CYBER BEZBEDNOST HIGIJENA

Predavač: dr Dušan Stefanović

SAJBER BEZBEDNOST

Sajber bezbednost je način na koji pojedinci i organizacije smanjuju rizik od sajber napada.

Tehnološke mere

Upotreba softverskih i hardverskih alata za zaštitu

Obuka zaposlenih

Edukacija o prepoznavanju i sprečavanju prevara

Politike upravljanja rizikom

Razvoj strategija za ublažavanje rizika

Protokoli reagovanja na incidente

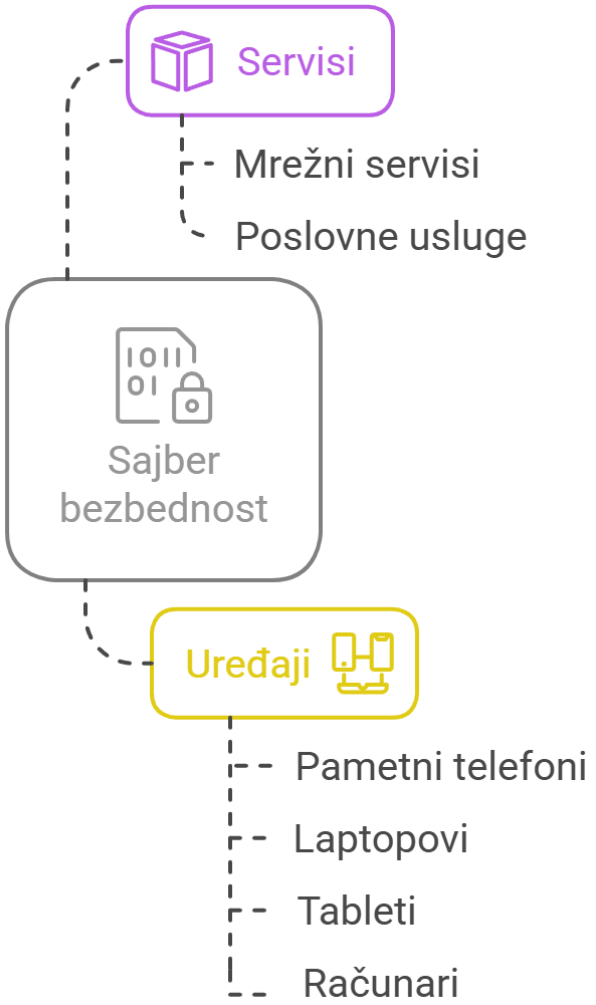
Planovi za odgovor na sajber napade

SAJBER BEZBEDNOST

Osnovni zadatak sajber bezbednosti je da zaštitite :

- Uređaje koje svi koristimo(pametni telefoni, laptopovi, tableti i računari)
- Servise (usluge) kojima pristupamo na mreži i na poslu

od krađe, oštećenja ili nedostupnosti usluge



TEHNIKE I ALATI ZA ODBRANU OD SAJBER NAPADA - OSNOVNA ZAŠTITA

Redovna Ažuriranja

Redovno instalirajte zakrpe i ažuriranja kako biste zatvorili poznate ranjivosti.

Instalirajte pouzdana rešenja za zaštitu od malvera i virusa.

Zaštita od Malvera

Korišćenje Firewalla

Koristite hardverske i softverske firewall programe za kontrolu saobraćaja.

TEHNIKE I ALATI ZA ODBRANU OD SAJBER NAPADA - NAPREDNE TEHNIKE ZAŠTITE

Šifrovanje podataka

Štiti osetljive podatke od neovlašćenog pristupa.

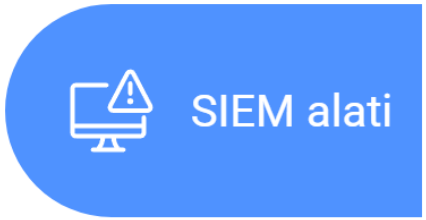
Dodaje dodatni sloj verifikacije identiteta.

