Cyber
Ready
Balkans

Cyber Ready Balkans

Vodič za mlade u sajber bezbjednost

Sadržaj

Mi smo tim Chevening stipendista za sajber bezbjednost iz cijelog Balkana. Stipendisti su profesionalci sa različitim pozadinama u oblasti sajber bezbjednosti – od etičkog hakovanja i digitalne forenzike, do upravljanja rizicima, upravljanja (governance) i sajber edukacije.

Ovaj projekat, Cyber Ready Balkans, finansiran je od strane Ministarstva vanjskih poslova, Komonvelta i razvoja Ujedinjenog Kraljevstva (FCDO) kroz Chevening Fellowship program. Nastao je iz zajedničke misije: da poveže region, smanji jaz između obrazovanja i prilika, te mladima približi svijet sajber bezbjednosti na jeziku koji razumiju.

Iz prve ruke smo vidjeli da mnogi studenti na Kosovu, u Sjevernoj Makedoniji i Crnoj Gori imaju talenat i radoznalost, ali nemaju dovoljno smjernica ili pristup da uđu u ovu oblast. Kroz ovaj projekat, cilj nam je da to promijenimo.

Sadržaj knjige

Šta je sajber bezbjednost

Kako steći obrazovanje u oblasti sajber bezbjednosti na Kosovu

Gdje raditi u oblasti sajber bezbjednosti na Kosovu

Šta je sajber bezbjednost

01: Zašto bi vas trebalo brinuti

Cilj poglavlja:

da vas natjera da shvatite da sajber bezbjednost nije samo za IT štrebere; ona se odnosi na vas, vaše živote i vašu budućnost. Ono je osmišljeno da vam pokaže da ste već dio sajber svijeta, bez obzira da li vam se to sviđa ili ne.

1. Poziv na buđenje

Počnimo sa pričom.

Arta je imala 12.000 pratilaca na Instagramu. Objavljivala

je fotografije, delila rilove, izgradila malu zajednicu. Jednog dana je kliknula na poruku u kojoj se nudi besplatan poklon objektiva za kameru. Izgledalo je legitimno. Za nekoliko minuta je bila odjavljena. Njena lozinka nije radila. Njen nalog je nestao. Neko ga je preuzeo, promenio imejl i počeo da prevara njene pratioce kripto šemama.

Nikakvo upozorenje. Nikakvog povratka.

2. “Ali ja nisam niko...”

To je ono što većina ljudi misli.

- “Nisam poznata.”
- “Nemam novac.”
- “Zašto bi me neko hakovao?”

Evo istine: njih nije briga ko ste vi.

Hakeri bacaju široke mreže. Žele pristup: vašem imejlu, vašem telefonu, vašim pratiocima, vašim fajlovima. Zašto?

- Vaši podaci = mogu biti prodati.
- Tvoj uređaj = može se koristiti za napade.
- Vaš nalog = može da prevari druge.
- Vaš identitet = može biti kopiran.

Niste nevidljivi. Povezani ste. I to je dovoljno.

3. Šta je zapravo u riziku?

Sajber bezbjednost zvuči apstraktno. Zato hajde da je učinimo stvarnom.

Bez nje možete izgubiti:

- Vaši razgovori, direktne poruke i fotografije
- Vaš novac i pristup bankarskim podacima
- Vašu reputaciju – kroz lažne postove ili procureli sadržaj
- Vašu budućnost - prijave za fakultet, prijave za posao, sve kompromitovano
- Vaše ideje - ukradene, kopirane ili izbrisane

Ovdje nije pitanje “da li”. Pitanje je “kada”.

4. To se već dešava u Crnoj Gori

Ovo nije samo holivudski problem.

Upravo Ovdje u Crnoj Gori:

- Studenti su prevareni lažnim Erazmus linkovima.
- Roditelji su kliknuli na malver u WhatsApp i Viber grupama.
- Vladini organi su bili pogođeni DDoS napadima i malverom.
- Prevare preko telefona i fišing imejlovi se svake godine sve više povećavaju.

Pitajte u svom okruženju. Neko koga poznajete je već bio pogođen.

5. Zamislite svoj digitalni život kao kuću

Pojednostavimo.

Zamislite svoj telefon ili laptop kao svoju kuću.
Vaše poruke = vaši privatni razgovori.
Vaše fotografije = vaša lična sećanja.
Vaši imejlovi = vaš posao i budućnost.

Sada zamislite da svaki dan ostavite ulazna vrata široko otvorena. Sa porukom na kojoj piše: “Slobodno uzmite.”

Zvuči ludo? Tako većina ljudi živi na internetu. Slabe lozinke. Klikanje na nasumične linkove. Nemaju pojma šta se dešava u pozadini.

Sajber bezbjednost je upravo ovo: zatvaranje vrata. Njihovo zaključavanje. Postavljanje alarma.

6. Ovo nije samo za danas. To je vaša budućnost.

Vi niste danas samo na internetu.

Učiti ćete, raditi, zabavljati se, obavljati bankarske poslove, kupovati, glasati, a možda čak i voditi posao preko interneta.

Sve je povezano. I to znači:

- Propust može naštetiti vašoj reputaciji.
- Prevara može isprazniti vaš račun.
- Hakovani telefon može uništiti vaš intervju za posao pre nego što uopšte počne.

Digitalno vi ste podjednako stvarni kao i fizičko vi.
Ako ga ne zaštitite, neko drugi može da ga kontroliše.

7. Sajber bezbjednost = Kontrola, Moć, Sloboda

Zaboravite predstavu o sajber bezbjednosti kao dosadnu, tehničku ili samo za "hakere".

Evo šta to zapravo jeste:

- Kontrola - Vi odlučujete ko vidi vaše stvari.
- Moć - Ne dozvoljavate da vas prevare. Razumijete kako stvari funkcionišu.
- Sloboda - Možete bezbjedno da se krećete kroz digitalni svijet.

Učenje sajber bezbjednosti nije samo pametno, već i osnažuje. Čini vas oštrijim, bržim i svesnijim.

To je veština koja vas štiti, pomaže drugima i otvara vam vrata karijere svuda.

8. Da li ste u riziku? (Brza samoprovera)

Odgovorite iskreno:

- Da li svuda koristite istu lozinku?
- Da li ste ikada kliknuli na čudan link sa Instagrama ili Vibera?
- Da li koristite javni Wi-Fi bez VPN-a?
- Da li znate da li je vaša e-pošta ikada procurila?

Ako ste na bilo koje od ovih odgovorili "da"... Već ste izloženi.

Ali ne brinite. Ovaj vodič je Ovdje da to promeni.

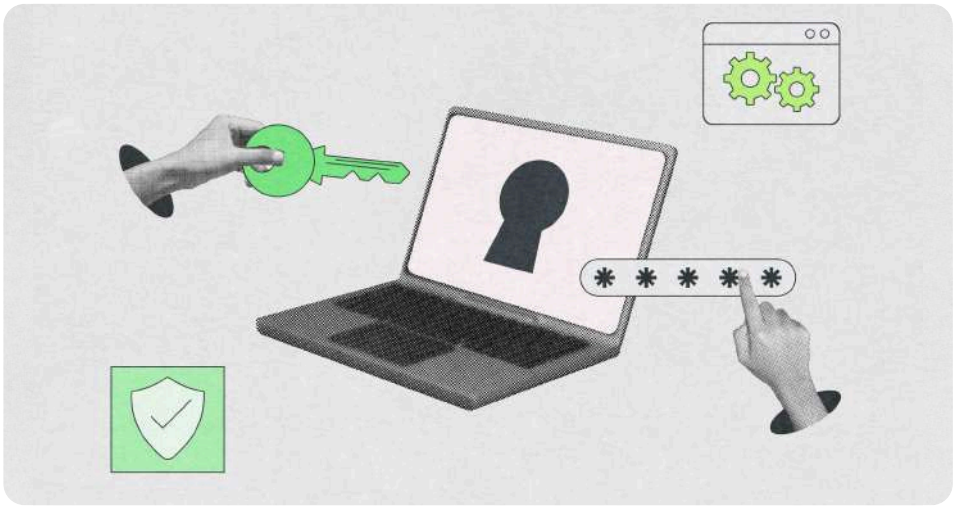
Završna riječ

Ne morate da se plašite. Morate biti svesni.

Ovo je početak učenja kako da se zaštitite, a možda jednog dana i zaštitite druge.

Hajde da krenemo.

POGLAVLjE 2: Šta je sajber bezbjednost



Šta je sajber bezbjednost

Radi se o tome da vaš digitalni život bude bezbjedan, iznutra prema spolja.

1. Sajber bezbjednost u jednoj riječenici

Sajber bezbjednost znači **zaštitu računara, mreža, uređaja i podataka od krađe, oštećenja ili zloupotrebe.**

Tako je jednostavno.

2. Šta treba zaštititi?

Šta treba zaštititi?

- Vaš telefon
- Vaš laptop
- Vaši nalozi
- Vaše fotografije, fajlovi i poruke
- Školski sistemi, bankarski serveri, čak i infrastruktura za vodu i energiju

Ako je povezano na internet, može biti napadnuto. Ako može biti napadnuto, potrebno mu je obezbeđenje.

3. Triagolnik sajber bezbjednosti (CIA trijada)

Ovo je ABV sajber bezbjednosti, koristi se svuda u svijetu.

- C - Povjerenje

  Čuvajte ga privatnim. Samo ovlašćene osobe treba da imaju pristup.
  Primjer: Vaše poruke ne bi trebalo da vide stranci.

- I - Integritet

  Čuvajte tačnost. Bez neovlašćenih izmijena.
  Primjer: Ne bi trebalo da ih menja neko drugi.

- A - Dostupnost

  Obezbjedite mu pristupnost. Trebalo bi da ga možete koristiti kada vam zatreba.

  Primjer: Vaše onlajn bankarstvo treba da radi kada se prijavite.

