

*Prolećni semestar, 2020/21*

*PREDMET: IT370 INTERAKCIJA ČOVEK-RAČUNAR*

Domaći zadatak: **15**

Ime i prezime: **Bogdan Janković**

Broj indeksa: **3920**

Datum izrade: **02.06.2021.**

# Tekst domaćeg zadatka:

**Ispitivanje stava korisnika prema bezbednosti sistema**

Na osnovu prethodnih vežbi sastavite izveštaj o ispitivanju stava o bezbednosti studenata UM ili neke druge kompanije/organizacije.

Izveštaj treba da bude na dve strane sa navedenim referencama ka člancima i blogovima koje ste koristili za istraživanje.

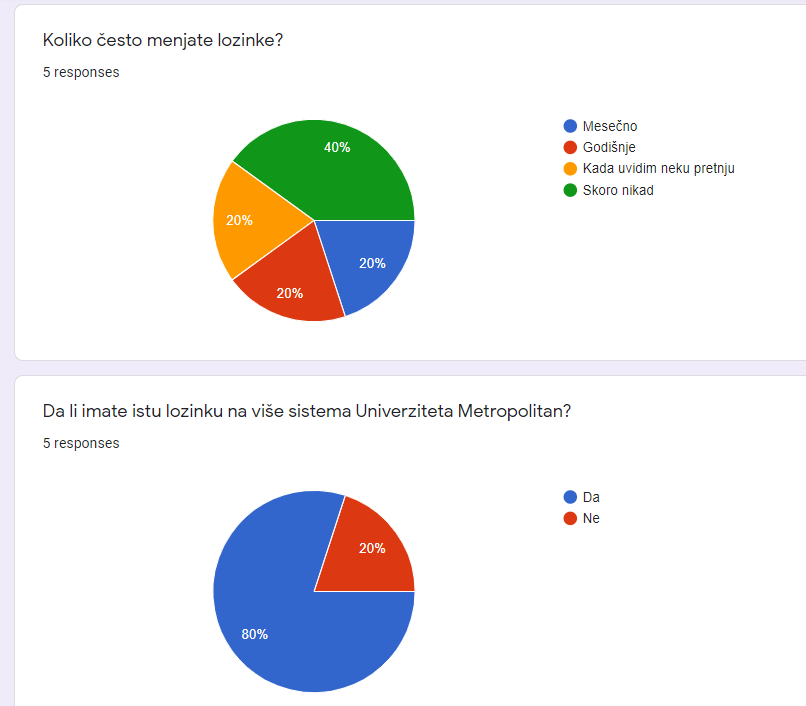
# Rešenje zadatka:

Digitalni svet je opasan svet. Savremeni sajber kriminalci i hakeri koriste sve sofisticiranija sredstva za pristup najosetljivijim podacima i ličnim podacima.

Ovih dana ne treba ni da kliknete na zaraženu vezu da biste završili skrivenim malverom koji može da evidentira pritiske tastera, skenira sistem za lične datoteke ili otme vaše sesije bankarstva na mreži. Lažnjaci često podmeću veb lokacije, adrese e-pošte i profile na društvenim mrežama kako bi manipulisali poverenjem korisnika i stekli pristup ličnim podacima. Popularne usluge poput besplatnog Wi-Fi-ja, bankomata i javnih računara mogu dovesti do kompromisa podataka, finansijskog gubitka i krađe identiteta.

Kako sve više digitalizujemo svoj život, izlažemo se većem riziku. Bez obzira da li ćete upisati prvu ili poslednju godinu fakulteta, nikad nije kasno da se pozabavite internet savetima za bezbednost i povećate svoju svest o sajber bezbednosti.