Višefaktorska autentifikacija

Testiranje ranjivosti

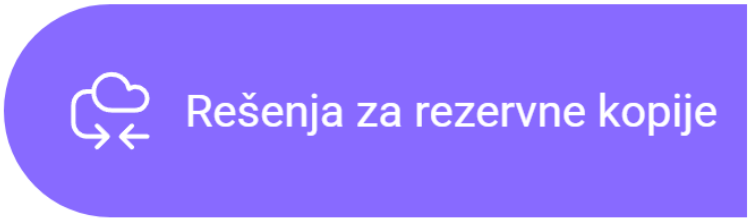
Identifikuje potencijalne rizike kroz audite i testove.

TEHNIKE I ALATI ZA ODBRANU OD SAJBER NAPADA - ALATI



Alati za praćenje i analizu sigurnosnih događaja u realnom vremenu.

Sigurna veza za udaljene radnike, štiteći podatke tokom prenosa.



Automatsko pravljenje rezervnih kopija podataka kako bi se omogućio oporavak u slučaju napada.

PHISHING (PECANJE)

- Organizovanje obuka kako bi zaposleni naučili da prepoznaju sumnjive e-mailove i linkove
- Korišćenje alata za filtriranje phishing poruka pre nego što stignu do korisnika
- Redovno simuliranje phishing napada kako bi se proverila svest zaposlenih

RANSOMWARE

- Pravljenje rezervnih kopija podataka na sigurnim lokacijama, van mreže
- Deljenje mreže na manje segmente kako bi se ograničilo širenje ransomware-a
- Razrada plana za brzi oporavak u slučaju napada (Disaster Recovery Procedure)

DDOS

- Angažovanje provajdera koji nudi zaštitu od distribuiraniih napada uskraćivanja usluge
- Postavljanje mrežnih uređaja tako da detektuju i blokiraju sumnjivi saobraćaj
- Kontinuirano praćenje i analiza mrežnog saobraćaja kako bi se otkrile anomalije

MIT ILI REALNOST

Složenost

Sajber bezbednost je previše složena za razumevanje

Sofisticiranost napada

Napadi su visoko sofisticirani i teški za zaustavljanje.

Ciljanje

Napadi su često visoko ciljani, što dovodi do verovanja da naša kompanija nije privlačna napadačima.

Jaka lozinka osigurava bezbednost podataka

Verovanje da jake lozinke same po sebi pružaju potpunu zaštitu podataka

Brisanje fajlova uklanja podatke trajno

Pretpostavka da brisanje fajlova trajno uklanja sve tragove podataka

Enkripcija nije potrebna

Ideja da enkripcija nije neophodna za zaštitu podataka

Sajber bezbednost je samo za IT

Gledište da je sajber bezbednost isključivo odgovornost IT sektora

NEW ZEALAND / MEDIA & TECHNOLOGY

Waikato DHB cyber attack: Medical files may have been taken

5:46 pm on 24 May 2021

Share this

Cyberattack Sees UniSA Systems Shut Down

BY ADMIN ON MAY 18, 2021

APP-ACSM, CYBER SECURITY, EDITOR'S DESK, FEATURED, GOVERNANCE, RISK & COMPLIANCE, HACKING & PENETRATION TESTING, INFORMATION SECURITY, VULNERABILITIES

A cyberattack at the University of South Australia is continuing to impact staff and students. The circumstances surrounding the attack remain unclear, but key systems are still offline two days after the University noticed the first outage.

"UniSA experienced a cyberattack on the weekend which caused an outage of its staff email system," a UniSA spokesperson told MySecurity Media. "The University is still investigating the issue."

NSW driver's licence data stolen in Accellion breach

By Justin Hendry
Feb 25 2022
6:30AM

Some customers, agency staff only now being notified.

Driver's licence details were among the personal information stolen from Transport for NSW in the Accellion data breach last year, *iTnews* can reveal.

