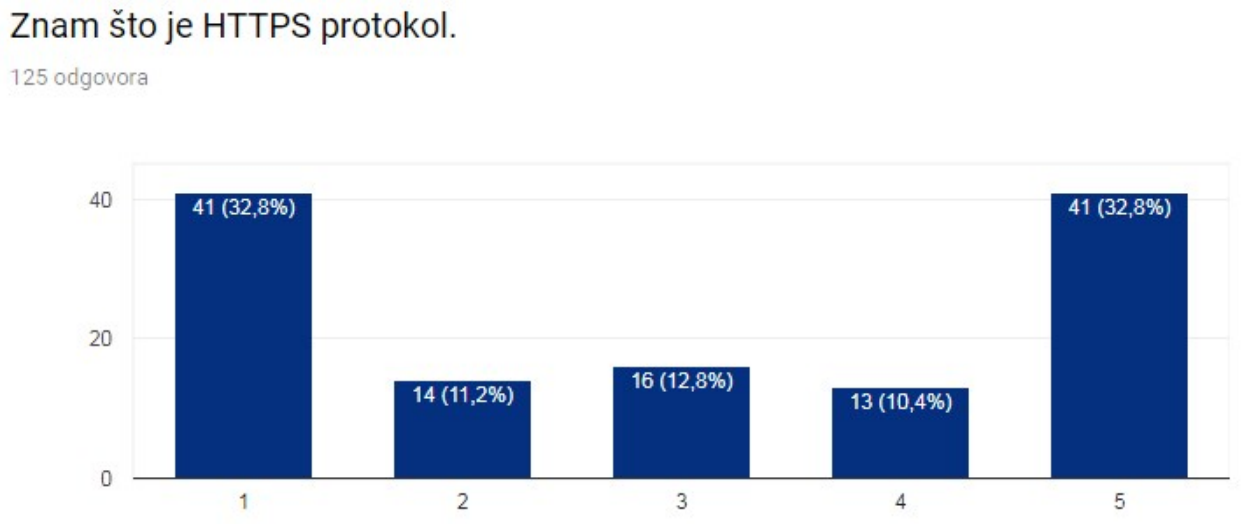


U prethodnim poglavljima vidjeli smo koliko je bitno kupovati sa provjerenih izvora. Naši ispitanici u većini slučajeva kupuju na stranicama koje se već od prije provjerene od drugih kupaca.

Vrlo je bitno da web adresu prodajnog mjesta upisujete sami. Ako pratite linkove iz poruka, e-maila, chatova, društvenih mreža, moguće je da će Vas odvesti na neke phishing stranice koje će Vam htjeti ukrasti lozinku. Ovdje su rezultati skoro podjednako podijeljeni, no ipak samo 36,3% ispitanika web adresu upisuje samostalno dok njih 13.7% povremeno ulazi na stranice preko linka.



Prije same kupovine mali broj kupaca pročita sve uvjete. Većina nas ih samo preskoči tj. ako treba označi ih kao pročitane bez da ih pogledamo. Vrlo je bitno da znamo po kojim uvjetima kupujemo i čemu to dajemo našu suglasnost. Prema ovoj anketi samo 25% ljudi pročita uvjete kupnje, dok isti taj postotak ljudi nikada ne čita uvjete.