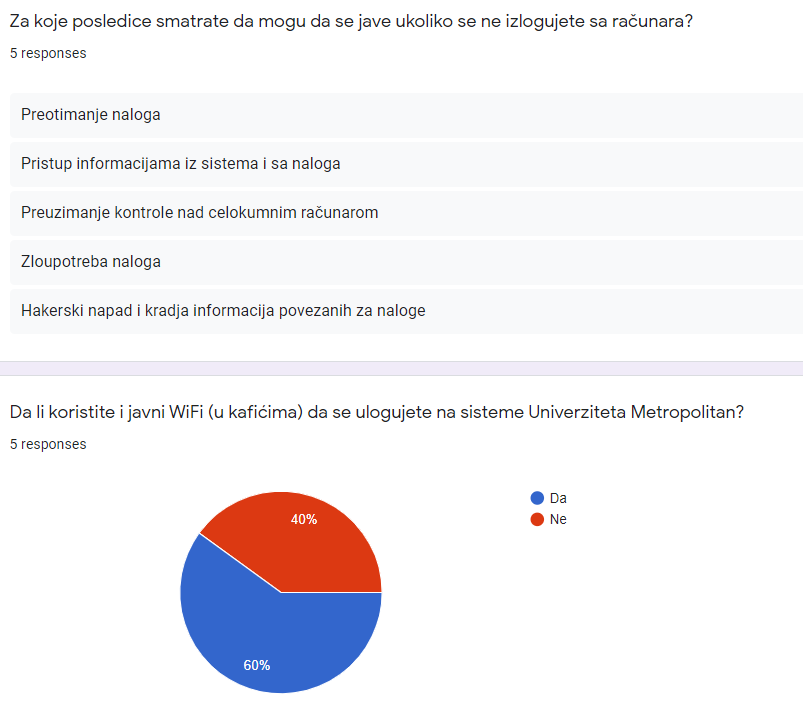
Najbolji način za borbu protiv sajber kriminala je prevencija. Koristite sledeće statistike, priče i savete da biste se spremni i na univerzitetu i van njega.



Istraživanje je pokazalo da procentualno mali broj korisnika menja lozinku kao što se to inače preporučuje a naravno mnogo veći procenat to ne radi skoro nikad ili tek kad uvide neku pretnju, za šta je već gotovo sigurno kasno.

Odgovor na drugo pitanje je takođe veoma zabrinjavajuć gde je samo jedan korisnik naveo da ima različite lozinke na sistemima Univerziteta Metropolitan. Dok naravno puno korisnika i ostavlja svoje generičke lozinke što je bilo izloženo u predavanja, naravno koje su konstruisane od strane administratora sistema ali i generalno poznate ostalim korisnicima istih sistema. Ovo govori da je bitno još jednom se podsetiti osnova oko kreiranja lozinki što predstavlja odličan korak prema sigurnijem digitalnom okruženju:

* Koristite jedinstvene lozinke za svaki nalog: nemojte ih kopirati ili samo malo podesiti.
* Koristite frazu, a ne reč: pristojna lozinka mogu biti tri slučajne reči, poput „močvarno zemljište sa zavesama“.
* Ne koristite lične podatke kao lozinke: ovo uključuje sve, od vašeg mesta rođenja do vaše omiljene destinacije za odmor.
* Izaberite dugačke lozinke: što su duže, teže ih je razbiti.
* Ne dozvolite pregledaču da čuva vaše lozinke: zlonamerni softver se može prikrasti računaru i ukrasti ih.