Sajber bezbjednost se svodi na **uravnoteženje ova tri.**

4. Šta sajber bezbjednost nije

Rasčistimo neke nedoumice.

To nije samo “hakovanje sistema”.

Ne radi se o sedenju u mračnoj sobi i kucanju koda kao u filmovima.

Nije samo za genije ili IT stručnjake.

Da, etičko hakovanje je dio toga. Ali tu su i:

- Analiza rizika
- Pisanje politika
- Obuka o bezbjednosnoj svijesti
- Istrage
- Dizajn sistema

Sajber bezbjednost je timski sport.

5. Ko radi u oblasti sajber bezbjednosti?

Postoji mnogo različitih uloga:

- **SOC analitičar** - Prati prijetnje 24/7
- **Penetracioni tester** - pokušava da hakuje sisteme (legalno!)
- **Responder za incidente** - Uskače kada nešto pođe po zlu
- **Inženjer bezbjednosti** - gradi bezbjedne sisteme
- **CISO (glavni službenik za informacionu bezbjednost)** - postavlja strategiju u širokim crtama
- **Forenzički stručnjak** - Istražuje ko je šta uradio

Neki ljudi pišu kod.
Neki ljudi pišu izveštaje.
Neki ljudi obučavaju druge.

Postoji uloga za svaki tip mozga.

6. Već se bavite sajber bezbjednošću (u nekom smislu)

Ako ste ikada:

- Postavili jaku lozinku
- Koristili dvofaktorsku autentifikaciju (2FA)
- Prijavili sumnjivu poruku
- Ignorisali sumnjiv link

...čestitamo. Već ste počeli. Sada je vreme da zaronite dublje.

7. Zašto je to važno (više nego ikad)

- Što više živimo onlajn, to nam je potrebnija zaštita.
- Kompanije, bolnice, škole, pa čak i vlade ne mogu da funkcionišu bez sajber bezbjednosti.
- Napadi nisu rijetki. Dešavaju se svaki dan.

Sajber bezbjednost više nije niša. To je neophodnost.

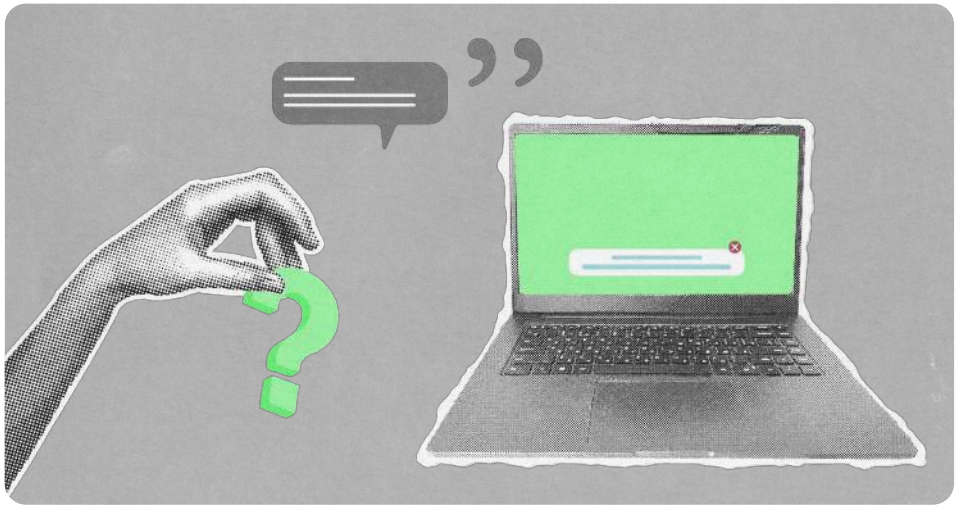
Sažetak

Sajber bezbjednost se odnosi na **zaštitu ljudi i sistema u digitalnom svijetu.**

To nije jedna stvar, već univerzum veština i uloga.

I ne morate biti stručnjak da biste započeli.
Samo treba da budete znatiželjni i oprezni.

POGLAVLjE 3: Ko su dobri i loši momci



U svijetu sajber bezbjednosti, nijesu svi hakeri opasni.

Neki te štite. Neki ti kradu. A neki žive u sivom polju.

1. Hajde da pričamo o hakerima

Kažite riječ “haker” i većina ljudi zamisli ovo:

> Mladić u dukserici, kuca kao lud u mračnom podrumu, a zeleni kod leti po ekranu.

Pa... ne.

To je Holivud. Evo stvarnosti:

> Hakeri su svi koji razumeju kako sistemi funkcionišu i kako ih probiti ili poboljšati.

Postoje dobri hakeri. Loši hakeri. I oni koji su pomalo i jedno i drugo.

2. Sistem šešira

Hakere delimo po “boji šešira” da bismo pokazali njihovu nameru:

- Crne kape: Zli momci

  Upadaju u sisteme bez dozvole.

  Oni kradu, uništavaju, špijuniraju, prevare ili drže podatke za otkup.

Zašto hakuju:

- Para (krađa kreditnih kartica, prodaja podataka)
- Ego (“Uradio sam to zato što sam mogao.”)
- Osvijeta ili haos
- Vladine misije (tzv. državno sponzorisani hakeri)

Primjer:

- Bande sa ranomsomverom zaključavaju sisteme bolnica dok ne budu plaćene.

- Tinejdžer haker prodaje podatke za prijavljivanje na Instagram.
- Strana vlada špijunira izbore u drugoj zemlji.

- Bijele šešire: Dobri momci

  To su profesionalci za sajber bezbjednost koji pomažu organizacijama da ostanu bezbjedne.

  Testiraju sisteme uz dozvolu, otklanjaju probleme, obučavaju korisnike i spriječavaju napade.

Šta rade:

- Pronađite ranjivosti pre nego što ih zlikovci otkriju
- Reaguju na sajber incidente
- Izgraditi sigurne mreže
- Obučavaju timove i podižu svest

Oni su digitalni telohranitelji.

- Sivi šeširi - Nejasna sredina

  Oni hakuju bez dozvole, ali ne da bi nekome naštetili.

  Ponekad to rade "za veće dobro". Ali i dalje je rizično.

Primjer:

- Neko pronađe propust na vladinoj veb-stranici, ne traži dozvolu, ali ga ipak prijavi.
- Mogu da prekrše pravilo, ali ne sa lošim namerama.

Ipak... namera ne briše posledice. Sivi šeširi hodaju opasnom linijom.

3. Kriminalni tipovi

Hajde da razložimo uobičajene crne šešire na koje možete naići (ili o kojima čujete):

- Skript kids
  - Koriste alate koje u potpunosti ne razumeju
  - Preuzimaju stvari sa interneta i “isprobavaju” ih na slučajnim metama
  - Više dosadni nego opasni, sve dok ne uzmu sreće
- Organizovani kriminal
  - Seriozni hakeri za angažman
  - Rade kao preduzeća
  - Koriste ransomware, kradu podatke i povlače novac preko kriptovaluta
- Haktivisti
  - Miješavina riječi “haker” i ”aktivista”
  - Prodiru u sisteme da bi protestovali ili širili političku poruku
  - Primjer: oskrnavljenje veb-sajtova ili curenje dokumenata
- Državni akteri

  - Rade za vlade
  - Ciljaju druge zemlje, kompanije ili političke grupe
  - Visoko obučeni, dobro finansirani i opasno ozbiljni

4. Sajber dobri momci (uloge bijelih šešira)

U stvarnom svijetu, Bijele kape rade kao:

- **Proveravači propustljivosti (pentesteri)** - plaćeni da uđu pre nego što to učine loši momci.
- **Analitičari SOK-a** - Prate sisteme 24/7 zbog sumnjivih aktivnosti.
- **Reagovanje na incidente** - vatrogasci sajber svijeta.
- **Forenzički stručnjaci -** prate ko, šta, kada i kako napada.
- **Inženjeri bezbjednosti** - grade odbrane poput zaštitnih zidova, sistema za detekciju i bezbednih mreža.

Oni su ti koji održavaju svijetla upaljena - i vašu podatke bezbednim.

5. Zašto nije samo “ispravno protiv pogrešno”

Ponekad stvari postanu zbrkane.

- Tinejdžer hakuje sistem svoje škole iz znatiželje. Da li je on crni šešir? Ili samo zalutao?

- Uzbunjivač otkriva državno nadgledanje. Heroj za neke, kriminalac za druge.

Sajber bezbjednost nije uvijek crno-bela. Ali vaši izbori su važni. Namera je važna. Dozvola je važna, kako i vladavina prava.

6. Dakle... Kakvom hakeru želiš da budeš?

Ako ste znatiželjni... dobro. Ako volite zagonetke... odlično. Ako želite da gradite, branite i štitete, dobrodošli na put Bijele kape. Svijetu su potrebni etički hakeri. Nisu pobunjenici bez razloga, već ratnici sa svrhom.

Sažetak

Hakeri nisu samo jedna stvar. To su ljudi sa veštinama koje se koriste za dobro, zlo ili nešto između. Što više Razumijete kako hakeri razmišljaju, to bolje možete da se odbranite... ili da se pridružite odbrani.

Sledeće: Istražićemo kako se sajber-napadi zapravo dešavaju, korak po korak.
Spojler: često počinje jednim klikom.

POGLAVLjE 4: Kako se sajber-napadi zapravo dešavaju

Hakeri ne upadaju kao u filmovima.

Oni planiraju. Oni čekaju. Oni vas varaju.
Hajde da razložimo kako napad zapravo funkcioniše.

1. Dovoljan je samo jedan klik

Većina sajber-napada ne počinje sa složenim kodom.
Oni počinju sa vama.

Kliknete na link.
Otvarate fajl.
Verujete pogrešnoj stvari.

Istina? Hakeri ne “hakuju unutra.” Oni se “prijavljuju”, jer im je neko dao pristup.

Pogledajmo kako se to dešava.