Nine Network under attack by cyber hackers, threatening news services nationwide

By 9News Staff | 7:04am Mar 29, 2021

Tweet Facebook Mail

POLITICS

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

PUBLISHED TUE, JUN 8 2021.10:17 AM EDT | UPDATED WED, JUN 9 2021.8:24 AM EDT

JBS Foods pays $14m to ransomware attackers

By Ry Crozier
Jun 10 2021
11.23AM

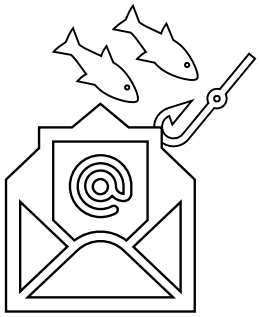
Says the decision to make payment was 'very difficult'.

JBS Foods, the meat processor whose Australian and US operations were hit by a ransomware attack earlier this month, paid "the equivalent of US$11 million" (A$14 million) to the group behind the attack.

The company made the payment despite the "vast majority of the company's facilities" already having been operationally recovered.

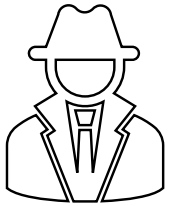
TRENUTNO STANJE
ŽRTVE CYBER SECURITY NAPADA

TRENUTNO STANJE



Phishing napad je i dalje napad broj 1

Ransomware napadi su u porastu



Social Engineering je vodeći napad za razne vrste prevara

VEKTORI NAPADA

Termin se odnosi na način ili put koji napadač koristi da bi izvršio napad na računarski sistem, mrežu ili aplikaciju.

Razlikuju se po vrsti napada i cilja a najdominatniji su:

VEKTORI NAPADA

Phishing

Napadači mogu koristiti phishing emailove ili poruke kako bi prevarili korisnike da otkriju svoje korisničko ime, lozinku ili druge osetljive informacije.

Ransomware

Ransomware je vrsta malicioznog softvera (malware-a) koji šifrira podatke na računaru ili mreži i zahteva otkup (ransom) od žrtve kako bi se dekriptovali podaci.

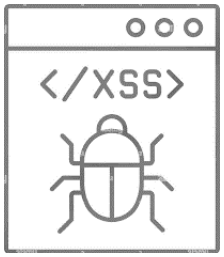
VEKTORI NAPADA

Brute Force

Napadači mogu koristiti brute force napad kako bi pokušali razbiti lozinke ili druge autentifikacione mehanizme pokušavanjem svih mogućih kombinacija sve dok ne pronađu ispravnu.

SQL Injection

Ovaj napad se koristi za ubacivanje zlonamernog SQL koda u SQL upite.
To može omogućiti napadaču da izvršava neovlašćene operacije na bazi podataka, kao što su izvlačenje, menjanje ili brisanje podataka.



Cross-Site Scripting

XSS napadi se koriste za ubacivanje zlonamernog koda u web stranice ili aplikacije koje se zatim izvršavaju na uređajima korisnika koji pristupaju tim stranicama.
To može omogućiti napadaču da ukrade sesije korisnika

SCAM WATCH IZVEŠTAJ ZA 2020

Otkrivanje prevara

Identifikacija i otkrivanje prevarantskih aktivnosti

Praćenje prevara

Praćenje prevara u realnom vremenu

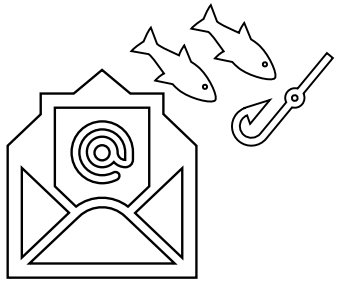
Sprečavanje prevara

Strategije za sprečavanje prevara

Obaveštavanje javnosti

Obaveštavanje javnosti o prevarama

PHISHING NAPADI

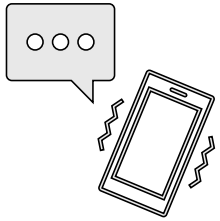


Phishing email

COVID 19 vakcine

Vishing (Voice Phishing)

Lažno predstavljanje da je potrebno da se očisti virus na vašem računaru



Smishing (SMS Phishing)

Lažna poruka da vam račun ne bi bio blokiran traži se da kliknete na link

Department of Health impersonation email

Australian Government
Department of Health

Dear Recipient,

My colleague have contacted you earlier but there was no response from you.