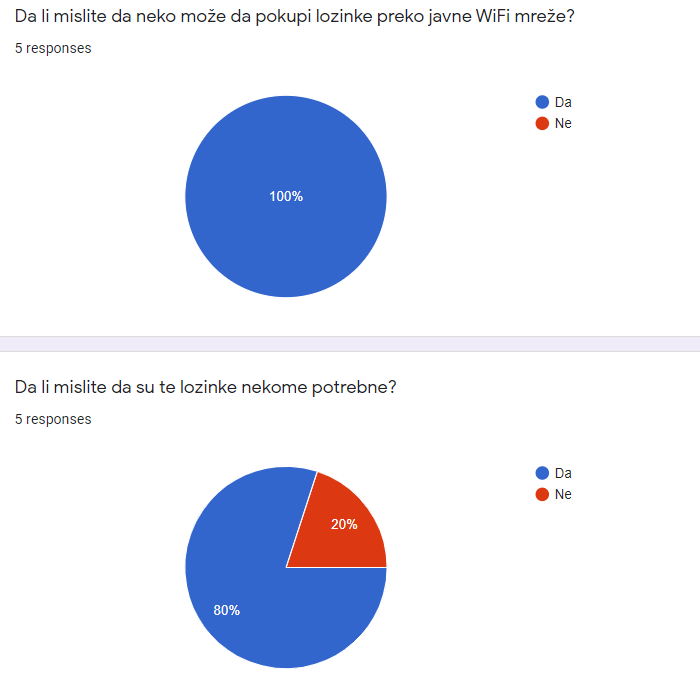


Odgovori navedeni od strane korisnika govore da su upoznati sa svim potencijalnim problemima. Ovo govori da se o bezbednosti itekako priča i razmenjuju iskustva i stavovi korisnika koji su ih iskusili i onih koji su skeptici i naravno onih nemarnih. Svi odgovori su apsolutno tačni i mogu biti realizovani od strane hakera veoma lako, te se na ovakve stvari treba što više obratiti pažnja jer jednostavan potez logout-a od dve sekunde na samom kraju korišćenja sistema i računara može značiti mnogo.

Naravno može se reći da polovina korisnika koristi i javne mreže pored svojih mobilnih podataka da pristupa sistemima univerziteta. Ovo govori da možda korisnici nisu u potpunosti sigurni šta sve javne mreže donose sa sobom te evo kratkog pregleda i dodatnih preporuka:

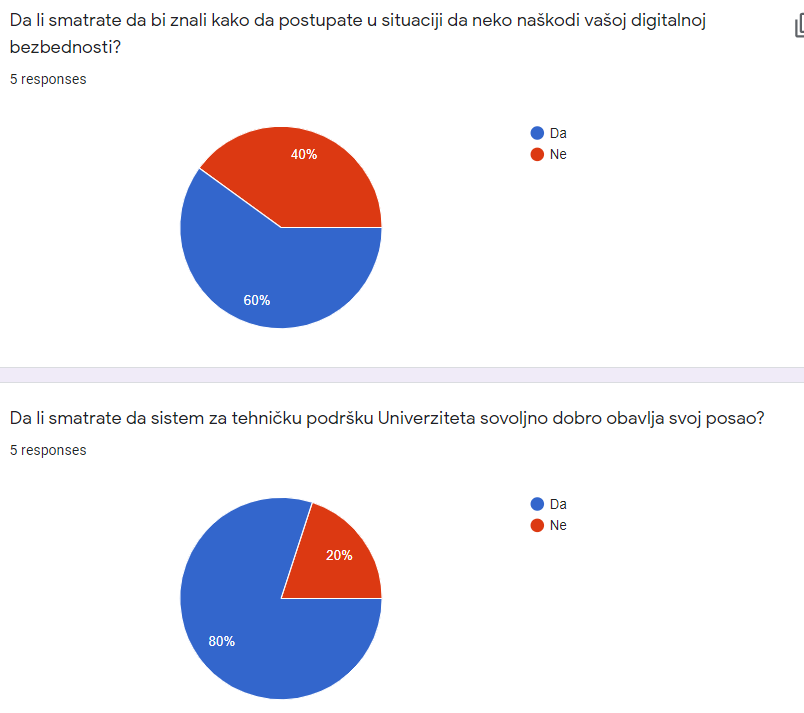
Postoje dve vrste javnih Wi-Fi veza: zaštićene i neosigurane. Svako ko je u dometu može se povezati sa nezaštićenom mrežom, dok za sigurnu mrežu obično treba lozinka.