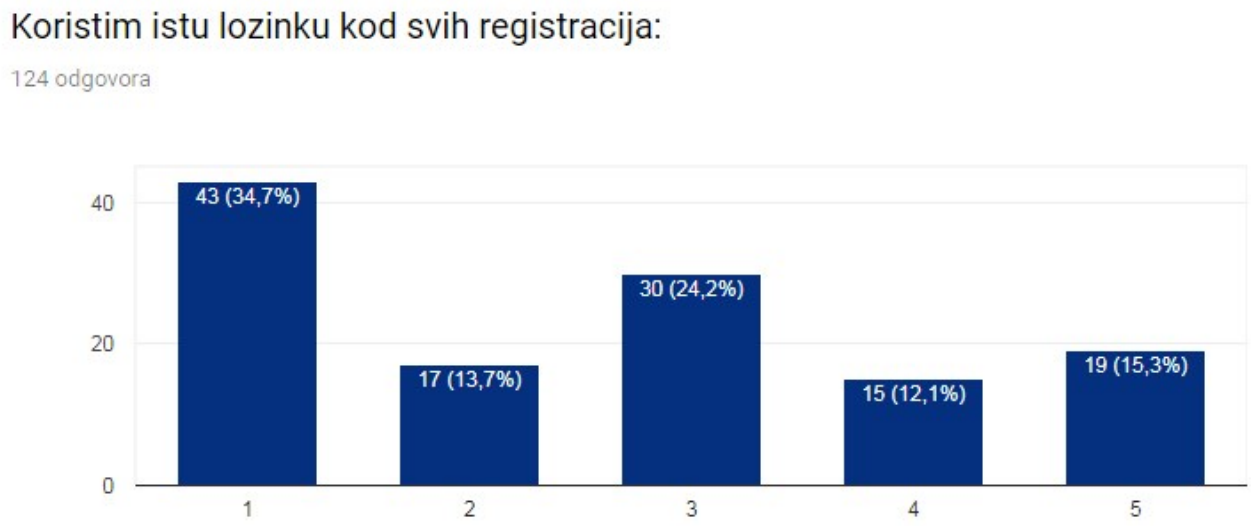


Za sigurnost protokola na web stranicama zna 32,8% ispitanika, a isti taj postotak nije nikad čulo za to. Ostali ispitanici su podijeljeni tj. samo su čuli za HTTPS protokol.

Većina ispitanika obavlja kupnju sa svog računala. Svakako kupnja se može obaviti i sa drugih računala ali je vrlo važno paziti da ne ostavimo naše podatke tj. da ne označimo “zapamti me“. Osim toga, ako je računalo na javnom mjestu, ne možemo nikad biti sigurni da neka treća osoba

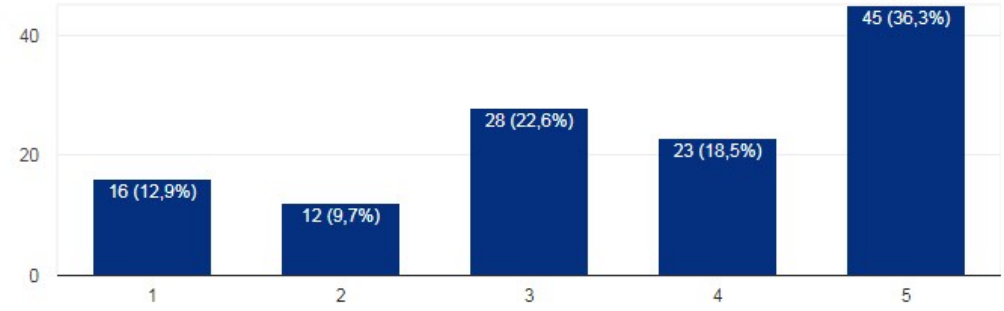
nije ostavila program koji prikuplja sve unesene zaporke na tom računalu. Zato je svakako najsigurnije kupnju obavit sa vlastitog računala.

Još uvijek samo manji broj ljudi, 36,3%, redovno ažurira svoj operativni sustav, a njih 11,3% to radi povremeno.



Moja lozinka je snažna (sadrži slova, brojeve i znakove poput točke, zareza, uskličnika...)

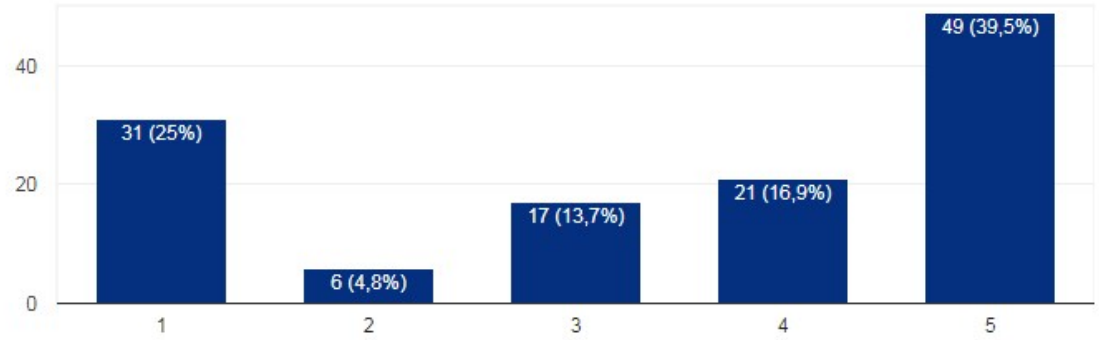
124 odgovora



Korištenje iste lozinke kod svih registracije nije dobro iz razloga ako nam netko ukrade lozinku imat će pristup svim vašim računima i stranicama gdje ste koristili tu lozinku. Većina ispitanika je svjestan koliku važnost pridonosi ispravan odabir lozinke (korištenje snažne lozinke).