There were three COVID-19 confirmed cases in your area earlier this week and one of the patients has listed you as one of her physical contacts within the last 14 days.

In line with the contact tracing modalities and within the laws on which we operate at the Department of Health, we strongly advice that you submit yourself for COVID-19 testing.

The neccessary details of your appointment with the Department of Health are contained in the attached document.

Read through the guidelines properly and ensure that you submit yourself for testing as failure to do so will result in arrest and prosecution.

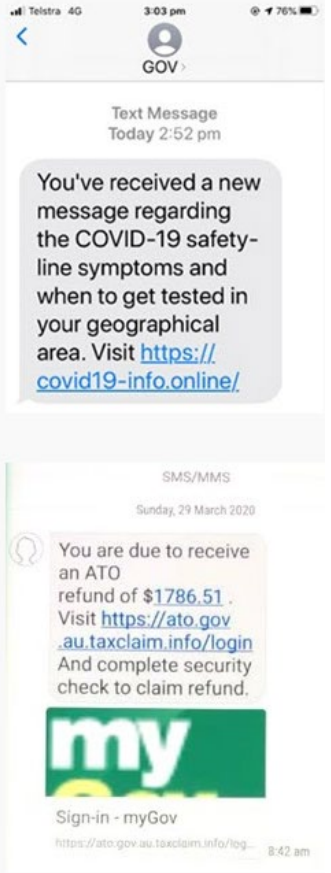
If you have any questions concerning this email, feel free to contact me anytime.

Regards.

