# Pitanja Lozinka

1. **Da li znaš sta je lozinka?**
2. Riječ duža od 8 karaktera koja sadrži specijalne znakove
3. Lozinka je niz tajnih znakova koji nam omogućavaju provjeru da li zaista pravi korisnik pristupa nekom nalogu, uređaju, aplikaciji...
4. Lozinka je niz tajnih znakova koji nam omogućavaju provjeru da li zaista pravi korisnik pristupa nekom nalogu, uređaju, aplikaciji...
5. Upustvo za korišćenje aplikacija ili igrica

**Edukativni tekst:**

Lozinka, koja se ponekad naziva i šifra je tajni podatak, obično niz znakova, koji se koriste kako bi se uspješno provjerilo da li pravi korisnik pokušava da pristupi nekom nalogu, aplikaciji ili uređaju i da mu se omogući pristup i korišćenje

1. **Da li znaš koja nauka se bavi proučavanjem lozinki?**
2. Matematika
3. Šifrovanje(kriptografija)
4. Informatika

**Edukativni tekst:**

Kriptografija ili šifrovanje je nauka koja se bavi metodama očuvanja tajnosti informacija.

1. **Šta misliš koja od sledećih lozinki je najčešće korišćena lozinka?**
2. 123456
3. Asdf
4. Iloveyou
5. Monkey

**Edukativni tekst:**

Najčesće korišćena lozinka je samim tim i najslabija lozinka. Ljudi često koriste lozinke koje je lako zapamtiti, a samim tim jedna od najkorišćenih jeste 123456. Slabe lozinke su jedan od načina gubitka povjerljivih informacija.

1. **Šta misliš da li je tačna sledeća definicija o jakim lozinkama - Jaka lozinka se sastoji od najmanje 8 znakova. Trebalo bi da postoji kombinacija znakova- velikih i malih slova, brojeva i simbola (@, #, $, %, itd.). Jaka lozinka ne smije biti neka uobičajna riječ ili fraza?**
2. Tačno
3. Netačno

**Edukativni tekst:**

Što više znakova sadrži neka lozinka, to je jača. Kombinacija različitih simbola i znakova omogućava nam da povećamo sigurnost lozinke. Potrebno je izbjegavati uobičajne fraze, poznate citate i tekstove pjesama.

1. **Odaberi primjere za koje misliš da predstavljaju jaku lozinku:**
2. Suncandan
3. Patern2kosarka#4muski!
4. laura123
5. 987654321

**Edukativni tekst:**

"Patern2kosarka#4muski!" bi bila jaka lozinka jer ima 22 znaka, uključuje velika i mala slova, brojeve i specijalne znakove. Takođe ne predstavlja uobičajenu frazu.

1. **Šta misliš da li treba koristiti lične podatke za lozinku?**
2. Da
3. Ne

**Edukativni tekst:**

Nemojte koristiti lozinke koje su zasnovane na ličnim podacima kojima je lako pristupiti ili pogoditi. To znači da ne treba da koristiti važne datume, poput svog rođendana, rođendana svojih roditelja i sl. Ne treba koristiti ni imena ljubimaca ili vama bliske osobe.

1. **Da li znaš kako da se osiguraš u slučaju da zaboraviš lozinku?**
2. Kažete staratelju ili roditelju koji može da zaštititi lozinku za vas
3. Zapišete na papir pored računara
4. Kažete svojim prijateljima koji će vas podsjetiti ukoliko zaboravite

**Edukativni tekst:**

Nikada ne dijelite lozinke sa drugim ljudima čak i ako su to vaši prijatelji. Ispravno je jedino podijeliti svoju lozinku sa roditeljima koji će da je čuvaju i osiguraju za vas.

1. **Šta misliš da li je dobra ideja zapisivati lozinke?**
2. Nije, jer neko može pronaći vašu lozinku
3. Jeste, ukoliko je taj papir na bezbjednom mjestu(recimo kod vaših roditelja)
4. Edukativni tekst:

**Edukativni tekst:**

Zapisivanje lozinki je dobra ideja, ali zapisanu lozinku obavezno treba držati na bezbjednom mjestu, a to je kod vaših roditelja. Nemojte je zapisivati i ostavljati negdje gdje drugi mogu da je pronađu. Ako je zapišete i ostavite na svom stolu, pored računara, ili, još gore zalijepite papir sa lozinkom na računar činite je lako dostupnom drugim ljudima.

1. **Šta misliš da li je pametno koristiti istu lozinku za vise različitih naloga?**
2. Jeste, jer nam omogućava da ne pamtimo veliki broj lozinki
3. Jeste, samo ukoliko imamo jaku lozinku
4. Nije, jer to nije bezbjedno

**Edukativni tekst:**

Možete korisiti istu lozinku za naloge do kojih vam zaista nije stalo i koji se ne mogu koristiti za pristup drugim nalozima. Osim toga, trebalo bi da imate posebnu lozinku za sve. Ukoliko neko dođe do lozinke tada su svi nalozi na kojima imate istu lozinku ugroženi.

1. **Šta misliš, u proseku, koliko onlajn naloga ljudi imaju za koje su potrebne lozinke?**
2. 3
3. 9
4. 23
5. 400

**Edukativni tekst:**

Prema istraživanjima je pokazano da ljudi u prosjeku imaju 23 online naloga za koje koriste 13 jedinstvenih lozinki.