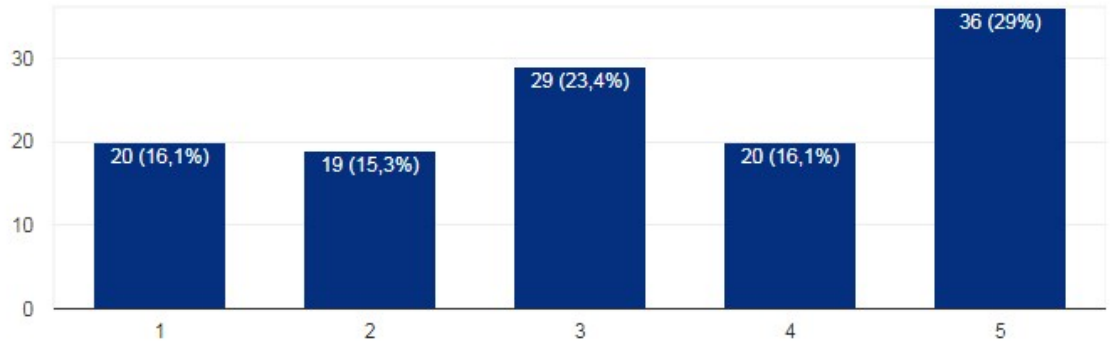
Koristim besplatnu verziju antivirusnog programa

124 odgovora



Uvijek pazim da je antivirusni program ažuriran

124 odgovora



I dalje većina ljudi koristi besplatne verzije antivirusnih programa. One nam pružaju samo osnovnu zaštitu i vrlo je bitno da su uvijek ažurirane. Zloćudni programi su svaki dan sve napredniji i svaki dan ih je sve više pa ako ne ažuriramo antivirusni program on se ne može borit protiv novih verzija zloćudnih programa što nam je jednako kao i da ga nemamo.

Promotrimo i Spearmanovu korelacijsku analizu između odabranih varijabli:

- Ako su jedna ili dvije varijable dane u rangu, tj. rezultati nisu mjerne vrijednosti već su dani samo u redoslijedu, koristimo Spearmanov koeficijent korelacije
- Prema intenzitetu korelacija može biti:
  - $|r_s| \geq 0{,}8$ tj. jaka korelacija
  - $0{,}5 < |r_s| < 0{,}8$ tj. polujaka korelacija
  - $|r_s| \leq 0{,}5$ tj. slaba korelacija

Tablica 2 Korelacija podataka unos web adrese i kupovina od provjerenih izvora

			Kupujem od provjerenih izvora (Amazon, eBay, Aliexpres)	Web adresu prodajnog mjesta upisujem sam/a (ne slijedim linkove iz poruka, društvenih mreža...)
Spearman's rho	Kupujem od provjerenih izvora (Amazon, eBay, Aliexpres)	Correlation Coefficient	1.000	.440**
		Sig. (2-tailed)	.	.000
		N	124	124
	Web adresu prodajnog mjesta upisujem sam/a (ne slijedim linkove iz poruka, društvenih mreža...)	Correlation Coefficient	.440**	1.000
		Sig. (2-tailed)	.000	.
		N	124	124

Izvor: Izrada autora

U tablici 2 vidimo pozitivnu slabu korelaciju. Rezultat koji je dobiven znači da ljudi koji samostalno upisuju web adresu prodajnog mjesta kupuju od provjerenih izvora.