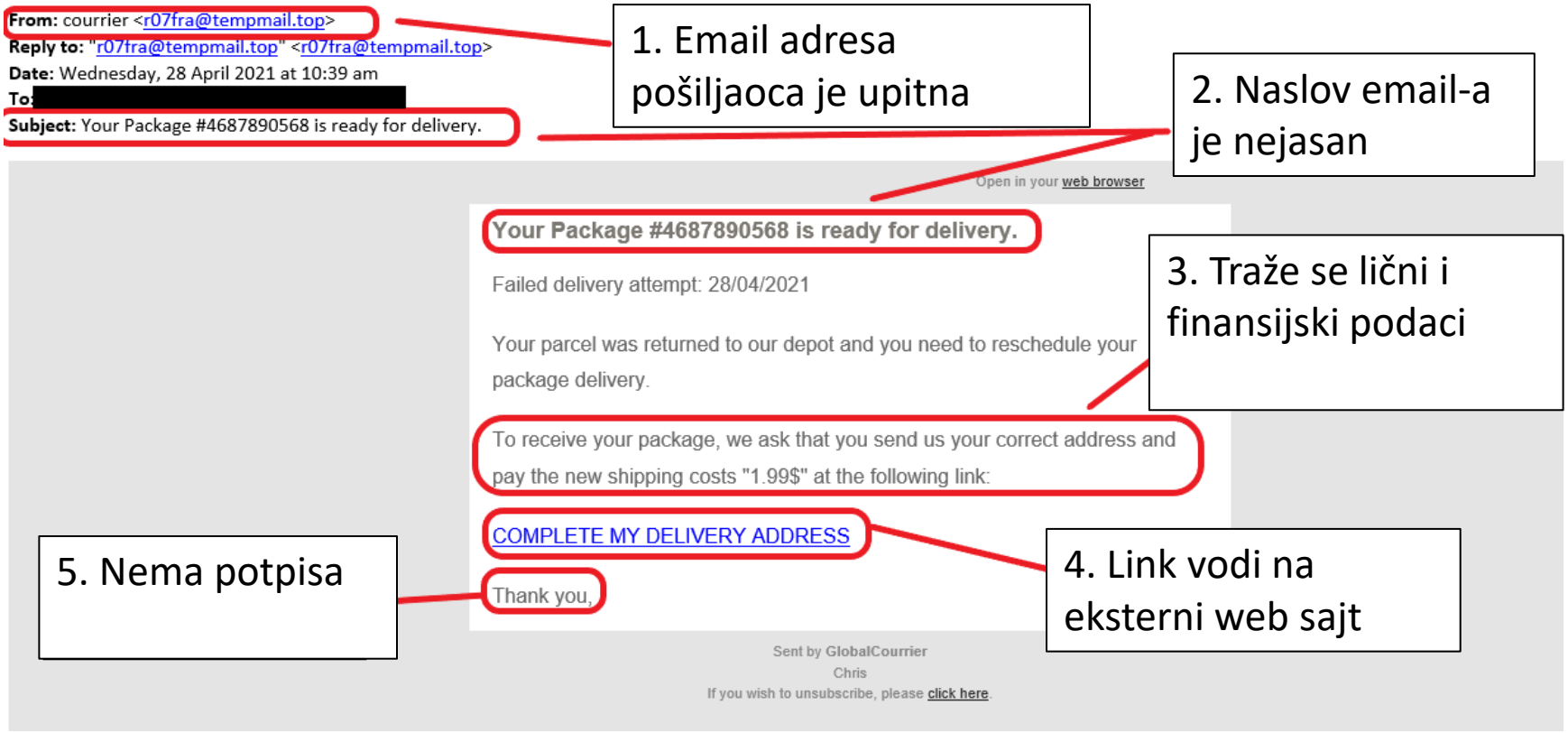
Greg Hunt MP

Department of Health
GPO Box 9848
Canberra ACT 2601
Australia

Fake myGov texts



PRIMER ZA PHISHING NAPAD



RANSOMWARE

Ransomware je vrsta malicioznog softvera (malware-a) koji šifrira podatke na računaru ili mreži i zahteva otkup (ransom) od žrtve kako bi se dešifrirali podaci.

Kako?

Email attachments

Website downloads

Email links

Website links

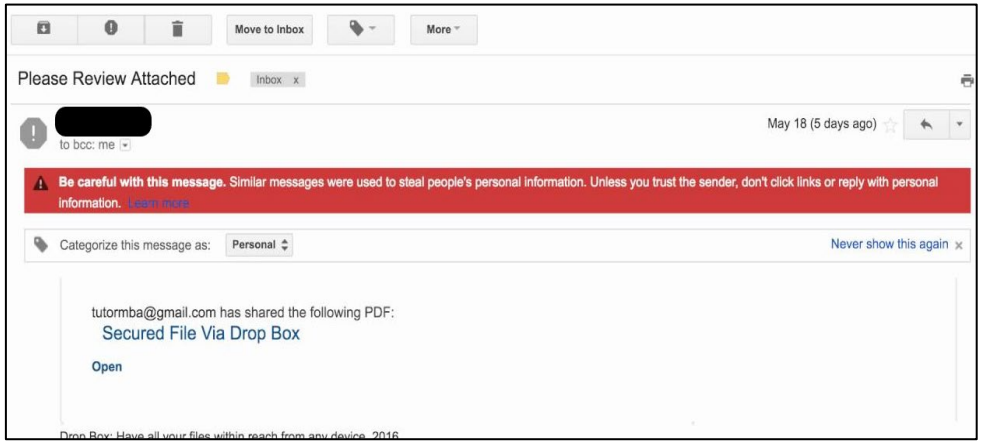
Zaštita

Redovni backup

Updates

Verifikacija email-ova

Ne PLAĆAJ!