1. **Da li znaš na koji od sledećih načina informacije mogu pasti u pogrešne ruke?**
2. Kreiranje slabih lozinki
3. Dodavanje pogrešnih primalaca u e-poštu
4. Izgubljeni ili ukradeni uredjaji
5. Sve od navedenog

**Edukativni tekst:**

Ljudi često svojim postupcima mogu da dovedu da povjerljive informacije padnu u pogrešne ruke. Jednostavna rešenja da ne dodje do toga su:

da dvaput provetite sve e-pošte prije nego što budu poslate. Kreirajte jake lozinke, mijenjajte podrazumijevane lozinke, vodite računa o svim prenosivim uređajima koji se koriste.

1. **Šta misliš da li je pametno koristiti istu lozinku (ukoliko je jaka) godinama?**
2. Da
3. Ne

**Edukativni tekst:**

Ukoliko koristite istu lozinku godinama velika je mogućnost da može biti otkrivena od strane zlonamjernih korisnika.

1. **Šta misliš kolika je minimalna dužina lozinke koju nije moguće razbiti putem korišćenja kombinacije svih mogućih karaktera?**
2. 8 karaktera
3. 3 karaktera
4. 12 karaktera

**Edukativni tekst:**

Za lozinku koja ima dužinu 12 karaktera bi bilo potrebno 34 hiljade godina da bi se razbila, dok bi se lozinke od 8 karaktera mogla razotkriti u kratkom roku.

1. **Šta misliš da li je pametno označiti "pamćenje lozinke" prilikom logovanja na neki sajt ukoliko taj računar koristi više ljudi?**
2. Da
3. Ne

**Edukativni tekst:**

Ne treba označiti "pamćenje lozinke" na računaru koji koristi više ljudi jer samim tim vaše privatne informacije mogu pasti u ruke zlonamjernih ljudi.

# Pitanja online maltretiranje

1. **Šta je online maltretiranje (zlostavljanje na mrezi)?**
2. Predstavlja ponašanje koje ima za cilj da zadirkuje, ponižava ili uznemirava neku osobu putem internet
3. Predstavlja pristup internet sadržaju koji namenjen djeci.
4. fizički napad od strane nepoznate osobe (Npr. fizički napad ispred vaše škole ili na drugim mjestima)

**Edukativni tekst:**

Online maltretiranje(zlostavljanje)je svako maltretiranje koje se odvija „ virtuelno “preko različitih uređaja i platformi. Za razliku od drugih oblika maltretiranja, maltretiranje preko interneta se može desiti u bilo koje doba dana ili noći – kad god i gde god vi ili vaši prijatelji imate pristup internetu

1. **Da li se slažete sa sledećom izjavom:**

**„Online maltretiranje(zlostavljanje) nije loše, to nije zlostavljanje kao u pravom životu jer ga obično lako zaboravite “**

1. Da
2. Ne

**Edukativni tekst:**

Nikada nemojte da se zavaravate, zlostavljanje na internetu je podjednako loše i opasno kao i bilo koje drugo zlostavljanje.

1. **Kako se maltretiranje(zlostavljanje) putem interneta razlikuje od ostavih tipova nasilja?**
2. Može da bude anonimno(od strane nepoznate osobe)
3. Zlostavljanje se vrši licem u lice
4. Teže se sprečava od ostalih tipova nasilja

**Edukativni tekst:**

Zlostavljanje putem interneta se ne odvija licem u lice vec putem društvenih mreža, emailova i drugih tipova elektronske komunikacije. Samim tim počinilac moze da ostane anonimam odnosno skriven, pa se zbog toga ovaj vid nasilja teže sprečava.

1. **Da li znaš koji od navedenih primjera predstavljaju online maltretiranje (više tačnih odgovora)?**
2. Osramotiti nekoga u javnosti
3. Saplitanje/Guranje
4. Pisanje  ružnih komentara na društvenoj mreži koji mogu da povrede druge osobe
5. Slanje prijetećih poruka putem internet

**Edukativni tekst:**

Online maltretiranje predstavlja vid nasilja koji nije fizičke prirode, odnosno vid nasilja

koji se sprovodi putem interneta. Znači prijeteće poruke kao i uvredljivi komentari su jedan od tipova ovakvog načina zlostavljanja.

1. **Šta mislis da li postavljanje slike na kojoj je vaš prijatelj bez njegove dozvole predstavlja online maltretiranje(zlostavljanje)?**
2. Da
3. Ne

**Edukativni tekst:**

Bilo kakvo postavljanje slika bez odobrenja koje na neki način uznemiravaju i vrijeđaju osobu sa slike je jedan vid online maltretiranja.

1. **Šta biste uradili ukoliko se nađete u situaciji:**

**Neko je u školi snimio vaseg drugara/drugaricu kako se neprikladno ponaša na vašoj školskoj zabavi. Vi ste dobili taj snimak?**

1. Nasmijao/la bih se i proslijedila snimak dalje
2. Ispričao/la nekoj pouzdanoj odrasloj osobi situaciju, recimo roditelju ili uciteljici
3. Pogledao/la snimak ali ne bi ga dalje širio

**Edukativni tekst:**

Ovo je oblik nasilja putem interneta. Nemojte se pridružiti niti podržavati prosleđivanjem objave! Prijavite to nastavniku ili osoblju. Možete razgovarati sa osobom na snimku i ponuditi joj podršku kako biste je obavestili da nije sama.

1. **Šta mislite da li je ljudima lakše da vrijeđaju jedni druge putem interneta (preko društvenih mreza) nego u stvarnom životu?**
2. Da
3. Ne

**Edukativni tekst:**

Ljudima je lakše da pišu štetne stvari drugima na mreži nego u stvarnom životu. Bez znakova koje dobijate iz razgovora sa drugom osobom licem u lice, često se možete osećati moćnije jer mozete biti „nepoznati “na mreži.

