



Osnove informacione bezbednosti



Preporuke za zaštitu korisničkih naloga, uređaja i podataka

Ovaj vodič sadrži ključne smernice za bezbedno korišćenje interneta, sa ciljem unapređenja informacione bezbednosti, edukacije i zaštite korisnika u onlajn okruženju.

SADRŽAJ

	ZAŠTITA	03
	PREPORUKE ZA ONLAJN KUPOVINU	06
	SAVETI ZA LOZINKE	07
	FIŠING PREVARE	08





ZAŠTITA

FAJLOVI I UREĐAJI**Ažuriranje softvera**

Zastareli softver povećava rizik od kompromitovanja uređaja. Radi smanjenja rizika, podesite automatska ažuriranja softvera i redovno proveravajte da li su operativni sistem i svi programi ažurirani. Na taj način obezbeđujete da uređaji imaju najnovije bezbednosne zacrpe i ostaju zaštićeni od poznatih ranjivosti.

Ažuriranja instalirajte što je pre moguće nakon objavljivanja, naročito kada otklanjaju kritične bezbednosne ranjivosti.

Preuzmite i instalirajte mobilne aplikacije isključivo iz zvaničnih prodavnica (*Google Play, App Store i Microsoft Store*), uz dodatnu proveru proizvođača, broja preuzimanja i korisničkih ocena.

**Zaštita datoteka**

Redovno pravite rezervne kopije važnih datoteka na eksternom disku ili u oblaku (*cloud*). Koristite antivirusni softver za zaštitu datoteka i uređaja.

**Koristite dvofaktorsku autentifikaciju (2FA)**

Nikada ne odobravajte 2FA zahtev koji niste sami pokrenuli. Pored unosa lozinke, potrebno je potvrditi svoj identitet dodatnim faktorom:

- 1 aplikacija za autentifikaciju
- 2 hardverski bezbednosni ključ
- 3 biometrijska potvrda ili
- 4 jednokratni verifikacioni kod

**Koristite lozinke**

Za svaki uređaj ili korisnički nalog postavite jedinstvenu i kompleksnu lozinku. Ne koristite istu lozinku za više korisničkih naloga, zato što kompromitovanje jednog može ugroziti i ostale.

**Šifrovanje uređaja**

Šifrujte uređaje i druge medije koji sadrže osetljive podatke.

Enkripcija štiti podatke od neovlašćenog pristupa. Posebno je efikasna u slučaju gubitka ili krađe uređaja. Pri prenosu podataka preko mreže, koristite protokole i servise koji obezbeđuju šifrovanu komunikaciju.



ZAŠTITA BEŽIČNA MREŽA



Zaštita rutera

Promenite podrazumevanu administrativnu lozinku rutera. Koristite kompleksnu lozinku za Wi-Fi mrežu.

Redovno proveravajte da li postoji nova verzija *firmware*-a za ruter. Isključite udaljeni pristup administraciji rutera, jer može predstavljati čest vektor napada.



Korišćenje WPA3 ili WPA2

Ukoliko vaš ruter podržava bezbednosni protokol WPA3 (ili bar WPA2), preporučuje se njegovo korišćenje radi zaštite podataka od neovlašćenog pristupa i/ili zloupotrebe. Važno je ne koristiti stare protokole WEP ili WPA.



Podesite zaštitni zid

Zaštitni zid (*firewall*) je sigurnosni sistem (uređaj ili softver) koji služi kao barijera između pouzdane interne mreže i manje pouzdanih spoljnih mreža, poput interneta. Zaštitni zid nadgleda i kontroliše dolazni i odlazni mrežni saobraćaj na osnovu unapred definisanih bezbednosnih pravila. Većina savremenih operativnih sistema ima ugrađen zaštitni zid koji treba ostaviti uključenim.



Nemojte koristiti zastarele uređaje

Uređaje koje više ne koristite zbog zastarelosti, isključite sa mreže. Njihova bezbednost može biti ugrožena zbog zastarelih bezbednosnih funkcionalnosti.

Ovi uređaji su ranjivi i mogu biti iskorišćeni od strane napadača za ulazak u mrežu. Resetujte uređaje na fabrička podešavanja pre nego što ih odložite ili prodate.

Posebno obratite pažnju na *IoT* uređaje, koji predstavljaju jedan od najčešćih ulaznih vektora napada. To su kamere, DVR, pametni TV uređaji i ostali.