2. Sajber lanac ubijanja (pojednostavljeno)

Evo korak-po-korak strategije koju većina napadača sledi. Zamislite to kao priručnik sa taktikama. To se zove Cyber Kill Chain – i ne, nije iz Call of Duty.

Korak 1: izviđanje

Saznajte sve o cilju.

- Guglaju te
- Pratite svoje društvene mreže
- Provjerite koji softver vaša škola ili kompanija koristi
- Skenirajte svoju veb-stranicu
- Potražite svoju adresu elektronske pošte ili broj telefona

Zašto? Da bi mogli da isplaniraju savršenu prevaru.

Korak 2: Oruđizacija

Izgradite napad na osnovu onoga što su pronašli.

- Kreirajte lažnu veb-stranicu (izgleda baš kao prijava na vašu banku ili školu)
- Napravite PDF sa skrivenim malverom

- Napišite imejl koji zvuči kao da je od vašeg šefa, profesora ili kompanije

Zašto? Da bi zamka izgledala bezbjedno.

Korak 3: Dostava

Pošaljite zamku.

- E-pošta
- Privatne poruke na društvenim mrežama
- Aplikacije za razmenu poruka
- Zlonamerni oglasi ili linkovi za preuzimanje

Zašto? Da biste interagirali. To je ključ.

Korak 4: Eksploatacija

Otvorite fajl ili kliknete na link.

Sada:

- Malver radi tiho
- Vaš uređaj počinje da šalje informacije napadaču
- Slećete na lažnu stranicu i unosite svoju stvarnu lozinku

Zašto? Da bi preuzeo kontrolu, a da vi to ni ne primetite.

Korak 5: Instalacija

Postavljena su zadnja vrata.

- Malver se trajno instalira

- Napadači sada imaju tajni ulaz
- Možda ćete i dalje koristiti uređaj kao i obično… ali oni su unutra

Zašto? Da bi ostali unutra neprimećeni.

◆ Korak 6: Komanda i kontrola

Napadač izdaje uputstva na daljinu.

Mogu:

- Preuzmite još malvera
- Koristite svoj uređaj da napadnete druge
- Krađu lozinki, fajlova ili kreditnih kartica

Zašto? Vaš uređaj postaje alat.

◆ Korak 7: Akcije na ciljevima

Vreme je da završite misiju.

- Zaštitite svoje datoteke i zatražite otkup
- Ukradi novac ili podatke
- Špijunirajte svoju aktivnost
- Izbrišite sisteme ili ih oštetite

Zašto? To je cilj. Sve ostalo je bilo priprema.

3. Primjer iz stvarnog svijeta (pojednostavljen)

Recimo da dobijete ovaj imejl:

> "Hej! Ovdje je administrator vaše škole. Dostupno je bezbjednosno ažuriranje za vaš nalog.
> Molimo vas da se prijavite Ovdje: school-portal-login.site"

Izgleda ispravno. Kliknete. Unesete svoje korisničko ime. Bum. Ušao si. Ali… I napadač takođe.

Sada oni:

- Prijavite se kao vi
- Promeni lozinku
- Preuzmite privatne fajlove
- Pošaljite fišing imejlove svojim školskim drugovima koristeći vaše ime

I baš tako, **jednim klikom došlo je do propusta.**

4. Bonus trik: Pivotiranje

Kada hakeri uđu u jedan sistem, traže načine da se još više uvuku. Ovo se zove **pivotiranje.**

> Hakuju tvoju e-poštu → Onda je koriste da pristupe tvom cloud disku
> Upadnu na server jedne škole → Zatim preskoče u sistem za ocenjivanje
> Hakuju jednog zaposlenog → Onda dosežu celu kompaniju

Sajber-napadi rastu kao virusi. Zato je rano otkrivanje ključno.

5. Oni žele da im to bude lako

Većina napadača ne želi izazov.

Većina napadača ne želi izazov.

- Slabe lozinke
- Stari softver sa poznatim propustima
- Ljudi koji klikaju bez razmišljanja
- Sistemi bez dvostepene autentifikacije

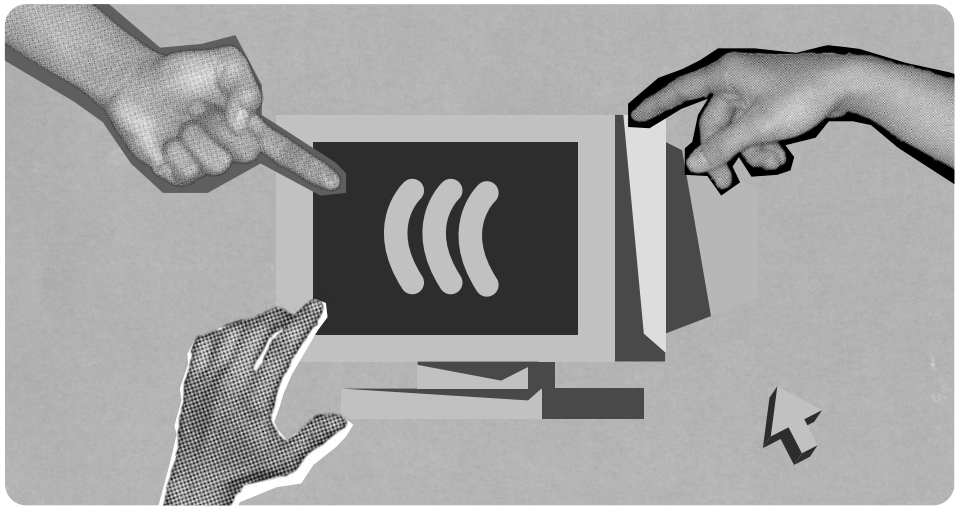
Oni žele malo truda, veliku nagradu. Nemojte im to dati.

Sažetak: Kako se događaju napadi

1. Oni vas **prate.**
2. Oni vas **varaju.**
3. **Ulaze**.
4. **Oni ćute.**
5. Oni **kradu, hakuju ili špijuniraju.**

Sajber napadi nisu magija. Oni su pametni, lukavi i strpljivi.

POGLAVLjE 5: Vrste sajber pretnji (koje ćete zaista videti)?



Zaboravite holivudske hakove.

Hajde da pričamo o stvarima koje zaista pogađaju vas: vaš telefon, vaše naloge, vaše prijatelje.

1. Fišing: Zamka lažne poruke

Šta je to: Lažni imejl, direktna poruka ili poruka koja pokušava da vas prevari da kliknete na zlonamerni link, preuzmete malver ili otkrijete informacije.

Kako izgleda:

- “Vaš paket je kašnje. Kliknite Ovdje da ga pratite.”
- “Vaš školski nalog će biti suspendovan. Prijavite se sada.”
- “Dobili ste besplatan iPhone!”

Zašto to funkcioniše:

- Izgleda hitno.
- Izgleda legitimno.
- Kliknete bez razmišljanja.

Kako ga prepoznati:

- Provjerite adresu pošiljaoca – da li izgleda čudno?
- Pređite mišem preko linka - vodi li na pravu stranicu?
- Loša gramatika ili neočekivan pritisak = crveni alarm.

Pravilo: Ne kliknite na linkove i ne preuzimajte datoteke osim ako niste 100% sigurni.

2. Malver: Tihi upadnik

Šta je to: Zlonamerni softver koji zaražava vaš uređaj.

Tipovi na koje možete naići:

- **Špijunski softver:** Prati vas, snima šta kucate.
- **Keyloggeri:** Hvataju vaše lozinke i poruke.

- **Trojanci:** izgledaju kao obična datoteka - ali otvaraju vrata hakerima.
- **Otkupni softver (ransomware):** zaključava vaše datoteke i traži uplatu da bi ih otključao.

Kako ulazi:

- Klikom na sumnjive linkove
- Preuzimanje piratskih igara, filmova ili hakovanog softvera
- Priključivanje slučajnog USB stika

Pravilo: Ako je besplatno, ali sumnjivo... verovatno je zamka.

3. Napadi na lozinku: Vaša najslabija karika

Šta je to: Hakeri pokušavaju da pogode, ukradu ili probiju vašu lozinku.

Uobičajene metode:

- **Brutfors:** Probaju hiljade kombinacija dok ne uđu.
- **Popunjavanje akreditiva:** Korišćenje lozinki procurelih sa drugih sajtova koje ste koristili.
- **Fišing:** Obmanom vas natjeraju da unesete lozinku na lažnu stranicu.

Znaci da ste pogođeni:

- Odjavljeni ste i ne možete da se vratite.

- Dobijate imejlove za resetovanje lozinke koje niste zatražili.
- Vaši prijatelji dobijaju čudne poruke od vas.

Pravilo:

- Koristite jake, jedinstvene lozinke.
- Uključite 2FA (dvofaktorsku autentifikaciju).
- Nikada ne ponovo koristite lozinke.

4. Socijalni inženjering: Hakuju vas, a ne računar

Šta je to: Psihološki trikovi koji vas navode da otkrijete informacije ili omoguće pristup.

Kako se to dešava:

- "Hej, ja sam IT administrator tvoje škole – možeš li mi brzo poslati svoje akreditive?"
- "Ja sam prijatelj tvog rođaka, treba mi tvoja pomoć sa nečim hitnim."

Radi zato što:

- Želimo da pomognemo.
- Ne želimo da izgledamo grubo.
- Pretpostavljamo da su ljudi oni za koje se predstavljaju.

Pravilo: Uvijek dvaput Provjerite identitete. Budite

ljubazni, ali skeptični.

5. Javni Wi-Fi napadi: Zamka besplatnog interneta

Šta je to: Otvoreni Wi-Fi u kafićima, školama, aerodromima može biti lažni ili nesiguran.

Šta se može dogoditi:

- Hakeri mogu da prate šta radite.
- Mogu da presretnu lozinke, poruke, pa čak i podatke o plaćanju.
- Mogu da se predstavljaju kao Wi-Fi mreža za koju mislite da je bezbedna.