1. **Da li znaš koji su znači koji ukazuju na to da je neka osoba možda zlostavljana preko interneta?**
2. Voli da ide u školu i jako je komunikativna
3. Nervozna je, bez samopouzdanja i jako povučena
4. Provodi mnogo vremena sa prijateljima
5. Postaje samouvjerena poslije gledanja u telefon

**Edukativni tekst:**

Ukoliko je neko maltretiran putem interneta mogući simptomi su često: Strah ili nervoza da ide u školu (preskakanje škole). Oni najčesće znaju da budu povučeni i provode mnogo vremena sami i nemaju samopouzdanja. Gledanje u njihove telefone ili uređaje moglo bi ih uznemiriti ako su primili poruku od nasilnika.

1. **Šta biste uradili da dođete u situaciju da vas neko zlostavlja putem interneta?**
2. Ne bi govorili odraslima o tome
3. Odmah obrisali poruku i zanemarili je
4. Odgovorili na poruku takođe vređajućim sadržajem
5. Sačuvali poruku i prijavili ili blokirali napadača

**Edukativni tekst:**

Ne odgovarajte! Oni će mnogo brze izgubiti interesovanje ako ne dobiju odgovore. Takođe je veoma važno sačuvati sve poruke primljene od napadača kao dokaz. Napravite snimke ekrana ili ih odštampajte. Kada to uradite, obavezno ih blokirajte (tu opciju imate na većini platformi društvenih medija)

1. **Šta mislite koliko djece će obavijestiti svoje roditelje ako dođu u situaciju da budu maltretirani(zlostavljani) putem interneta?**
2. Jako mali broj
3. Svi
4. Polovina

**Edukativni tekst:**

Prema istraživanjima pokazano je da će samo jedno od desetoro djece reći svojim roditeljima/starateljima da su bili zlostavljani putem interneta. Ta odluka je jako loša jer postoji mogućnost da će se maltretiranje(zlostavljanje) nastaviti i da počinilac neće biti otkriven.

1. **Neko koga poznajete je zlostavljan putem interneta, a vi poznajete napadača, šta biste od navedenog uradili u takvoj situaciji?**
2. Rekli svojim prijateljima da tu osobu izbjegavaju i blokiraju
3. Obavijestili stariju osobu o njegovom ponasanju
4. Razotkriti  ga i vrijedjati pred ostalima

**Edukativni tekst:**

Nikada se sami ne ponašajte kao nasilnik, često je i toj osobi potrebna podrška i često postoje razlozi njihovog ponašanja. Najpametniji način jeste reći odrasloj osobi koja će da porazgovara sa njim i pokuša da objasni da takvo ponašanje nije ispravno.

1. **Šta misliš koji od sledećih podešavanja na društvenim mrežama smanjuju šanse da dođe do maltretiranja(zlostavljanja) na internetu?**
2. Samo osobe kojima dozvolite mogu da postanu vaši prijatelji/pratioci
3. Nepoznate osobe nemaju mogućnost da gledaju i komentarisu vaše objave
4. Isključivanje ili blokiranje korisnika za koje smatrate da nisu bezbjedni
5. Sve od navedenog

**Edukativni tekst:**

Svaka društvena mreža nudi različite alate koji omogućavaju korisnicima da ograniče ko može da komentariše, gleda objave ili ko može da postane njihov prijatelj ili pratilac. Mnogi od ovih alata uključuju jednostavne korake za blokiranje, isključivanje ili prijavljivanje nasilja na internetu. Što znači da svako od ovih mogućnosti da postavimo ograničenja i zaštitimo sebe pomažu u smanjenju šansi da dođe do maltretiranja na internetu?

# Pitanja krađa naloga

1. **Kao što znamo većina korisnika Interneta ima više identiteta (nešto što je jedinstveno za neku osobu i omogućava nam da je razlikujemo od drugih). Da li znaš šta od navedenog predstavlja identitet korisnika?**
2. Nalozi na društvenim mrežama
3. Visina nekog korisnika
4. Adresa korisnika
5. Broj pasoša

**Edukativni tekst:**

 Većina korisnika Interneta ima više identiteta a to su: Nalog na Facebook-u, Gmail, Twitter, Snapchat, itd., kreditne i debitne kartice, broj vozačke dozvole, lične karte, pasoša. Dok neke fizičke osobine ili nesto što nije jedinstveno za korisnike ne predstavljaju njihov identitet. Adresa korisnika takođe ne predstavlja identitet korisnika jer ne mora biti jedinstvena (može više ljudi da živi na istoj adresi.)

1. **Da li smatrate da ukoliko ste mlađi od 18 godina ne morate da brinete o krađi identiteta?**
2. Da
3. Ne

**Edukativni tekst:**

Ukoliko imate manje od 18 godina, odnosno ukoliko niste punoljetni takođe možete da se suočite sa krađom identiteta.

1. **Šta mislite da li je “krađa vašeg naloga “(nalog na Instagram-u, Faceebook-u, Gmail, Snapchat) krađa identiteta?**
2. Da
3. Ne

**Edukativni tekst:**

Obzirom na to da svaki od vaših naloga na društevnim mrežama predstavljaju vaš identitet, samim tim i krađa vašeg naloga jeste krađa identiteta.

1. **Da li znaš sa koje od sledećih e-adresa dolaze poruke o vašem Facebook nalogu? (Više tačnih odgovora)**
2. fb.com
3. facebook.com
4. facebook123.com
5. face\_\_book.com
6. facebookmail.com

**Edukativni tekst:**

E-poruke o vašem Facebook nalogu uvijek dolaze sa adresa: fb.com, facebook.com, facebookmail.com. Uvijek možete da posjetite [www.facebook.com](http://www.facebook.com/) ili otvorite aplikaciju Facebook da biste provjerili da li ste dobili neku važnu poruku od Facebook-a.