ZAŠTITA

IDENTITET I PRIVATNOST



Zaštitite svoj onlajn identitet

Kada otvarate novi korisnički nalog, instalirate aplikaciju ili nabavljate novi uređaj, podesite bezbednosne opcije za deljenje informacija. Redovno proveravajte i ažurirajte podešavanja, da se uverite da nisu promenjena bez vašeg znanja.



Pažljivo delite informacije

Budite obazrivi pre objavljivanja bilo kog podatka na društvenim mrežama. Razmislite šta objava otkriva, ko je može videti i kako može uticati na vas i ostale osobe. Zloupotreba često počinje od informacija koje se dele na društvenim mrežama. Ograničite vidljivost ličnih podataka samo osobama kojima verujete. Napadači ove informacije mogu iskoristiti za socijalni inženjering, krađu identiteta ili pokušaje otkrivanja lozinki.



Oprezno koristite besplatne Wi-Fi mreže

Javne Wi-Fi mreže mogu predstavljati bezbednosni rizik jer korisnik nema kontrolu nad njihovom konfiguracijom i zaštitom. Isključite automatsko povezivanje na javne mreže. Ako koristite besplatne javne Wi-Fi mreže, izbegavajte prijavljivanja na korisničke naloge elektronske pošte i ne obavljajte finansijske transakcije putem aplikacija za elektronsko bankarstvo.

Ukoliko ste u mogućnosti, koristite mobilnu pristupnu tačku (*hotspot*) ili drugu pouzdanu mrežu, kako biste obezbedili sigurnu i šifrovanu vezu.



Zaključavanje ekrana

Koristite PIN, lozinku ili biometrijsku zaštitu za zaključavanje mobilnog telefona, računara, tableta i ostalih uređaja.



QR kod prevare

Česta je zloupotreba QR kodova u fišing napadima, poznata kao *quishing*. Važno je da pre skeniranja QR koda proverite njegov izvor. Skeniranje može voditi na lažnu internet stranicu ili pokrenuti preuzimanje zlonamernog sadržaja. Oprezno sa QR kodovima postavljenim na javnim mestima, oglasima i nalepnicama, jer mogu biti zamenjeni zlonamernim kodovima.



PREPORUKE ZA ONLAJN KUPOVINU



Zaštitite podatke i novac prilikom onlajn kupovine:



Koristite bezbedan način plaćanja

Za plaćanja koristite virtuelnu karticu koja nije direktno povezana sa tekućim računom. Ograničite raspoloživi iznos samo na sumu potrebnu za konkretnu kupovinu. Proverite da li adresa internet stranice počinje sa **https://**, i da li je prikazana ikonica katanca.



Redovno proveravajte svoje izvode

Proveravajte bankarske izvode i stanje na računu. Aktivirajte obaveštenja (elektronska ili SMS poruka) kao dodatni servis banke u kojoj imate račun. Na taj način, nakon svake transakcije izvršene platnom karticom, dobijate informaciju kojom se potvrđuje transakcija.



Proverite prodavca pre kupovine

Pre svake onlajn kupovine proverite prodavca i recenzije drugih korisnika. Uverite se da su navedeni kontakt podaci i fizička adresa prodavca tačni i proverljivi. Budite posebno oprezni sa prodavnicama koje nude nerealno niske cene, jer to može biti indikator potencijalne prevare. Proverite starost domena prodavca. Nedavno registrovani domeni mogu biti indikator potencijalne prevare i razlog za dodatnu proveru.



Ne delite lične podatke

PIN broj i CVV/CVC kod platne kartice, jednokratni kodovi koje dobijate na telefon putem SMS poruke ili aplikacije, kao i podaci za pristup korisničkom nalogu namenjeni su isključivo vama i služe samo za potvrdu identiteta i autorizaciju transakcija. Ove podatke nikada ne treba deliti sa drugim licima, bez obzira na to da li se osoba predstavlja kao zaposleni u banci, prodavac ili kao tehnička podrška. Banka ne poziva klijente telefonom i ne traži lične ili bezbednosne podatke.