Pravilo:

- Izbegavajte unošenje lozinki ili bankarskih podataka na javnom Wi-Fi.
- Koristite VPN ako morate da se povežete.
- Pitajte: "Da li je ovo zvanična mreža?"

6. Preuzimanje naloga: Kada izgubite kontrolu

Šta je to: Neko preuzme kontrolu nad vašim imejlom, Instagramom, Snepčatom ili bankovnim računom.

Kako to rade:

- Phishing
- Weak passwords

- Fišing
- Slabe lozinke
- Ponovo korišćene lozinke iz prethodnih propusta
- Sim-svoping (preuzimaju vaš broj telefona)

Zašto je opasno:

- Mogu da prevare vaše pratioce.
- Procurenje vaših privatnih poruka.
- Zaključavaju vas izvan sopstvenog života.

Pravilo:

- Koristite 2FA.
- Pratite prijave.
- Postupite brzo ako vam nešto deluje čudno.

7. Lažne aplikacije, preuzimanja i alati: Trojanski konj

Šta je to: Aplikacije koje se predstavljaju kao korisne, ali su tajno zlonamerne.

Uobičajene zamke:

- "Preuzmite ovu aplikaciju da biste videli ko je pregledao vaš profil!"
- Krekovane verzije igara ili alata za uređivanje
- Lažni antivirusni ili "čistači" aplikacije

Mogu:

- Kradu podatke
- Špijuniraju vas
- Zaštitite svoj uređaj

Pravilo: Preuzimajte samo iz zvaničnih prodavnica aplikacija. Provjerite recenzije. Izbegavajte sumnjive veb-sajtove.

8. Dezinformacije: Laži koje se šire kao vatra

Šta je to: Lažni ili obmanjujući sadržaj namenjen da vas prevari, razdvoji ili manipuliše vama.

Zašto je to važno u sajber bezbjednosti:

- Hakeri koriste lažne vesti da bi izazvali haos.
- Dezinformacione kampanje ciljaju izbore, proteste ili određene grupe.
- Možete nesvesno pomoći u njenom širenju.

Kako ga prepoznati:

- Provjerite izvor.
- Provjerite kod drugog (pouzdanog) izvora.
- Budite oprezni sa emotivnim naslovima ili virusnim objavama.

Pravilo: Ne budite zrtva. Razmislite pre nego što podelite.

Sažetak: Prijetnje koje ćete zaista videti

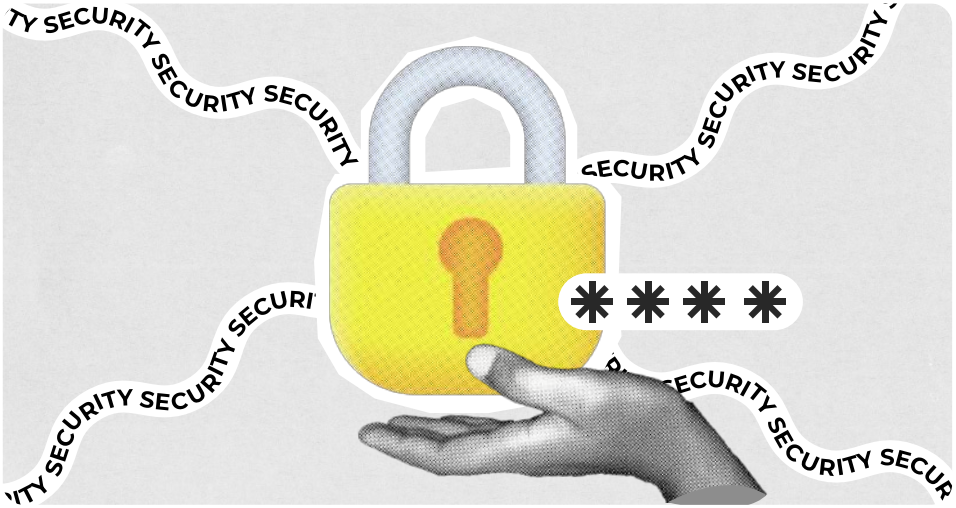
Nećete videti lasere ili eksplozije. Videćete:

- Lažna stranica za prijavu
- Sumnjiv imejl
- “besplatnu” aplikaciju
- Poruka koja deluje… čudno

Ali sada ćete znati na šta treba da obratite pažnju.

Sledeće:
Pogledaćemo šire i pokazati Gdje se sajber bezbjednost zapravo dešava: u vašem domu, vašoj školi, vašoj zemlji. To nije samo vaš telefon, već je svuda.

POGLAVLjE 6: Gdje se dešava sajber bezbjednost



Sajber bezbjednost nije samo na vašem ekranu.

Ona je u vašoj školi, vašem gradu, vašoj zemlji. Ona je iza kulisa svega na šta se oslanjate.

1. Veće je nego što mislite

Kada ljudi čuju “sajber bezbjednost”, oni misle:

- Hakeri
- Telefoni
- Lozinke

Ali je mnogo veće.

Sajber bezbjednost je nevidljiv štit koji štiti čitave sisteme:

- Škole
- Bolnice
- Banke
- Aerodromi
- Vlade
- Čak i elektrane i vodovodni sistemi

2. U kući: Vaša lična sajber zona

Vaš dom je digitalno bojište, bez obzira da li to primećujete ili ne.

Uređaji u riziku:

- Telefoni
- Laptopovi
- Pametni televizori
- Wi-Fi ruteri
- Pametni zvučnici (kao što su Alexa ili Google Home)

Uobičajene prijetnje:

- Slabe Wi-Fi lozinke
- Lažne aplikacije
- Fišing poruke

- Malver iz piratskih preuzimanja

Dobre navike = dobra odbrana.
Kada je vaš dom bezbjedan, teže je da postanete meta.

Savet: Promenite lozinku za Wi-Fi. Koristite jedinstvene lozinke za sve uređaje. Držite softver ažuriranim.

3. U školi: Igralište hakera

Škole koriste puno tehnologije:

- E-poruke
- Sistemi za onlajn ocenjivanje
- Učenički dosijei
- Platforme za učenje (Google Classroom, Moodle)

Zašto su škole na nišanu:

- Lako pristupanje
- Ogromne količine ličnih podataka
- Ograničena IT bezbjednost na mnogim mestima

Šta može poći po zlu:

- Promenjene ocene
- Ispiti procurili
- Privatni podaci ukradeni

Savet: Ne delite svoje akreditive za prijavu sa prijateljima. Prijavite sve sumnjivo IT timu svoje škole.

4. Na poslu: čak i poslovi s kraćim radnim vremenom

Ako radite u kafiću, banci, teretani ili bilo Gdje Gdje se obrađuju:

- Kreditne kartice
- Informacije o kupcima
- Unutrašnji sistemi

...sada ste u sajber igri.

Šta hakeri žele:

- Baze podataka o kupcima
- Pristup čitačem kartica
- Prijave zaposlenih

Mala preduzeća = velika meta.
Zašto? Češće ih je lakše hakovati.

Savet: Pazite šta otvarate na radnim uređajima. Nikada ne otvarajte lični imejl ili sumnjive veb-sajtove na njima.

5. U javnosti: Zamka besplatnog Wi-Fi-ja

Svako mjesto koje nudi besplatan Wi-Fi predstavlja potencijalnu zonu rizika. Zamislite:

- Kafići
- Aerodromi

- Biblioteke
- Biblioteke
- Tržni centri

Šta se može dogoditi:

- Hakeri špijuniraju vaš saobraćaj
- Lažne Wi-Fi mreže vas prevare da se povežete
- Mogu da ukradu vaše podatke za prijavu u realnom vremenu

Savet: Izbegavajte prijavljivanje na osetljive naloge na javnom Wi-Fi. Koristite VPN ako morate da se povežete.

6. U bolnicama: Sajber-napadi mogu da ubiju

Ovo je ozbiljno. Bolnice su:

- Puni tehnologije
- Povezani sa nacionalnim sistemima
- Prepune kritičnih podataka

Prava opasnost:

- Napadi ransomvera mogu onemogućiti rad opreme za spasavanje života
- Evidencija pacijenata može biti ukradena ili izmenjena
- Hitne službe mogu biti zamrznute usred operacije

Ovo nije samo pitanje podataka, već i života.

7. U vladama: Sajber hladni rat

Vlade su uvijek pod napadom.

Šta je na nišanu:

- Nacionalni sistemi za identifikaciju
- Kontrola granica
- Izborna infrastruktura
- Poverljive informacije

Ko stoji iza toga:

- Hakeri koje podržavaju države iz drugih zemalja
- Haktivisti
- Organizovane grupe za sajber-kriminal

Zašto? Moć, novac, uticaj.

Crna Gora, kao i svaka druga zemlja, dio je ovog sajber bojišta. Zato je izgradnja lokalnog sajber talenta sa ljudima poput vas nacionalni prioritet.

8. U kritičnoj infrastrukturi: Isključite svijetla

Zamislite ovo:

- Šta ako struja nestane u cijeloj zemlji?
- Šta ako pumpe za vodu prestanu da rade?
- Šta ako letovi budu obustavljeni na nekoliko dana?

Ovi sistemi zavise od mreža, a te mreže mogu biti napadnute. **To se zove kritična infrastruktura,** a njena odbrana je vrhunska sajber bezbjednost. Zemlje sada tretiraju sajber odbranu kao nacionalnu odbranu.

Ovdje sajber bezbjednost postaje pitanje nacionalne bezbjednosti.

9. Svuda gdje idete

Sajber bezbjednost nije mjesto. To je sloj.

Svaki put kada:

- Povezujete se
- Prijavite se
- Dodirnite karticu
- Podelite nešto
- Koristite pametnu tehnologiju

...vi ste dio sistema koji zahteva zaštitu.