1. **Šta misliš kako prepoznati sumnjive poruke na Facebook nalogu?**
2. Pijrete brisanjem ili zabranom vašeg Facebook naloga
3. Traže novac
4. Nude poklone
5. Sve od navedenog

**Edukativni tekst:**

Ako umijete da prepoznate sumnnjive poruke ili e-poruke, onda ćete mozda moći da izbjegnete prevare sa krađom identiteta. Ne vjerujete porukama koje: traže novac, nude poklone ili prijete brisanjem ili zabranom vašeg Facebook naloga.

1. **Ukoliko ste recimo na neki način došli do lozinke vašeg prijatelja/prijateljice na njihovom Facebook nalogu. Šta mislite da li prijava na njihov nalog, čitanje poruka ili pisanje istih u njihovo ime krivično djelo?**
2. Nije
3. Nije, zato sto se radi o mojim prijateljima
4. Jeste

**Edukativni tekst:**

Svaki vid korišćenja tudjeg identiteta jeste krivično djelo, bez obzira da li se radi o vašim prijateljima i poznanicima.

1. **Da li znas koja je zvanična Instagram adresa e-poste?**
2. [\_security@rnail.instagrarn.com](mailto:_security@rnail.instagrarn.com)
3. [security@mail.instagram.com](mailto:security@mail.instagram.com)
4. [security@m.instagram.com](mailto:security@m.instagram.com)

**Edukativni tekst:**

security@mail.instagram.com je zvanična Instagram adresa e-pošte. Međutim postoje određene taktike kao što je malo izmijenjena (npr. u prvom primjeru m je zamijenjeno sa rn) adresa e-pošte tako da vas um ne uhvati razliku između orginala i lažne. Zbog toga budite pažljivi jer svaka poruka koja nije od zvanične Instagram adrese može biti pokušaj krađe vašeg naloga.

1. **Primili ste poruku na vašem Instagram nalogu od korisnika sansumg\_rs .Poruka glasi:**

**“Danas je vas srećan dan. Odabrali smo vas kao dobitnika nagradne igre za telefon marke Samsung Galaxy A13. Sve što nam treba jeste da uđete na dati link i unesete vaše podatke kako bismo vas registrovali kao dobitnika. Šta biste uradili u takvoj situaciji, da li biste ušli u link I unijeli podatke?**

1. Da
2. Ne

**Edukativni tekst:**

Dijeljenje ličnih podataka nepoznatim stranicama i autorima može dovesti do krađe vašeg naloga i nikako se ne preporučuje. Ukoliko mislite da je stranica pouzdana opet ni u kom slučaju ne dijelite svoje podatke bez nadzora i savjeta roditelja.

1. **Ukoliko mislite da je vaš nalog na Instagramu “hakovan” (neko je neovlašćeno pristupio vašem nalogu i predstavlja se kao vi) ili je izvršen pokušaj hakovanja ali jos uvijek možete da se prijavite, postoje stvari koje mozete uraditi da zaštitite svoj nalog. Šta od navedenog mislite da je ispravno uraditi?**
2. Promijeniti lozinku ili poslati sebi e-poštu za poništavanje lozinke
3. Da su vaš broj telefona i adresa e-pošte u postavkama naloga tačni
4. Uklljučite dvostepenu autentifikaciju (provjera da li ste vi pravi vlasnik toga naloga na 2 načina recimo prilikom prijave pored lozinke Instagram vam traži i unos koda koji dobijate na svoj broj telefona)
5. Sve od navedenog

**Edukativni tekst:**

Neki od načina na koji možete zaštiti svoj nalog ukoliko sumnjate na pokušaj hakovanja ili hakovanje jesu: promjena lozinke, kreiranje jake lozinke, u postavkama naloga obavezno da stoji tačan broj vašeg telefona I tačna email adresa, dvostepena autentifikacija. Ovi vidovi zaštite se takodje preporučuju odmah pri kreiranju naloga na društvenoj mreži Instagram.

1. **Ukoliko imate nalog na nekoj od društevnih mreža (recimo nalog na Facebook-u i Instagram-u, Twitter-u). Šta misliš šta se može desiti ukoliko dođe do krađe nekog od vaših naloga, a da toga niste svjestni? (Više tačnih odgovora)**
2. Mogu doći do vaših ličnih podataka
3. Ne mogu doći do ličnih podataka
4. Mogu doći do osjetljivih informacija o vama
5. Ništa od navedenog

**Edukativni tekst:**

Krađa nečijeg naloga na društvenim mrežama najčešće ne bude zaustavljena samo na tome. Hakeri dolaze do vaših ličnih podataka (recimo iz postavki profila), dobijaju osjetljive informacije o vama (npr. Iz poruka sa vašim prijateljima). Nikako nije pametno koristiti iste lozinke za sve profile jer u tom slučaju krađom jednog vašeg naloga dobijaju pristup i svim drugim nalozima.

1. **Šta misliš da li je najpopularnija vrsta krađe identiteta odnosno kradje naloga putem e-pošte?**
2. Da
3. Ne

**Edukativni tekst:**

Najpopularnija vrsta krađe identiteta je *phishing* putem e-pošte. Izraz „phishing’ je nastao od engleske rijeci „fishing“(pecanje) pošto hakeri ovakvom poštom „bacaju udicu“ kao u pecanju i čekaju da se neko od ciljanih korisnika „upeca“.