SAVETI ZA LOZINKE



Postoji više načina za kreiranje jedinstvene i kompleksne lozinke. U nastavku teksta dati su osnovni saveti:



Koristite kompleksne i jedinstvene lozinke ili pristupne fraze. Preporučuje se da lozinka sadrži najmanje 12 karaktera i kombinaciju malih i velikih slova, brojeva i specijalnih znakova. Ne treba koristiti uobičajene reči, lične podatke, fraze ili pojmove iz privatnog života. Na ovaj način umanjujete rizik od neovlašćenog pristupa i dodatno unapređujete bezbednost svojih korisničkih naloga.



Ne koristite istu lozinku za različite korisničke naloge. Ne preporučuje se čuvanje lozinke u internet pregledačima, posebno kada je reč o nalogima za elektronsku poštu i pristup bankarskim računima. Za bezbedno kreiranje i čuvanje lozinke, preporučuje se korišćenje pouzdanih aplikacija kao što su menadžeri lozinke. Ako je teško zapamtiti lozinku, nemojte je zapisivati u izvornom obliku, već koristite podsetnik (*hint*) koji upućuje na pravu lozinku.



Ako aplikacija prilikom kreiranja korisničkog naloga zahteva unos sigurnosnih pitanja, savetuje se izbor onih na koja samo vi znate odgovor. Pitanja služe za ponovno postavljanje lozinke, ako je korisnik zaboravi. Treba izbegnuti pitanja čiji se odgovori mogu pronaći na internetu. Ako postoji mogućnost izbora, prednost treba dati dvofaktorskoj autentifikaciji, umesto sigurnosnih pitanja.



Lozinku je neophodno odmah promeniti ukoliko postoji sumnja da je korisnički nalog kompromitovan, nakon potvrđenog bezbednosnog incidenta, u slučaju otkrivanja ili curenja lozinke, kao i kada je ista lozinka korišćena na više različitih servisa. Radi dodatne zaštite korisničkog naloga, preporučuje se redovna izmena lozinke, najmanje jednom u tri meseca.



FIŠING PREVARE



Fišing (*phishing*) je vrsta prevare čiji je cilj prikupljanje i zloupotreba ličnih i finansijskih podataka, kao što su lozinke za društvene mreže i elektronsku poštu, brojevi platnih kartica, brojevi bankarskih računa, CVV/CVC kodovi platnih kartica, PIN brojevi. Napadači šalju poruke putem elektronske pošte, SMS poruka, aplikacija za razmenu poruka (*Viber, WhatsApp*), društvenih mreža. U porukama se od korisnika traže lični i finansijski podaci, koje napadači kasnije koriste za otvaranje novih ili pristup postojećim korisničkim nalogima. Uobičajeni oblici fišing napada uključuju:



Obaveštenja o navodnim sumnjivim aktivnostima ili pokušajima prijavljivanja na korisnički nalog.



Obaveštenja da postoji problem sa korisničkim nalogom ili platnom karticom uz zahtev da unesete lične ili finansijske podatke. Cilj ovakvih poruka je preuzimanje poverljivih ličnih podataka i podataka o platnoj kartici.



Slanje lažnih elektronskih ili SMS poruka građanima, koje izgledaju kao zvanična prepiska državnih organa. U porukama se navodi da je protiv primaoca pokrenuta istraga ili da postoji neizmirena obaveza.



Poruke u kojima se navodi da imate pravo na povraćaj novca od države ili se nude kuponi za besplatne proizvode.



Zahtev da pristupite linku i potvrdite lične podatke ili izvršite uplatu. Link najčešće vodi na lažnu internet stranicu koja izgleda kao legitimna, sa ciljem preuzimanja ličnih podataka, adrese elektronske pošte i lozinke, ili pokretanja zlonamernog softvera.



Slanje lažnih faktura ili dokumenata u prilogu elektronske pošte ili SMS poruke. Dokument poslat od nepoznatog pošiljaoca ne treba otvarati.



VAŽNO! Budite obazrivi prilikom prijema poziva, SMS ili elektronskih poruka od nepoznatih pošiljalaca koji traže potvrdu ličnih podataka. Ne pristupajte linkovima, ne preuzimajte priloge iz sumnjivih elektronskih poruka. Za internet plaćanja koristite posebnu karticu i ograničite iznos na sumu potrebnu za konkretnu kupovinu. Primenom veštačke inteligencije, fišing poruke mogu biti uverljive i personalizovane jer napadač koristi javno dostupne informacije sa društvenih mreža. Treba biti oprezan i kada poruka izgleda poznato ili je lično prilagođena.



Osnove informacione bezbednosti

www.cert.rs