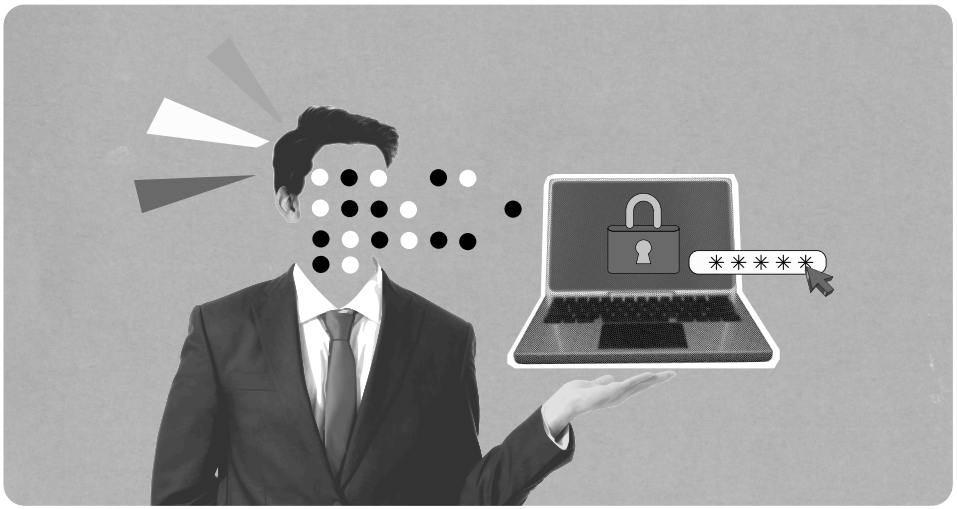
Zato profesionalci za sajber bezbjednost rade u svim sektorima: tehnologija, pravo, finansije, obrazovanje, zdravstvo i drugi.

Sažetak: Sajber bezbjednost je svuda

- Ona je u vašem domu, vašoj školi, vašem poslu.
- Ona štiti preduzeća, bolnice i cele zemlje.
- Nevidljiva je, ali vitalna.
- I sada znate šta je u igri.

Sledi:
Sada hajde da pogledamo šta profesionalci za sajber bezbjednost zapravo rade i koje različite uloge možete igrati u ovoj rastućoj oblasti.

POGLAVLjE 7: Šta profesionalci za sajber bezbjednost zapravo rade



Nije svako u sajber bezbjednosti haker.

Neki nadgledaju. Neki grade. Neki popravljaju. Neki vode. Upoznajmo tim.

1. Sajber bezbjednost je timski sport

Videli ste prijetnje. Videli ste bojno polje.

Sada upoznajte odbrambene stručnjake: ljude koji čuvaju sisteme, preduzeća, pa čak i zemlje bezbednim.

Sajber bezbjednost nije jedan posao. To je ceo svijet uloga. Različite veštine. Različiti umovi. Jedna misija. Hajde da ih razložimo.

2. Odbrambeni borci na prvoj liniji

- Analitičar SOK-a (Centar za bezbjednosne operacije)

Oni su čuvari digitalnog svijeta.

Šta rade:

- Pratite upozorenja
- Uočavaju neobičnu aktivnost
- Odgovaraju na rane znake napada

Voleo biste ovo ako: Volite zagonetke, uočavanje obrazaca i rad pod pritiskom.

- Odgovor na incidente

Uskaču nakon što nešto krene po zlu.

Šta rade:

- Suzbijanje propusta
- Čiste nered
- Otkriju kako se to dogodilo

Zamislite ih kao sajber vatrogasce.

Ovo bi ti se svidelo ako:
Ostajete mirni u haosu i volite brzo rešavati probleme.

3. Etički hakeri

- Proveravač propustljivosti (pentester)

Takođe nazivani “etički hakeri”. Oni pokušavaju da prodru u sisteme uz dozvolu.

Šta rade:

- Pronađite slabe tačke pre nego što to učine stvarni napadači
- Simuliraju napade
- Pišu detaljne izveštaje o tome kako su ušli

Svidelo bi ti se ako: Volite igre hakovanja, CTF (Capture the Flag) takmičenja ili razmišljanje kao zlikovac, radi dobre svrhe.

4. Graditelji i inženjeri

- Bezbjednosni inženjer

Oni izgrađuju i održavaju alate koji štite sisteme.

Šta rade:

- Konfigurisanje zaštitnih zidova
- Dizajniraju bezbjedne mreže
- Instalirati bezbjednosni softver
- Automatizujte odbranu

Svidelo bi ti se ako: Volite da gradite stvari, pišete

skripte i činite da sistemi funkcionišu bez problema.

- Arhitekta bezbjednosti

Oni dizajniraju čitave bezbjednosne strategije.

Šta rade:

- Planiraju kako da obezbede velike sisteme
- Rade sa inženjerima i menadžerima
- Razmišljaju i o tehničkoj i o poslovnoj strani

Svidelo bi vam se ovo ako: Vi ste planirač, mislilac u okviru sistema i volite da osmišljavate rešenja sa široke perspektive.

5. Istražitelji

- Stručnjak za digitalnu forenziku

Oni istražuju nakon incidenta, kao digitalni detektivi.

Šta rade:

- Ispituju logove i datoteke
- Prate aktivnost hakera
- Prikupljaju dokaze za sudske postupke

Svidelo bi ti se ako: Uživate u istragama, detaljima i praćenju istine.

- Analitičar za obaveštajne podatke o pretnjama

Šta rade:

- Praćenje hakerskih grupa
- Analiziraju globalne trendove
- Upozoravaju kompanije o novim napadima

Voleli biste ovo ako: Znatiželjni ste, strateški nastrojeni i volite da budete korak ispred igre.

6. Lideri i komunikatori

- CISO (glavni službenik za bezbjednost informacija)

Šef za sajber bezbjednost.

Šta rade:

- Vodite tim za bezbjednost
- Donositi strateške odluke
- Upravljanje budžetima, rizicima i ljudima

Ovo bi vam se svidelo ako: Želite da vodite, planirate i ostavljate uticaj na najvišem nivou.

- Konsultant za sajber bezbjednost / Trener

Rade u različitim kompanijama i pomažu drugima da razumeju sajber rizike.

Šta rade:

- Pisanje politika
- Obučavaju zaposlene

- Savetovanje timova o najboljim praksama

Svidelo bi vam se ovo ako:
Volite da objašnjavate stvari, da radite sa ljudima i da unapređujete sisteme.

7. Sačekajte: Da li moram da budem tehnološki genije?

Ne..

Neke uloge zahtevaju tehničke veštine (kao što su programiranje ili umrežavanje). Drugi zahtevaju jake komunikacione veštine, analitičke sposobnosti, pa čak i znanje prava i psihologije.

Zapravo:

- Neki od najboljih konsultanata nekada su bili nastavnici.
- Neki od najboljih analitičara potiču iz svijeta igara ili vojske.
- Neki neverovatni etički hakeri nikada nisu pohađali univerzitet.

Sajber bezbjednost je stav. Zbog znatiželje. Fokusiran. Etičan. Rešavač problema.

8. Gdje se nalaze ova radna mesta?

Svuda.

- Tehnološke kompanije
- Banke i telekomunikacije
- Bolnice i škole
- Vlada i vojska
- NVO i međunarodne organizacije

I da, **i u Crnu Goru takođe.**

Sažetak: Pronađite svoju ulogu

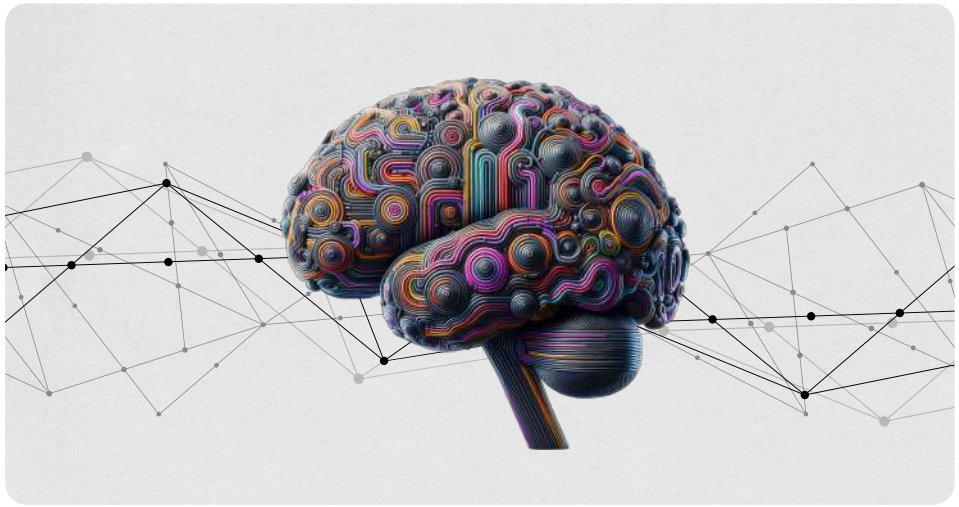
Evo istine: Ne morate biti haker da biste se bavili sajber bezbjednošću.

Možete:

- Gledajte
- Izgradi
- Istraživati
- Savetovati
- Vodite

Koja god da je vaša snaga, postoji uloga za vas.

POGLAVLjE 8: Da li treba da budete genije ili programer?



Kratak odgovor: Ne.

Dug odgovor: Razbijmo mit.

1. Mit koji zaustavlja ljude

Kada čujete “kiber bezbjednos”, šta zamišljate?

- Čovek u dukserici koji kuca 1.000 riječi u sekundi?
- Genije koji je hakovao NASA-u kada je imao 12 godina?
- Programer koji tečno govori pet programskih jezika?

Evo istine: **Ne morate biti genije. Ne morate biti programer.**

Šta vam je zaista potrebno:

- Razišljivost
- Rešavanje problema
- Malo strpljenja
- Volja za učenjem

To je sve. Ostalo se može naučiti.