Tablica 3 Korelacija podataka unos web adrese i kupnja preko kreditne kartice

			Koristim kreditnu karticu pri on-line kupnji	Web adresu prodajnog mjesta upisujem sam/a (ne slijedim linkove iz poruka, društvenih mreža...)
Spearman's rho	Koristim kreditnu karticu pri on-line kupnji	Correlation Coefficient	1.000	.395**
		Sig. (2-tailed)	.	.000
		N	124	124
	Web adresu prodajnog mjesta upisujem sam/a (ne slijedim linkove iz poruka, društvenih mreža...)	Correlation Coefficient	.395**	1.000
		Sig. (2-tailed)	.000	.
		N	124	124

Izvor: Izrada autora

U tablici 3 vidimo slabu pozitivnu korelaciju koja nam govori da ljudi koji sami upisuju web adersu e-trgovine preko koje kupuju tu kupnju plaćaju sa kreditnom karticom.

Tablica 4 Korelacija podataka o ažuriranju programa i operativnog sustava

			Uvijek pazim da je antivirusni program ažuriran	Redovno radim ažuriranje operativnog sustava
Spearman's rho	Uvijek pazim da je antivirusni program ažuriran	Correlation Coefficient	1.000	.383**
		Sig. (2-tailed)	.	.000
		N	124	124
	Redovno radim ažuriranje operativnog sustava	Correlation Coefficient	.383**	1.000
		Sig. (2-tailed)	.000	.
		N	124	124

Izvor: Izrada autora

Tablica 4 nam pokazuje da ljudi koji redovno rade ažuriranja operativnog sustava isto tako rade i redovno ažuriranje svog antivirusnog programa

5. ZAKLJUČAK

Doba u kojem živimo mogli bih smo nazvati “Internetsko doba“. Poslovanje bez Interneta više nije moguće. Svaka tvrtka koja nudi određenu uslugu ili proizvod mora imati barem web stranicu a poželjno je da ima i e-trgovinu kako bi uspjela na današnjem tržištu prepunom konkurencije. Internet je virtualan prostor koji nam nudi bezbroj mogućnosti.

Ovim radom upoznali smo se sa e-trgovinom koja je sve naprednija i popularnija. U današnje moderno doba tvrtke bi trebale više svojih sredstva ulagati u informatizaciju i dostupnost njihovih proizvoda i usluga putem Interneta, a krajnji korisnici bi trebali više razmišljat o online kupovini jer nudi više mogućnosti nego standardne trgovine (više proizvoda i usluga, niže cijene, javna mišljenja drugih kupaca itd.).

Uz mnoge mogućnosti koje pruža Internet na njemu ima i mnogo prijetnji na koje možete naići. Postoje načini kako se od njih obraniti. Načine obrane možemo svrstat u dvije skupine. Jedna bi bila poduzimanje određenih sigurnosnih mjera prije spajanja na Internet, a druga bi bila određene mjere koje moramo poduzeti kada obavljamo e-kupovinu.

U anketi koja je provedena na uzorku od 125 ispitanika dobili smo okviran dojam koliko krajnji korisnici znaju o mjerama zaštite na Internetu i pri e-kupovini. Samo manji broj je potpuno svjestan svih prijetnji koje se nalaze na Internetu dok je većina korisnika potpuno neinformirana ili su čuli za određene mjere zaštite na Internetu ali nisu adekvatno upoznati sa njima te ih ne znaju pravilo koristiti.

Sve metode sigurnosti koje postoje da nas štite ne znače mnogo ako korisnici nisu educirani o tome kako ih koristit. Zaštita na Internetu je bitna kako za tvrtke , tako i za same krajnje korisnike. Ako zaposlenici u tvrtci nisu pravilno educirani o zaštita i ponašanju na Internetu može doći da raznih vanjskih napada, a ako krajnji korisnik nije upoznat sa mjerama sigurnosti može se dogodit da mu osobni podaci budu ukradeni i zloupotrebljeni. Pošto je Internet naša sadašnjost ali i budućnost treba ljude više educirati kako bi se znali samostalno zaštiti kada su online.

SAŽETAK

Internet je platforma koja bilježi konstantan rast broja korisnika od kako je nastala. U današnje vrijeme Internet je toliko važan da se poslovanje bez njega više ne bi moglo zamislit. Sve više tvrtki svoje poslovanje okreće prema Internet trgovini, a te iste Internet trgovine bilježe rast prodaje što znači da ima sve više korisnika koji kupuju putem e-trgovine. Kako svugdje postoje određene opasnosti tako je i na Internetu. Društvo te poslovno okruženje nije dovoljno upoznato sa svim rizicima takvog načina poslovanja. E-trgovina raste velikom brzinom ali nitko ne upozorava na prijetnje koje se mogu dogoditi. Cilj autora rada je upoznati tvrtke i krajnje korisnike sa značajem e-trgovine te mogućim rizicima tj. najčešćim opasnostima i prijetnjama koje postoje na Internetu sa posebnim naglaskom na sigurnost i mogućnostima kako ih spriječit prije nego nastanu.