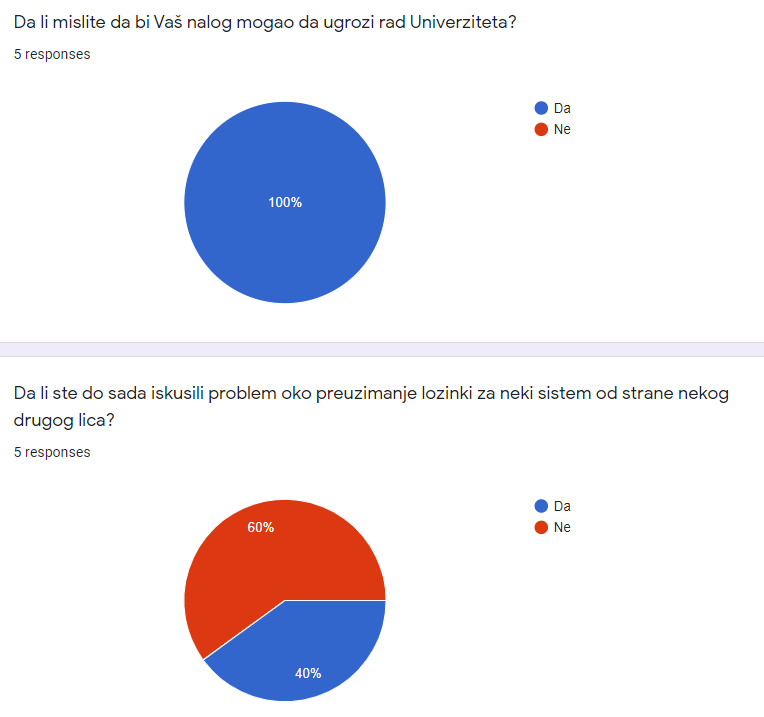
Sve javne veze se dele, što znači da je vidljiv svaki nešifrovani saobraćaj koji šaljete ili prenosite - pa iskusnom hakeru ne bi bilo previše zeznuto pregledati vaše podatke. Povezivanjem sa nezaštićenom mrežom (mrežom bez lozinke), drugima je još lakše da presretnu vaše podatke.Ako se odvodite negde na posao, možda bi bilo vredno osigurati oflajn pristup svemu što vam treba, kako biste izbegli upotrebu javne Wi-Fi mreže.



Naravno svi ispitani korisnici su odgovorili da znaju da im lozinke mogu biti pokupljene kada su povezani na javnu WiFi mrežu ali sa odgovorima na prethodno pitanje korisnici su i dalje u većoj meri koristili ove javne mreže te to govori da je ipak spoznaja problema tu ali obazrivost je mala sve dok se to i njima samima ne dogodi.

Takođe je dobro to što korisnici smatraju da su naravno i lozinke za sisteme univerziteta veoma bitne i naravno važne što se prvo ogleda u pogledu studenata koji bi onda dobili kontrolnu ulogu profesora ili asistenta a isto tako potrebne možda od strane konkurenata za pristup sistemu iznutra ili od strane neke neovlašćene malverzacione kontrole.

Ono što je ovde prikazano je odgovor da su svi ispitani korisnici svesni da bi njihov preotet nalog mogao da ugrozi sam rad univerziteta. To može biti na više nazličitih načina, kroz neovlašćene pristupe, iznude, oštećenja podataka u sistemima univerziteta, otvaranjem prostora za bezbedonosne pretnje kolegama i još mnogo drugih.

Iako je većina ispitanika navela da bi znala kako da odreaguje kako da postupa u situaciji a ima neki vid napada na digitalnu bezbednost te da joj ona bude i ugrožena, ovo sve je u kontradiktornosti sa prethodnim pitanjem gde je većina navela da nije iskusila neki vid problema odnosno napada. Ovo i govori o blagom osećaju da povreda bezbednosti nije veliki problem za korisnike odnosno da ga je ne smatraju nekom bitnom stavkom digitalnog sveta. Ovde je zbog toga dat kratak pregled osnova šta bi trebalo uraditi:

Preuzimanje podataka je često rezultat curenja podataka. I trebali biste biti informisani ako neki od vaših podataka procuri, jer postoje stroga pravila o preduzećima koja to brzo rade što bi u ovom primeru bila tehnička služba digitalne bezbednosti Univerziteta.

Vi sami možete brzo da saznate da li je na vašu adresu e-pošte uticalo kršenje podataka tako što ćete otići na veb stranicu <https://haveibeenpwned.com/> (Da li sam bio pod nadzorom) Ako je vaš nalog pronađen, promenite lozinku za prijavljivanje - i razmislite o bilo kom drugom nalogu za koji ste koristili istu lozinku (ne da bi to trebalo da radite, naravno).

# Korišćena literatura. : (opciono)