2. Mnoge uloge ne zahtevaju programiranje

Budimo jasni: Postoje poslovi u oblasti sajber bezbjednosti Gdje programiranje pomaže (kao što su penetraciono testiranje ili analiza malvera). Ali postoje i poslovi u kojima nikada nećete dodirnuti nijednu jedinu liniju koda.

Primjeri:

- Trener za bezbjednosnu svest
- Savetnik za politiku
- Analitičar SOC-a
- Procenjivač rizika
- Tehničar digitalne forenzike
- Analitičar za obaveštaj o pretnjama

Sajber bezbjednost je delimično tehnologija, delimično strategija, delimično komunikacija, delimično psihologija.

3. Šta zapravo više znači

- Kritičko razmišljanje

Možete li da razložite problem? Možete li da pratite tragove? Bićete iznenađeni koliko se napada zaustavi samo postavljanjem pametnih pitanja.

- Razigranost

Najbolji sajber profesionalci su znatiželjni. Istražuju. Testiraju. Istražuju.

- Komunikacija

Možda znate rizike, ali možete li ih objasniti drugima? Svaka organizacija treba ljude koji mogu da predaju, prezentuju i vode.

- Etika

Imaćete pristup sistemima, podacima i poverenju. Etika nije opcionalna; ona je sve.

4. Stvarni ljudi, stvarna poreklo

Neki od najboljih profesionalaca za sajber bezbjednost:

- Nikada nije studirao na univerzitetu
- Počeli u korisničkoj službi ili maloprodaji
- Došli iz vojske ili policije
- Prešli iz potpuno nepovezanih karijera

U ovu oblast možete ući odakle god.

5. Šta je sa sertifikatima?

Sertifikati mogu biti odličan način da dokažete svoje veštine, posebno ako nemate diplomu.

Za početnike pogodne su:

- **CompTIA Security+** - širok uvod u koncepte sajber bezbjednosti
- **Cisco CyberOps** - dobar za uloge u SOC
- **Google Cybersecurity Certificate** - odličan za samostalne učenike
- **TryHackMe / Hack The Box** - - praktične platforme za vežbanje veština

Možete početi od malih sertifikata. Za neke je potrebno samo nekoliko nedelja pripreme.

6. Šta je sa godinama?

Premlad? Prestar? Nije bitno.

- Tinejdžeri mogu da počnu sa onlajn laboratorijama i Jutjubom.
- Oni u dvadesetim mogu da pređu iz drugih oblasti.
- 30+? 40+? Donosite zrelost i životno iskustvo, ogromne prednosti u vođstvu, konsaltingu ili obuci.

Ne postoji **utvrđen put**. Postoji samo tvoj put.

7. Kako započeti bez programiranja

Evo putokaza:

- Naučite osnove iz knjiga, vidio snimaka ili kurseva
- Vježbajte bezbjedne navike (lozinke, svest o fišingu)
- Isprobajte besplatne alate kao što su Wireshark, VirusTotal, Shodan
- Gledajte YouTube analize stvarnih hakovanja
- Pratite stručnjake za sajber bezbjednost na društvenim mrežama
- Istražite besplatne platforme kao što su TryHackMe ili Blue Team Labs
- Pohađajte lokalne radionice, tehnološke susrete ili CTF takmičenja

Bićete iznenađeni koliko daleko možete doći bez napisanja nijedne linije koda.

8. Da li biste na kraju trebali da naučite programiranje?

Možda. Možda i ne.

Ako želite da uđete dublje (kao u hakovanje, skriptiranje ili izradu alata), učenje programiranja će vam pomoći. Ali čak i tada, to možete naučiti kasnije.

Ne morate to da znate na početku.

Većina ljudi u sajber prostoru je naučila stvari tokom posla, polako i korak po korak. Ne dozvolite da vas "neznanje koda" zaustavi.

Sažetak: Ne, ne moraš biti genije ili programer

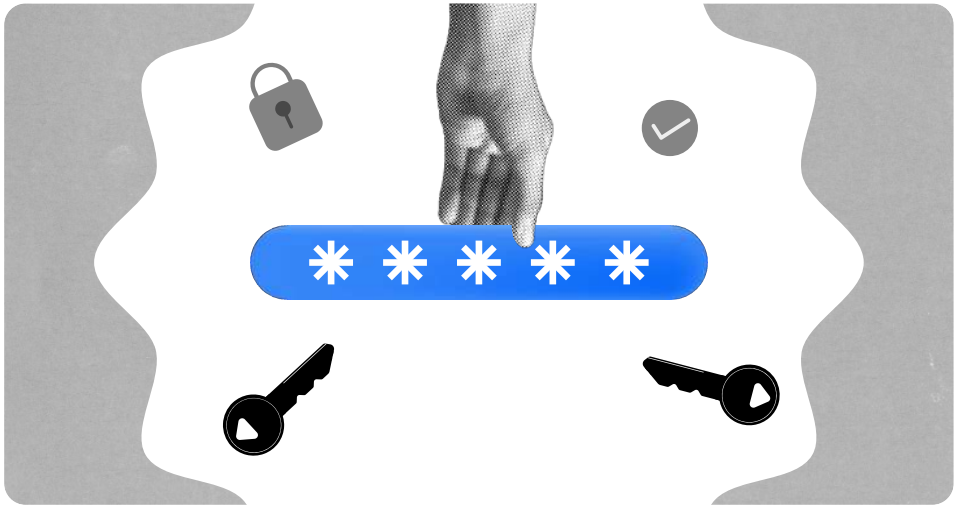
Potrebno vam je:

- Razigranost
- Oštroumnost
- Snažan osećaj za ispravno i pogrešno
- Pokret da učite i štite druge

To je ono što čini profesionalca za sajber bezbjednost.

Uskoro: Hajde da pričamo zašto je ovo važno izvan novca ili tehnologije: jer vam sajber bezbjednost daje moć, kontrolu i slobodu.

POGLAVLjE 9: Sajber bezbjed-nost = moć, kontrola i sloboda



Ovo nije samo o tehnologiji.

Radi se o povratku kontrole nad vašim životom, vašim identitetom, vašoj budućnošću.

1. Sajber bezbjednost nije samo zaštita

Kada ljudi čuju "sajber bezbjednost", oni misle: "Radi se o zaustavljanju hakera." To je dio toga.

Ali u svojoj suštini, sajber bezbjednost je nešto dublje:

- **Kontrola**
- **Moć**
- **Sloboda**

Hajde da to razložimo.

2. KONTROLA: Vi ste vlasnik svog digitalnog života

Internet je haotičan. Svi žele vašu pažnju, vaše podatke, vaše vreme.

Hakeri. Oglašivači. Prevaranti. Aplikacije. Algoritam. Sajber bezbjednost vam daje alate **da povratite kontrolu:**

- Vi odlučujete ko vidi vaše stvari.
- Znate kada je nešto sumnjivo.
- Vi postavljate pravila za svoju privatnost.

Većina ljudi ne kontroliše svoj digitalni život. Oni plutaju. **Sajber bezbjednost vas budi.** Pretvara vas iz pasivnog korisnika u aktivnog čuvara.

3. MOĆ: Vi Razumijete ono što drugi ne razumeju

Budimo realni: većina ljudi ne zna šta se dešava na internetu. Vi ćete.

- Znaćete kako se napadi dešavaju.
- Znaćete koje se podatke prikupljaju.
- Znaćete kako da zaštitite sebe i druge.
- Znaćete kako etički provaljivati u sisteme i kako ih potom popraviti bolje.

U svijetu punom digitalnih pretnji, znanje je moć.
Sajber bezbjednost vas pretvara u nekoga na koga drugi zavise. Ne gubite se. Vi predvodite.

4. SLOBODA: krećete se bez straha

Sajber napadi izazivaju strah.
Strah od nadgledanja.
Strah od hakovanja.
Strah od gubitka svega.

Ali kada znate kako da se odbranite, taj strah nestaje.

- Ne nasedate na prevare.
- Ne paničite zbog lažnih imejlova.
- Ne živiš paranoično, živiš pripremljen.

To je prava sloboda. **Sajber bezbjednost vam omogućava da živite na internetu sa Povjerenjem.**

5. Bonus: I vi možete pomoći drugima

Ono što naučite nije samo za vas.

Možete pomoći:

- Vaši roditelji izbegavaju prevare
- Vaša škola da zaštiti podatke učenika
- Vaše radno mjesto ostane bezbjedno
- Vaša zemlja jača svoju digitalnu otpornost

Ne štitete samo sebe. Vi ste dio pokreta etičnih, pametnih i sposobnih ljudi koji čine internet bezbednijim. To je stvarni uticaj. To je pravo liderstvo.

6. Ovo je veće od posla

Sajber bezbjednost nije samo nešto što “radite”.

To je nešto što jeste.

To je način razmišljanja:

- Uočite skriveni rizik.
- Misli kao napadač.
- Zaštitite ljude.
- Budi pametniji od prijetnje.

Bilo da postanete penetester, trener, konsultant ili samo neko ko zna kako da ostane bezbjedan, kroz svijet ćete prolaziti oštrije.

Zapravo, o tome se Ovdje radi.

Sažetak: Ovo je tvoja supermoć

Sajber bezbjednost vam pruža:

- **Kontrolu** nad svojim podacima i životom
- **Moć** da Razumijete prijetnje i nadmudrite ih
- **Sloboda** da istražujete digitalni svijet bez straha

A kada ga imate?

Niko vam to ne može oduzeti.

Sledi: Pa kako zapravo da započnete? Šta možete da uradite danas da započnete svoje putovanje? Hajde da porazgovaramo o tome.

POGLAVLjE 10: Kako početi da razmišljate kao haker (etički)

Da biste pobedili hakera, morate da mislite kao on.