KLJUČNE RIJEČI: E-TRGOVINA, INTERNET, SIGURNOST

SUMMARY

The Internet is a platform that is experiencing steady growth since it was created. Nowadays, it is so important that business operations without it could no longer be imagined. More and more companies are turning their business operations toward web shops, and the web shops are experiencing growth in sales, meaning that there are more and more customers who buy through e-commerce. Since there are everywhere certain dangers, there is no difference on the Internet. The society and business company’s are not sufficiently familiar with all the risks of such business operations. E-commerce is growing fast but nobody is warning you about the threats that may occur. The author's goal is to familiarize both business and end-users with the importance of e-commerce and the potential risks, ie the most common dangers and threats that exist on the Internet, with particular emphasis on security and the ability to prevent the risks before they occur.

KEY WORDS: E-COMMERCE, INTERNET, SECURITY

LITERATURA

Knjige:

1. Bott, E., Siechert, C. (2003): Microsoft Windows Security Inside Out for Windows XP and Windows 2000, Microsoft Press, Washington
2. Chaffey, D (2007): E-business and E-commerce management: Strategy, Implementation and Pratice, Prentice Hall
3. Conry-Murray, A., Weafer, V. (2005): Sigurni na Internetu, MIŠ d.o.o., Zagreb
4. Garača, Ž. (2007): Informatičke tehnologije, Sveučilište u Splitu, Split
5. Garača, Ž. (2008): Poslovni informacijski sustavi, Sveučilište u Splitu, Split
6. Greenstein, M., Feinman M T. (2000): Electronic commerce: Security, risk management and control, The McGrawe-Hill Companies, USA
7. Panian, Ž (2013): Elektroničko poslovanje druge generacije, Sveučilište u Zagrebu, Zagreb
8. Panian, Ž. (2000): Elektroničko trgovanje, Sinergija, Zagreb
9. Petric, D.(2002): Internet uzduž i poprijeko, Bug d.o.o., Zagreb
10. Ružić, D., Biloš, A., Turkalj, D. (2009): e- Marketing, Ekonomski fakultet u Osijeku, Osijek
11. Smith, B., Komar, B. (2005): Microsoft Windows Security, Microsoft Press, Washington
12. Strauss, J., El-Ansary, A., Frost, R. (2006): E-Marketing – fourth edition, Pearson Education Inc., New Jersey
13. Strauss, J., Frost, R. (2001): E-marketing, drugo izdanje, Prentice Hall, New Jersey

Članci:

1. CARNet, CERT, LS&S: „Spyware programi “, CCERT-PUBDOC-2009-10-280
2. Internet Society: Global internet report 2016

Internet izvori:

1. BetterBuys: Estimating Password-Cracking Times [Internet], raspoloživo na https://www.betterbuys.com/estimating-password-cracking-times/

2. ECeurope [Internet],raspoloživo na http://www.eceurope.com/
3. Europol: E-commerce: tips and advice to avoid becoming a fraud victim [Internet]; raspoloživo na https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim
4. Eurostat: E-commerce statistics for individuals [Internet], raspoloživo http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals
5. Eurostat: National and cross-border purchases by e-shoppers [Internet], , raspoloživo na https://goo.gl/2uWxXs
6. Eurostat:Internet purchases by individuals [Internet], raspoloživo na http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_ibuy&lang=en
7. Gemalto [Internet], raspoloživo na http://www.gemalto.com/review/Pages/infographic-the-number-of-internet-users-by-2020.aspx
8. Gemalto [Internet]; raspoloživo na http://www.gemalto.com/
9. Internet [Internet], raspoloživo na https://hr.wikipedia.org/wiki/Internet
10. Internet world stats [Internet], raspoloživo na na http://www.internetworldstats.com/stats.htm
11. Microsoft: 10 immutable laws of security [Internet]; raspoloživo na https://technet.microsoft.com/en-us/library/hh278941.aspx
12. O phisingu [Internet], raspoloživo na http://www.cert.hr/phishing
13. OptimaHosting: Što je HTTP [Internet]; raspoloživo na https://korisnik.optimahosting.hr/knowledgebase/104/Sto-je-HTTP.html
14. OptimID (2012): EDI – što je to? [Internet], raspoloživo na http://www.optimit.hr/hr/edi/-/asset_publisher/6a93Ij7DSOHe/content/edi-sto-je-to-