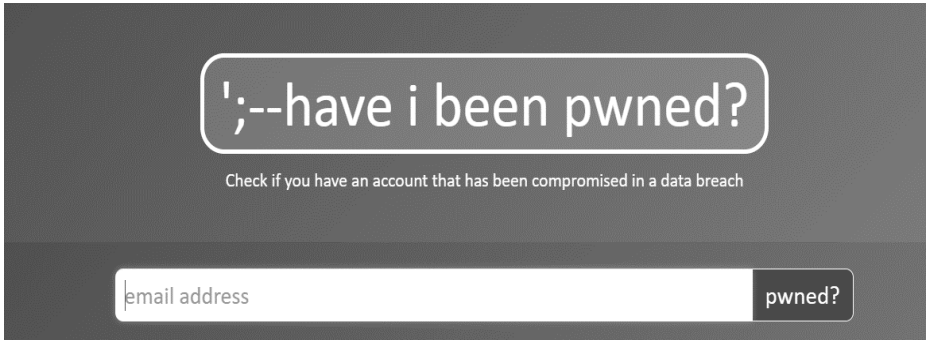


ZAŠTO JE SVEST O SAJBER BEZBEDNOSTI BITNA?

- Sve je UMREŽENO!
- Lični dokumenti
- Identitet
- Finansije
- Digitalni footprint (otisak)

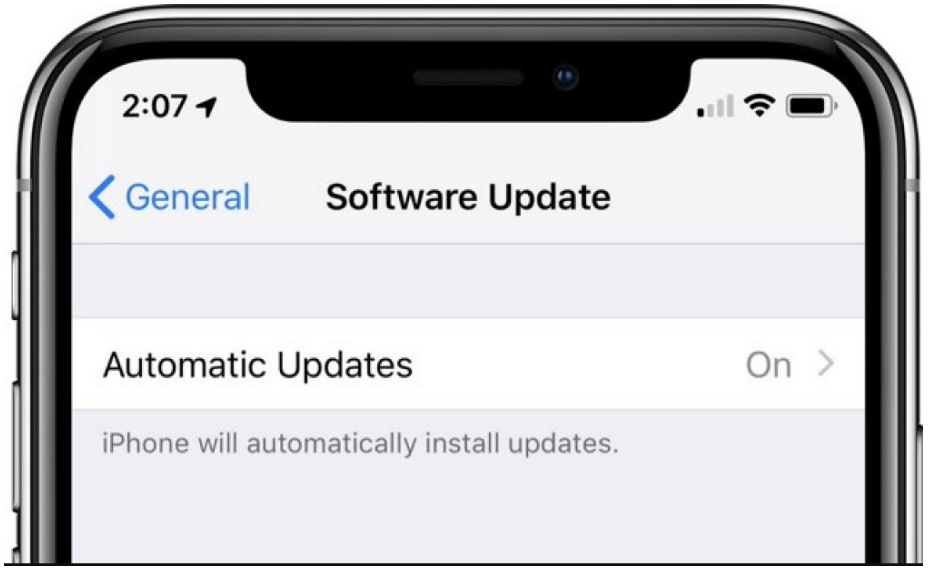
LOZINKE

- Duga i jaka.
- Omogućiti 2FA uvek kad je moguće
- Promena default lozinke
- Ne koristiti istu lozinku na različitim nalozima
- **Koristi Password manager (LastPass je Besplatan)**



UPDATES

Obezbediti da svi uređaji imaju najnoviji update → Uključiti AUTOMATIC UPDATES → Odvoji vreže za update → Redovno čistiti aplikacije