Ali da biste bili odlični u sajber bezbjednosti, morate to činiti **etički.**

1. Dobri hakeri razmišljaju drugačije

Hakeri vide svijet u smislu:

- Kako stvari funkcionišu
- Gdje mogu da prodru
- I kako ih popraviti (ili iskoristiti)

Ne radi se o haosu. Radi se o znatiželji. Najbolji branioci su kreativni. Oni vide rupe koje drugi ne vide.

Način razmišljanja je sledeći:

> "Šta ako kliknem ovdje? Šta ako je neko zaboravio da zaključa ovaj dio? Šta se dešava ako promenim ovaj ulaz?"

Ovako razmišljaju hakeri. A sada... i vi možete.

2. Hakerov mentalitet = znatiželja + skepticizam

Hajde da razložimo:

- Razigranost
  - Želite da Razumijete sisteme, a ne samo da ih koristite.
  - Istražujete podešavanja, zalazite u to kako stvari funkcionišu.
  - Pitate se: "Šta se dešava ako...?"
- Skepticizam
  - Ne verujete linkovima na slepo.
  - Dovodite u pitanje svaku stranicu za prijavu.
  - Primećuješ čudne obrasce koje drugi ignorišu.

Zajedno, to te čini moćnim.

Prestaješ da budeš samo "korisnik." Postajete **lovac.**

3. Počnite malo: Analizirajte ono što svakodnevno koristite

Probajte ovu vežbu: Pogledajte svoju omiljenu aplikaciju ili veb-sajt i zapitajte se:

- Šta se dešava kada kliknem na "Zaboravio sam lozinku"?
- Šta ako neko pogodi moje bezbjednosno pitanje?
- Mogu li ovo da otvorim u više kartica i zbunim ga?
- Da li se URL menja kada se prijavim? Šta tada prikazuje?

Ne kršite ništa. Učite. Ovo je početak izviđanja: ključna veština za etičke hakere.

4. Vježbajte "digitalnu svest" svakodnevno

Baš kao što borilački majstori ostaju na oprezu na ulici, sajber profesionalci ostaju na oprezu na internetu. Primjeri:

- Primetiš lažni link u poruci prijatelja.
- Primetiš da stranica za prijavu izgleda malo drugačije.
- Vidite USB stik koji leži u blizini i ne ubacujete ga.

Ove male odluke = hakerski način razmišljanja na delu. Vežbate oko.

5. Koristite iste alate kao pravi hakeri

Da, ozbiljno. Studenti sajber bezbjednosti koriste stvarne alate koje hakeri koriste, ali u laboratorijama, a ne na živim ciljevima. Možete isprobati:

- **TryHackMe** (besplatni gejmifikovani izazovi u hakovanju)
- **Shodan.io** (pretraživač izloženih uređaja)
- **VirusTotal** (skenirajte linkove i datoteke radi malvera)
- **Burp Suite** (za veb testiranje; počnite sa besplatnom verzijom)
- **Wireshark** (videti šta se dešava na mreži)

Važno: Testirajte samo sisteme koje posedujete ili za koje imate dozvolu da ih koristite. To je ono što vas čini etičnim.

6. Naučite da lomite stvari kako biste ih mogli popraviti

Budimo iskreni: razbijanje stvari je zabavno. Ali ono što vas čini "white hat" hakerom (dobra vrsta hakera) jeste vaša svrha. Vi lomite stvari da biste:

- Razumeti ih
- Poboljšati ih
- Pomozite drugima da ostanu bezbedni

Za to kompanije plaćaju. To je ono što školama, bolnicama i vladama treba.

7. Hakujte na pravi način (etičke granice)

Da:

- Pridružite se legalnim Capture The Flag (CTF) takmičenjima
- Hakujte test okruženja kao što su TryHackMe ili Hack The Box
- Učite od Jutjub kanala etičkih hakera
- Istraživanje ranjivosti u bezbednim sistemima zasnovanim na dozvolama

Ne:

- Ne testirajte veb-sajtove ili aplikacije bez dozvole
- Ne pristupajte nalozima koji nisu vaši
- Ne delite privatne podatke ili "curenja" na koja naiđete
- Nemojte misliti da "samo gledanje" znači da neće biti štete

8. Razmišljaj kao haker. Postupaj kao zaštitnik.

Odličan etički haker ne zna samo trikove. Oni znaju:

- Kako stvarni napadači deluju
- Kako sistemi mogu da otkažu
- Kako ljudi bivaju prevareni

Ali oni takođe:

- Znaju kada da prestanu
- Poštuju granice
- Radite za dobru stranu

To je kao da si otvarač brava koji pomaže u unapređenju dizajna vrata.

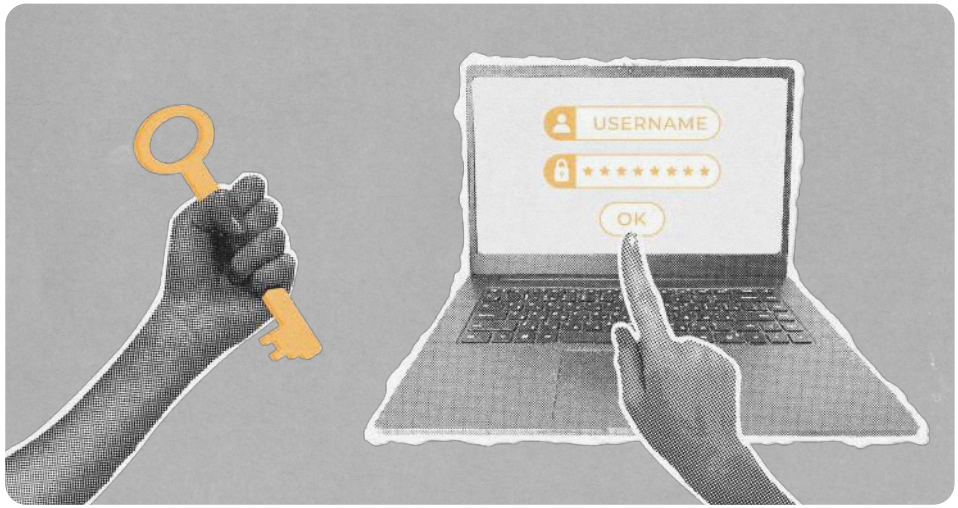
Sažetak: Trenirajte svoj um kao haker

Da biste počeli da razmišljate kao haker:

- Ostanite znatiželjni
- Dovodite u pitanje sve
- Istraži kako stvari funkcionišu
- Vježbajte bezbjedno
- I uvijek postupaj etično

Sledi: Pre nego što završimo, hajde da porazgovaramo o osnovnoj sajber higijeni, malim navikama koje vas štite odmah, čak i pre nego što karijera započne.

POGLAVLjE 11: Sajber higijena koju možete primeniti već danas



Ne morate biti stručnjak da biste ostali bezbedni na internetu.

Nekoliko jednostavnih navika mnogo znači. Učinimo ih delom vašeg svakodnevnog života.

1. Šta je sajber higijena?

Sajber higijena je kao i lična higijena.

- Svakodnevno pereš zube da bi spriječio karijes.
- Tuširate se da ne mirišete kao torba za vežbanje.
- Siječete nokte, čistite uši i perete ruke.

Sajber higijena = male digitalne navike koje sprječavaju veće probleme.

Ne trebaju vam napredni alati. Samo doslednost i svest.

2. Koristite jake, jedinstvene lozinke

Ako svuda koristite istu lozinku, to je kao da koristite jedan ključ za kuću, automobil, ormančić i bicikl. Ako neko jednom ukrade lozinku, on poseduje ceo vaš život.

Kako to popraviti:

- Koristite različite lozinke za svaki sajt.
- Neka budu duge (najmanje 12 znakova).
- Izbegavajte imena, datume ili lake pretpostavke.

Profesionalni savet: Koristite menadžer lozinki (kao što su Bitwarden ili 1Password).

On pamti sve, pa vi ne morate.

3. Uključite dvofaktorsku autentifikaciju (2FA)

Ovo je jedna od najmoćnijih odbrana koje možete koristiti.

Kako funkcioniše:

- Prijavljujete se sa svojom lozinkom.
- Zatim potvrđujete da ste zaista vi kodom sa svog telefona ili aplikacije.

Čak i ako neko ukrade vašu lozinku, i dalje ne može da uđe.

Gdje ga koristiti:

- E-pošta
- Društveni mediji
- Bankarstvo
- Sve što je važno

Uključite ga. Danas.

4. Ne kliknite na nasumične linkove

Ako vam nešto deluje sumnjivo, verovatno i jeste.

Primjeri sumnjivih linkova:

- Kliknite Ovdje da preuzmete svoju nagradu!
- Vaš nalog je suspendovan, prijavite se odmah!
- Skraćene veze (bit.ly, tinyurl) od nepoznatih osoba

Šta uraditi umjesto toga:

- Idite direktno na sajt (ne kliknite; unesite adresu)
- Pređite mišem preko linka da biste videli Gdje zapravo vodi
- Zapitajte se: Da li bi me ova kompanija zaista

kontaktirala na ovaj način?

Ako niste sigurni, ne kliknite. Nikad.

5. Držite svoj softver ažuriranim

Da, ažuriranja su dosadna. Da, ažuriranja su važna. Većina hakera koristi **stare ranjivosti,** stvari koje su ažuriranja već popravila.

Šta ažurirati:

- Tvoj telefon
- Vaše aplikacije
- Vaš laptop
- Vaš pregledač
- Tvoj ruter (da, čak i on)

Napravite to navikom. Ažuriranja = zakrpe = zaštita.

Napravite to navikom. Ažuriranja = zakrpe = zaštita.

Javni Wi-Fi je kao da vičete svoje lozinke preko prepune sobe.

Bezbednije opcije:

- Koristite mobilne podatke ako je moguće.
- Ako morate da koristite javni Wi-Fi:

- Ne prijavljujte se na osetljive naloge.
- Ne prijavljujte se na osetljive naloge.

7. Razmislite pre nego što podelite

Taj smešan post, simpatičan selfi ili ljuti tvit mogu biti bezopasni.