1. **Da li znaš šta od navedenog predstavlja karakteristike e-pošte koja se koristi za krađu identiteta(phishing)?**
2. Hakeri(napadači) koji šalju ovakve poruke često koriste adrese koje su slične zvaničnim adresama.
3. Sadržaj poruke najčešće sadrži određene gramatičke i pravopisne greške
4. U prilogu mejla najčesće salju neki link ili sadržaj za preuzimanje
5. Poruke su najčešće napisane tako da izazovu paniku
6. Sve od navedenog

**Edukativni tekst:**

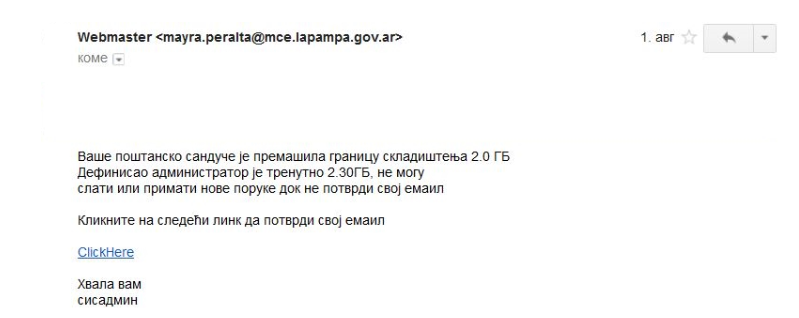
E-poruke koje se koriste za krađu identiteta(phishing) najčešće imaju određene propuste i odlike na koje je potrebno obratiti pažnju. Hakeri(napadači) koji šalju ovakve poruke često koriste adrese koje su slične zvaničnim adresama, pokušavaju da nađu najsličniju moguću adresu i na taj način izvrše prevaru. Sadržaj poruke najčesće sadrži određene gramatičke i pravopisne greške (greške u padežu i rodu, kao i nepostojanje dijakritičkih znakova (š, đ, ž, č, ć)). U prilogu mejla najčesće šalju link na koji treba da kliknete i unesete svoje lične podatke ili vas navode da preuzmete maliciozni sadržaj (bilo koji fajl kada ga preuzmete na računar i pokrenete, u pozadini izvršava kod koji omogućava kriminalcima da pristupe vašem računaru i urade manje–više šta žele.) iz priloga. Poruke su najčešće napisane tako da izazovu paniku (da je vaš nalog u opasnosti ili da mu je neko pristupio). Što znači da je sve od navedenog neka od odlika e-poruka za krađu identiteta.

1. **Ukoliko ste primili poruku sa 'hajhsyye@sound.ocn.ne.jp' koja vas poziva da resetujete lozinku. Šta biste uradili?**
2. Promijenili lozinku prema upustvima datim u e-poruci
3. Ni bi nastavili i izbrisali bi poruku

**Edukativni tekst:**

         Uputstva iz poruke koje nisu sa zvaničhih email adresa nikako ne treba pratiti.To su najčešće zlonamjerne e-poruke za krađu lozinki i privatnih informacija.

1. **Na sledecoj slici imas primjer jedne e-poruke za pokusaj kradje identiteta:**



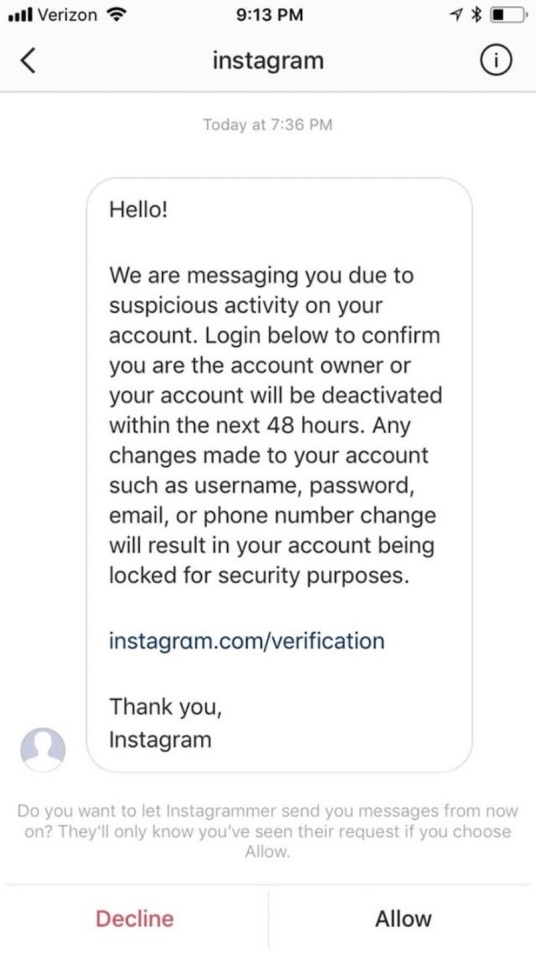
**Da li možes da prepoznaš koja od karakteristika ovakvih poruka je vidljiva na ovoj slici? (Više tačnih odgovora)**

1. Email adresa  je slična zvaničnoj adresi
2. Sadržaj poruke sadrži gramatičke ili pravopisne greške
3. U prilogu mejla je poslan link
4. Poruka je napisana tako da izazove paniku

**Edukativni tekst:**

Na datoj slici možemo jasno da uočimo gramatičke greške. Očigledno je da je orginalna poruka provučena kroz “Google Translate” ili neki sličan online prevodilac. Takođe možemo da uočimo da je u prilogu poruke poslan i link “ClickHere” kako bi se pratila dalja upustva. Jedno i drugo je jedna od osnovnih odlika poruka koje imaju za cilj krađu naloga odnosno krađu identiteta.