15. Progreso Grupa: Kreditne kartice:sve što trebate zanti [Internet]; raspoloživo na https://www.progreso.hr/blog/kreditne-kartice/
16. Što su virusi i ostali zlonamjerni programi [Internet]; raspoloživo na https://sites.google.com/site/zlonamjerniprograminainternetu/
17. TechTarget: Two-factor authentication [Internet]; raspoloživo na http://searchsecurity.techtarget.com/definition/two-factor-authentication
18. TechTerms: Antivirus [Internet]; raspoloživo na https://techterms.com/definition/antivirus
19. The Balance: What is paypal and how dose it wor with eBay [Internet]; raspoloživo na https://www.thebalance.com/paypal-working-on-ebay-1140193
20. The history of the Internet [Internet], raspoloživo na https://www.infoplease.com/history-internet-0

POPIS SLIKA

POPIS GRAFIKONA

POPIS TABLICA

PRILOZI RADU

Prilog 1: Provedena anketa na temu E-trgovina

E-trgovina

Ova anketa se provodi za potrebe pisanja završnog rada na temu "Internet sigurnost i e-trgovina". Anketa je u potpunosti anonimna i dobrovoljna te će rezultati dobiveni anketnim istraživanjem biti korišteni isključivo u svrhu izrade završnog rada.

Spol: *

- Muško
- Žensko

Dob: *

- Manje od 18
- 18-20
- 21-25
- 25-30
- 31-35
- 35+

Zanimanje: *

- Učenik
- Student
- Zaposlen
- Nezaposlen

Koliko često kupujete online? *

U koliko nema opcije koja odgovara Vašim možete upisat pod ostalo.

- ○ Jednom tjedna
- ○ Više puta tjedno
- ○ Jednom mjesečno
- ○ Dva do tri puta mjesečno
- ○ Više od tri puta mjesečno
- ○ Ne kupujem on-line
- ○ Ostalo...

Imam PayPal račun *

- ○ Da
- ○ Ne
- ○ Ne znam šta je PayPal

Koristim autorizaciju kartice preko tokena. *

- ○ Da
- ○ Ne

Ocijenite ocjenom od 1- 5 vaš stupanj slaganja s niže navedenim izjavama (zaokružite ocjenu) .

Tumačenje brojeva u odgovorima:
1 - uopće se ne slažem 2 - uglavnom se ne slažem 3 - niti se slažem niti se ne slažem 4 - uglavnom se slažem 5 – potpuno se slažem

Koristim kreditnu karticu pri on-line kupnji *

1	2	3	4	5
○	○	○	○	○

Kupujem od provjerenih izvora (Amazon, eBay, Aliexpres) *

1	2	3	4	5
○	○	○	○	○

Web adresu prodajnog mjesta upisujem sam/a (ne slijedim linkove iz poruka, društvenih mreža...) *

1	2	3	4	5
○	○	○	○	○

Uvijek pročitam uvjete kupnje. *

1	2	3	4	5
○	○	○	○	○

Znam što je HTTPS protokol. *

1	2	3	4	5
○	○	○	○	○

On-line kupnju obavljam sa vlastitog računala. *

1	2	3	4	5
○	○	○	○	○

Redovno radim ažuriranje operativnog sustava *

1	2	3	4	5
○	○	○	○	○

Koristim istu lozinku kod svih registracija: *

1	2	3	4	5
○	○	○	○	○

Moja lozinka je snažna (sadrži slova, brojeve i znakove poput točke, zareza, uskličnika...) *

1	2	3	4	5
○	○	○	○	○

Koristim besplatnu verziju antivirusnog programa *

1	2	3	4	5
○	○	○	○	○

Uvijek pazim da je antivirusni program ažuriran *

1	2	3	4	5
○	○	○	○	○