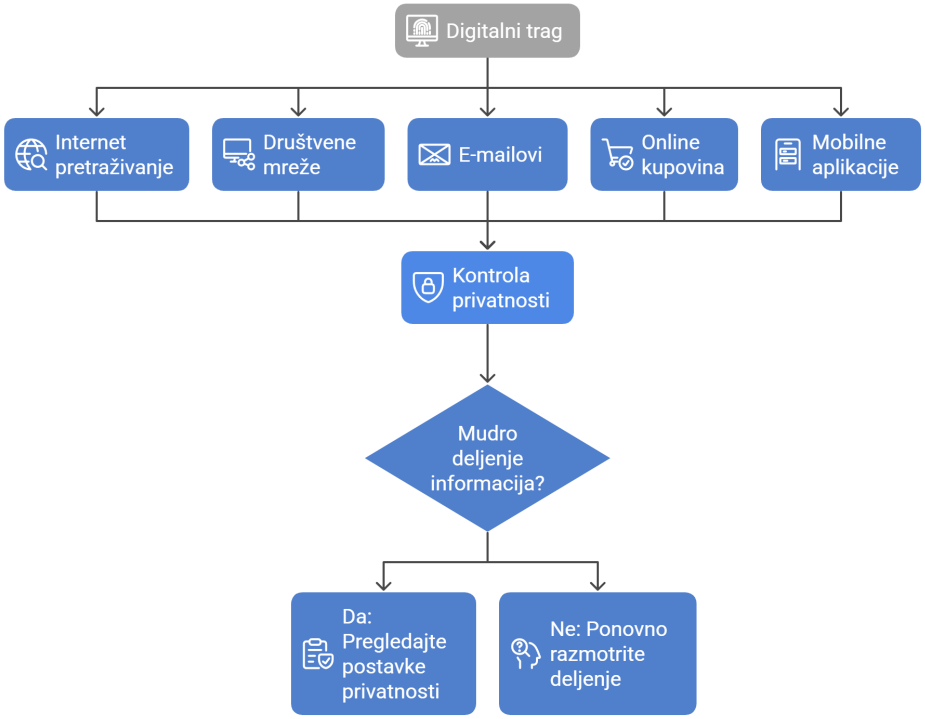
OPREZNOST OD PREVARA

1. Phishing - email
2. Vishing – telefonski pozivi
3. Smishing – SMS poruke

Obratiti pažnju na:

1. Hitnost
2. Traženje ličnih/finansijskih informacija
3. Sadrži link i (downloadable) fajl
4. Gramatičke greške
5. Isuviše dobro da bi bilo istinito

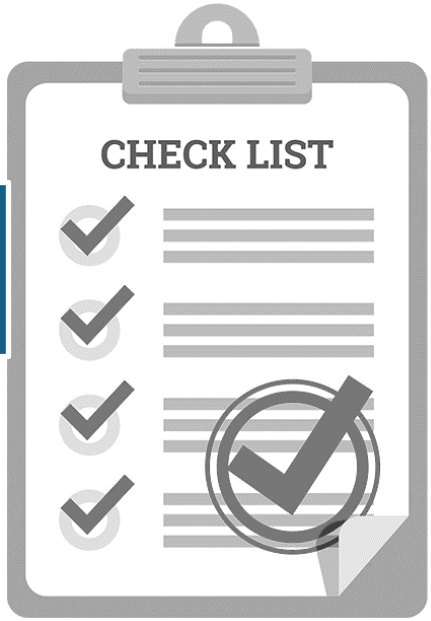
DIGITALNI TRAG



CYBER SECURITY CHECK LISTA

Da li su moji uređaji bezbedni? → Koristi *VPN* za pristup udaljenim resursima? → Budi oprezan korišćenjem *FREE Wi-Fi* → Da li je instaliran antivirus?

Da li imam back up bitnih podataka? *Cloud & Lokal* → Da li su uređaji up to date? → Omogući *two-factor* authentifikaciju *(2FA)* gde je moguće



STOP.

THINK BEFORE YOU CLICK.

SYBER BEZBEDNOST - ODGOVORNOST

Skoro sve organizacije zavise od digitalne tehnologije da bi funkcionisale.

Potencijalni trošak otklanjanja sajber incidenta može biti značajan.

Rizik od gubitka reputacije.

Sajber bezbednost je od suštinskog značaja i treba je shvatiti kao naizbežan faktor.