1. **Na Instagram nalogu ste dobili ovakvu poruku:**



**“Zdravo! Šaljemo vam poruku zbog sumnjivih aktivnosti na vašem nalogu. Prijavite se ispod da biste potvrdili da ste to vi ili će vam nalog biti deaktiviran u narednih 48 sati. Sve promjene unešene na nalog kao što su korisničko ime, lozinka, imejl ili promjena broja telefona će rezultirati da vaš nalog bude zaključan iz bezbjednosnih razloga.**

**instagrαm.com/verification**

**Hvala Vam,**

**Instagram „**

**Šta biste uradili u ovakvoj situaciji:**

1. Ušli na link „instagrαm.com/verification“ i pratili dalja upustva da bih spriječili deaktivaciju naloga
2. Nikako ne ulaziti u priloženi link jer može biti pokušaj krađe naloga. Obratiti se nekoj stručnijoj osobi

**Edukativni tekst:**

Ovakva poruka na Instagramu predstavlja POTPUNU PREVARU. Stručnjacima je potrebno samo par minuta da otkriju da su ovakve poruke prevara koja izaziva krađu naloga a zatim i ličnih podataka. Iako naizgled sve izgleda u redu, ukoliko bolje pogledamo link „instagrαm.com/verification “primijetićemo da "a" u "instagram.com" nije a, to je ALFA "α" znak. Ovo je dokaz da je poruka nije došla od strane Instagrama već je samo pokušaj krađe vašeg naloga. Zbog toga ukoliko primite ovakvu poruku nikako ne preduzimajte korake sami već tražite savjet od roditelja ili stručnih osoba.

**Licni Podaci**

1. **Da li znaš šta su lični podaci?**
2. Svi oni podaci koji se odnose na određeno fizičko lice, na osnovu kojih ono može biti identifikovano, a kojima se može ugroziti njegova privatnost
3. Ne predstavljaju fizičke i karakterne osobine neke osobe
4. Sve informacije koje znamo o nekom licu bilo da su pouzdane ili ne

**Edukativni tekst**:

Lični podaci su svi oni podaci koji se odnose na određeno fizičko lice, na osnovu kojih ono može biti identifikovano, a kojima se može ugroziti njegova privatnost, takođe u lične podatke spadaju i fizičke osobine osobe

1. **Sta misliš šta od navedenih primjera predstavljaju lične podatke neke osobe?**
2. ime I prezime
3. kucna adresa
4. broj lične karte ili pasoša
5. email adresu kao sto je [imeprezime@gmail.com](mailto:imeprezime@gmail.com)
6. ime vašeg prijatelja
7. marka telefona koji koristiti

**Edukativni tekst**:

Ime i prezime, kućna adresa, broj lične karte kao i email adresa koja u sebi sadrži ime i prezime predstavljaju lične podatke pomoću kojijh osoba može biti identifikovana dok ime vašeg prijatelja i marka telefona nisu podaci pomoću kojih mozemo identifikovati neku osobu pa samim tim ne spadaju u lične podatke.

1. **Da li znaš sta je zaštita podataka?**
2. Skup određenih procesa koje se koriste da bi se osigurala privatnost i dostupnost vaših podataka.
3. Zapisivanje ličnih podataka na papir, kao vid zaštite
4. Sakrivanje podataka od svojih roditelja

**Edukativni tekst**:

Zaštita podataka je skup određenih procesa koje se koriste da bi se osigurala privatnost i dostupnost vaših podataka

1. **Šta misliš da li je pravo na zaštitu ličnih podataka i privatnosti jedno od osnovnih ljudskih prava?**
2. Da
3. Ne

**Edukativni tekst:**

Pravo na privatnost i zaštitu ličnih podataka jeste jedno od osnovnih ljudskih prava. Ovo pravo odnosi se podjednako i na digitalno okruženje

1. **Šta misliš zašto je važna zaštita ličnih podataka?**

**(Više tačnih odgovora)**

1. zbog sprečavanja gubitka podataka
2. zbog sprečavanja razmjene informacija
3. zbog sprečavanja krađe podataka

**Edukativni tekst:**

Zaštita podataka je važna za svakog pojedinca kao i organizaciju jer sprečava gubitak i krađu ličnih podataka.

1. **Da li znaš na koji od sledećih načina dijeliš svoje lične podatke na Internetu?**
2. Otvaranje profila na nekoj društevnoj mreži
3. Postavljanje fotografija
4. Preuzimanjem nečeg sa Interneta
5. Sve od navedenog

**Edukativni tekst**:

Postoji više kategorija ličnih podataka korisnika na Internetu. Jedna od kategorije ličnih podataka na Internetu ubraja one podatke koje korisnici sami ostavljaju prilikom korišćenja Interneta, obično svjestno mada nekada i nenamjerno.Te podatke ostavljamo npr. prilikom kupovine nekih proizvoda, preuzimanja nečega sa interneta, postavljanja fotografija, otvaranja profila na nekoj društvenoj mrezi itd.)

1. **Šta misliš na koji od sledećih načina dolazi do krađe ličnih podataka?**

**(Vise tacnih odgovora)**

1. slabe lozinke
2. ljudske greske
3. jake lozinke
4. oprez prilikom dijeljenja ličnih podataka
5. dvostepena autentifikacija (provjera na više načina da li pravi korisnik pristupa nekom servisu)

**Edukativni tekst**:

Do krađe ličnih podataka može doći na više različitih načina. Neki od tih su slabe lozinke (korišćenje lozinke koju je lako pogoditi ili korišćenje iste lozinke za više naloga može omogućiti napadačima da dobiju pristup podacima.), ljudske greške (uključuju slanje osjetljivih informacija pogrešnoj osobi, kao što je greškom slanje e-pošte na pogrešnu adresu, prilaganje pogrešnog dokumenta ili predaja fizičkog fajla nekome ko ne bi trebao imati pristup informacijama.)

1. **Na društvenoj mreži ste upoznali nekoga vaših godina i ta osoba vam traži vašu adresu ili broj telefona kako biste mogli da se nađete. Šta biste uradili u takvoj situaciji?**
2. Poslao/la bih broj telefona i adresu, jer je to način da se uživo upoznamo
3. Obratio/la bih se roditeljima za savjet

**Edukativni tekst:**

Nikad ne bi trebalo da date svoje ime ili adresu ili bilo kakav lični podatak nekome koga upoznajete na mreži. Ako zaista želite da se uživo upoznate provjerite sa roditeljima da li mogu da smisle bezbjedan način da to organizuju.

1. **Šta misliš da li je važno da poštujemo uzrasna ograničenja prilikom registracije na neke sajtove, društvene mreže itd.?**
2. Da
3. Ne

**Edukativni tekst:**

Veliki broj sajtova i aplikacija traži od korisnika da prilikom otvaranja profila navede svoj uzarast (godine starosti). Na ovim servisima propisana je donja uzrasna granica za njihovo korišćenje baš iz razloga jer nije dozvoljeno prikupljanje ličnih podataka od djece bez odobrenja njegovih roditelja ili staratelja. Što znači da je uvijek važno da poštujemo uzrasna ogranicenja prilikom bilo kakve registracije.

1. **Da li znaš koja je uzrastna granica za korišćenje društvenih mreža (npr. Facebook, Snapchat, Twitter, Instagram, Skype)?**
2. 18 godina
3. 10 godina
4. 13 godina
5. 20 godina

Edukativni tekst:

Iako je za korišćenje većine društvenih mreža (npr. Facebook, Snapchat, Twitter, Instagram, Skype) uzrasna granica 13 godina istraživanja pokazuju da veliki procenat dece (kako u svijetu, tako i u Srbiji) počinje da koristi ove mreze u mnogo ranijem uzrastu od propisanog.

1. **Da li znaš šta od navedenog se može desiti ukoliko neko dijete prilikom otvaranja profila na nekom servisu ili društvenoj mreži navede da je starije nego što jeste?**
2. Bilo bi izloženo sadržajima koji su neprikladni za njegov ili njen uzrast
3. Ne bi izloženo sadržajima koji su neprikladni za njegov ili njen uzrast
4. Izgubi dodatne zaštite i postavke privatnosti koje se odnose na uzrast mlađi od navedenog
5. Imalo bi I dalje zaštite i postavke privatnosti koje se odnose na njegov uzrast

**Edukativni tekst**:

Ukoliko dijete prilikom otvaranja profila na nekom servisu ili društvenoj mreži navede da je starije nego što jeste, može se desiti da bude izloženo sadržajima koji su neprikladni za njegov uzrast (uznemirujući, nasilni) ili da vidi nesto što ne želi, da izgubi dodatne zaštite i postavke privatnosti koje se odnose na uzrast mlađi od navedenog. Gubitkom dodatne zaštite i privatnosti koje se odnose na dati uzrast ugrožavaju se lični podaci svakog djeteta, što naravno može dovesti do problema

1. **Da li znaš da li je zloupotreba tuđih ličnih podataka krivično djelo?**
2. Da
3. Ne

Edukativni tekst:

Svaki vid kršenja privatnosti ličnih podataka druge osobe jeste krivično djelo i kažnjivo je.

1. **Šta biste uradili da se nađete u sledećoj situaciji:**

**Od strane nepoznate osobe otvoren je nalog na društvenoj mreži Instagram, sa vašim imenom i prezimenom, sa vašim podacima, ta osoba takođe koristi i objavljuje vaše fotografije**?

1. Obratio/la bih se toj osobi putem poruke i zatražio/la brisanje lažnog naloga na moje ime
2. Zanemario/la bih to, ne smatram da je to nesto važno (vjerovatno šala od strane mojih prijatelja)
3. Odmah bih obavijestio/la svoje roditelje o takvim dešavanjima jer mogu biti opasna

**Edukativni tekst:**

Ukoliko dođete u ovakvu situaciju obavezno obavijestite svoje roditelje pa će oni poduzeti potrebne korake. Nikako ovako nešto ne zanemarujteo i ne smatrajte šalom jer osoba koja to radi može biti opasna i za vas i vaše prijatelje i potrebno je što prije otkriti “nepoznatu osobu”.

# Pitanja višestepena autentifikacija

1. **Da li znaš sta je višestepena autentifikacija?**
2. Metoda pomoću koje se korisniku odobrava pristup aplikciji ili veb stranici nakon što uspješno potvrdi svoj identitet na više različitih načina
3. Metoda pomoću koje se korisniku odobrava pristup aplikciji ili veb stranici nakon što uspješno potvrdi svoj identitet
4. Metode pomoću kojih se definišu prava pristupa nekog korisnika nakon što pristupi aplikaciji ili veb stranici

**Edukativni tekst:**

Viseštepena autentifikacija je metoda pomoću koje se korisniku odobrava pristup aplikciji ili veb stranici nakon sto uspješno potvrdi svoj identitet na više različitih načina.

1. **Koje su vrste metoda autentifikacije koje se koriste u višestepenoj autentifikaciji? (Više tačnih odgovora)**
2. Nešto što korisnik zna (lozinka)
3. Nešto što korisnik voli (omiljena pjesma.)
4. Nešto što korisnik posjeduje(mobilni telefon)
5. Nešto što korisnik jeste (otisak prsta)
6. Ništa od navedenog

**Edukativni tekst:**

Višestepena autentifikacija predstavlja viši nivo bezbjednosti i taj proces se ostvaruje pomoću 2 ili više elemenata provjere da li se o radi pravom korisniku (da li je to osoba za koju se predstavlja da jeste). Počinje sa nečim što samo vi znate (lozinka, korisničko ime), zatim nešto što korisnik posjeduje i nešto što korisnik jeste. Kombinacija bar dvije vrste metoda autentifikacije predstavlja višestepenu autentifikaciju.

1. **Sta misliš da li je dvostepena autentifikacija podskup višestepene autentifikacije?**
2. Da
3. Ne

**Edukativni tekst:**

Višestepena autentifikacija zahtijeva bar 2 načina provjere identiteta, dok dvostepena autentifikacija zahtijeva tačno 2 načina provjere identiteta. Samim tim zaključujemo da je dvostepena autentifikacija podskup od višestepene autentifikacije.

1. **Da li znaš zašto se koristi višestepena autentifikacija? (Više odgovora)**
2. ograničava broj hakerskih napada
3. omogućava kontrolu pristupa podacima nekog sistema
4. omogućava dodatnu sigurnost podataka
5. omogućava kopiranje podataka na neko drugo mjesto

**Edukativni tekst:**

Višestepena autentifikacija se prvenstveno koristi zbog dodatne sigurnosti podataka, a samim tim zbog dodatne sigurnosti podataka smanjuje se i broj hakerskih napada.

1. **Da li znaš šta od navedenog pripada metodi autentifikacije tipa “nešto što korisnik zna”?**
2. Korisničko ime
3. Otisak prsta
4. Prepoznavanje lica
5. Pin kod
6. Kreditna kartica

**Edukativni tekst:**

U metodu autentifikacije tipa “ono što korisnik zna” spada sve sto korisnik može da zapamti a zatim iskoristi u određenom trenutku (otkuca, izgovori), pa samim tim u ovo kategoriju spadaju: korisničko ime i pin kod.

1. **Da li znaš koja od metoda viseštepene autentifikacije je najsigurnija?**
2. Nešto što korisnik zna
3. Nešto što korisnik posjeduje
4. Nešto što korisnik jeste

**Edukativni tekst:**

Najsigurniji tip autentifikacije je nešto što korisnik jeste zato što se oslanja na jedinstvene biološke karakteristike svakog pojedinca kao sto su naprimjer otisak prsta, prepoznavanje glasa i lica itd. U ovom slučaju teško dolazi do prevare jer je skoro pa nemoguće kopirati otisak prsta druge osobe ili lice druge osobe.

1. **Stigla vam je poruka na telefon u kojoj se nalazi sigurnosni kod za pristup nekoj aplikaciji ili društvenoj mreži. Šta misliš u koju vrstu metoda autentifikacije spada ovaj primjer?**
2. Nešto što korisnik zna
3. Nešto što korisnik posjeduje
4. Nešto što korisnik jeste

**Edukativni tekst:**

Sigurnosni kod iz vaše poruke nije nešto što korisnik inače zna, već posredstvom mobilnog telefona dolazi do tog koda, pa samim tim zaključujemo da se radi o nečemu što korisnik posjeduje.

1. **Šta biste uradili ako biste primili sigurnosni kod u slučaju da trenutno ne pokušavate da se prijavite na vaš nalog?**
2. Iskoristićete  ga da se prijavite na nalog
3. Obratićete se roditeljima ili nekim stručnim osobama
4. Zanemarićete poruku koju ste primili

**Edukativni tekst:**

            Ukoliko primite ovakvu sigurnosnu poruku najbolje je da se obratite roditeljima ili nekoj stručnoj osobi jer u suprotnom moze doći do kradje vaseg naloga, odnosno napadač može da dobije pristup vašim ličnim podacima.

1. **Prilikom prijave na vaš nalog na društvenim mrežama sistem od vas zahtijeva unos korisničkog imena i lozinke I nakon ispravnog unosa vi možete da pristupite vašem nalogu. Šta misliš koji od sledećih tipova autentifikacije spade navedeni primjer?**
2. Višestepena autentifikacija
3. Dvostepena autentifikacija
4. Jednostepena autentifikacija

**Edukativni tekst:**

Unos korisničkog imena I lozinke predstavlja samo jednu metodu autentifikacije (ono što korisnik zna) pa samim tim ovaj primjer predstavlja jednostepenu autentifikaciju.

1. **Prilikom prijave na vaš Instagram nalog, pored vaše lozinke i korisničkog imena, sistem traži dodatno i sigurnosni kod, koji stiže na vaš broj telefona (onaj koji stoji u okviri ličnih podataka na Instagram nalogu) i tek nakon unosa koda vam je omogućen pristup nalogu.**
2. Jednostepena autentifikacija
3. Dvostepena autentifikacija
4. Višestepena autentifikacija

**Edukativni tekst:**

Unos korisničkog imena, lozinke I sigurnosnog koda predstavlja samo dvije metode autentifikacije (ono što korisnik zna i ono što korisnik ima), zbog toga ovaj primjer predstavlja dvostepenunu autentifikaciju, pošto je dvostepena autentifikacija podskup višestepene autentifikacije samim tim ovaj primjer takođe pripada i višestepenoj autentifikaciji.