Ili... to može:

- Otkriti svoju lokaciju
- Otkrivanje ličnih podataka
- Može biti iskorišćen da biste bili falsifikovani kasnije

Zapitajte se:

- Da li bih bio u redu ako bi ovo neko snimio snimkom ekrana i poslao nepoznatim osobama?
- Da li otkrivam više nego što mislim?

Digitalni otisci su trajni. Hodajte mudro.

8. Koristite antivirus (čak i besplatan)

Antivirus nije savršen. Ali pomaže da se uoči osnovni malver pre nego što se proširi.

Dobre besplatne opcije:

- Windows Defender (ugrađen u Windows)
- Bitdefender Free

- Avast ili AVG (sa oprezom; izbegavajte bloatware)

Samo se ne oslanjajte na njega kao na jedinu odbranu. Zamislite to kao vezivanje sigurnosnog pojasa — i dalje je bolje da ne dođe do sudara.

9. Napravite rezervnu kopiju svojih podataka

Ako vas pogodi ransomware, prestane da radi laptop ili vam se fajlovi obrišu... Zažalićete što niste napravili rezervnu kopiju.

Šta rezervisati:

- Fotografije
- Školski projekti
- Dokumenti
- Sve što vam je važno

Gdje da napravite rezervnu kopiju:

- Spoljni disk
- Cloud usluge (Google Drive, Dropbox, iCloud)

Radite to redovno. Vaša budućnost će vam biti zahvalna.

10. Pričajte o tome

Sajber higijena postaje jača kada se deli. Pomozite svojim:

- Roditelji ažuriraju svoje uređaje
- Braću i sestre upozorite da izbegavaju sumnjive preuzimanja
- Prijatelji prestaju da ponovo koriste “123456” kao lozinku

Ne moraš da propovedaš. Samo budi najpametniji u grupi. Bezbjednost se širi.

Sažetak: Male navike, velika zaštita

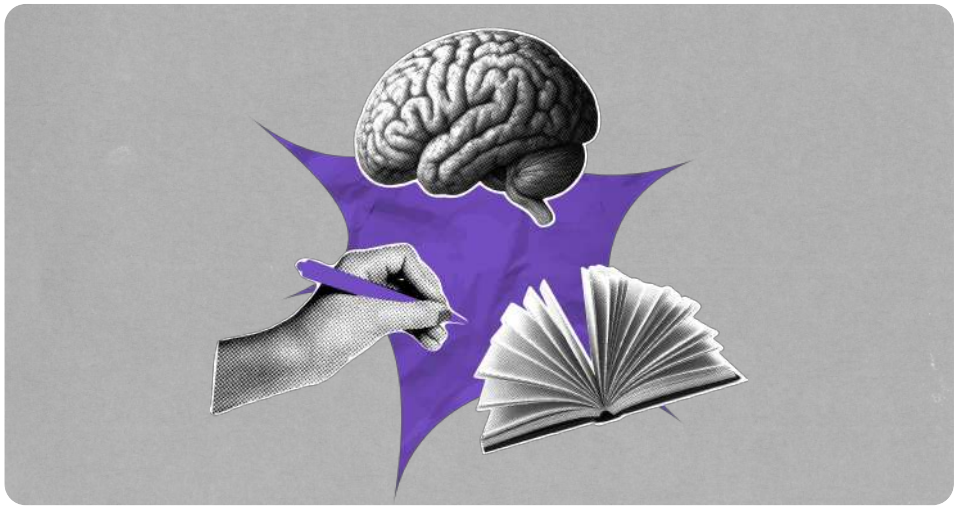
Počnite Ovdje. Počnite sada.

- Jedinstvene lozinke
- 2FA svuda
- Ne kliknite na sumnjive linkove
- Ažurirajte sve
- Napravite rezervnu kopiju svojih podataka
- Ostanite oštri i svesni

Ne morate sve da uradite odjednom. Ali što pre počnete, to ćete biti bezbedniji.

Sledeće: Završimo ovo putovanje vašim sledećim koracima: kako nastaviti sa učenjem, kako istražiti sajber karijere na Kosovu i kako sve ovo shvatiti ozbiljno, a da ne izgubite zabavu.

Kako steći obrazovanje u oblasti sajber bezbjedn-osti u Crnoj Gori



1: Zašto je ovo važno

Cilj poglavlja: Pokazati mladima da, ako žele da uđu u svijet sajber bezbjednosti, Crna Gora ima realne obrazovne puteve – akademske i profesionalne – koji mogu biti početak njihove karijere. Ne morate ići u inostranstvo da biste započeli svoje sajber putovanje. Crna Gora raspolaže univerzitetima, fakultetima i centrima za obuku koji nude studijske programe,

izborne predmete ili specijalizovane obuke iz oblasti informacionih tehnologija i sajber bezbjednosti. Imate opcije: akademsku diplomu, praktičnu obuku (bootcamp) ili profesionalne sertifikate – u zavisnosti od toga koliko brzo i koliko duboko želite da uđete u ovu oblast.

2: Univerziteti – Akademski put

1. **Univerzitet Crne Gore (UCG)**

PMF – Računarstvo i informatika

- Tehnička IT osnova: programiranje, mreže, informacioni sistemi
- Sajber-teme: osnove bezbjednosti podataka i sistema

➡️ Dobra baza za **tehničke sajber uloge.**

ETF – Elektrotehnika / IT

- Inženjerski fokus: telekomunikacije, mrežna infrastruktura
- Sajber-kontekst: sistemi i infrastruktura

➡️ Pogodno za **infrastrukturnu i mrežnu bezbjednost.**

Ekonomski fakultet

- Biznis i menadžment perspektiva
- Sajber-teme: upravljanje rizicima, digitalno poslovanje

➡️ Ulaz u cyber risk, compliance i governance.

Pravni fakultet

- Pravni okvir i regulativa
- Sajber-teme: sajber-kriminal, zaštita podataka, privatnost

➡️ Idealno za pravne i policy uloge u sajber oblasti.

2. Univerzitet Donja Gorica (UDG)

FIST – Fakultet za informacione sisteme i tehnologije

- Interdisciplinarni IT pristup
- Sajber-kontekst: bezbjednost sistema, digitalna transformacija

➡️ Za strateški i poslovno-tehnološki pristup.

3. Univerzitet Mediteran

FIT – Fakultet informacionih tehnologija

- Praktično orijentisani IT programi
- Sajber-teme: informatička bezbjednost, zaštita podataka

➡️ Dobar izbor za primjenjiva IT znanja sa sajber osnovom.

Ključna poruka (ukratko)

- U Crnoj Gori nema jedinstvene „Cybersecurity“ diplome

- Postoji više akademskih ulaza: IT, inženjerstvo, pravo, ekonomija
- Sajber-specijalizacija se gradi kroz predmete, projekte i dodatne obuke

➡️ Fakultet biraš po osnovi.
➡️ Sajber karijeru gradiš kroz praksu.

03. Iza univerziteta – stručne škole i obuke

Nije svima potreban pun univerzitetski stepen da bi započeli karijeru u sajber bezbjednosti. U Crnoj Gori postoje **realne, dostupne opcije** za kraće, praktične i tržišno orijentirane obuke — posebno kao dopuna fakultetu ili kao brži ulaz u IT/sajber svijet.

◆ ICT Cortex Academy

- ICT Cortex Academy je dio ICT Cortex inicijative, koja okuplja tehnološke kompanije i partnere s ciljem razvoja IT
- i digitalnih vještina u Crnoj Gori.
- Zvanična stranica: https://ictcortex.me/en/
- Programi i aktivnosti usmjereni su na:
  - ○ osnove informacionih tehnologija
  - ○ digitalne i tehničke vještine
  - ○ rad u IT okruženju i savremene tehnologije
- Poseban naglasak je na praktičnom učenju i povezivanju sa IT zajednicom.

➡️ Poseban naglasak je na praktičnom učenju i povezivanju sa IT zajednicom.

Training Providers Montenegro

- EduCom Academy (or “IT akademija Crna Gora” site — mostly general courses, not clear cyber focus) — some general IT training exists but not a dedicated cyber program.
- ICT Cortex Akademija — appears as a project/ initiative but not clearly an established cyber curriculum.
- Amplitudo Akademija — real training provider focused on IT development (web, apps), not necessarily a specific cyber program.

These can still be **listed as community partners or broader IT training options.**

04: Onlajn platforme i laboratorije

- Cyberlance
- Virtuelna, praktična obuka iz oblasti sajber bezbjednosti.
- Realistične simulacije = bezbjedno okruženje za vežbanje napada/odbrane.
- Koriste ga studenti, profesionalci, pa čak i kompanije.

Učenje sajber bezbjednosti ne dešava se samo u učionici. Onlajn platforme i tehnološki parkovi omogućavaju praktično učenje, eksperimentisanje i

povezivanje sa IT zajednicom.

- Ovakve platforme koriste
  - studenti
  - mladi profesionalci
  - IT kompanije za obuku kadrova

➡️ Idealno za razvijanje praktičnih sajber vještina uz sopstveni tempo učenja.

Naučno-tehnološki park Crne Gore (Podgorica)

Naučno-tehnološki park Crne Gore (Podgorica)

- IT kompanije
- startapove
- istraživačke i inovacione timove

Omogućava:

- rad na realnim tehnološkim projektima
- mentorsku podršku
- povezivanje sa industrijom i institucijama

Sajber-bezbjednost se pojavljuje kroz:

- razvoj digitalnih rješenja
- bezbjednost sistema i podataka

➡️ Dobra sredina za mlade koji žele praktično iskustvo i ulazak u IT ekosistem.

Tehnopolis – Nikšić

Inovaciono-tehnološki centar fokusiran na:

- IT
- inženjering
- startap razvoj

Podržava:

- obuke
- radionice
- projekte iz oblasti digitalnih tehnologija

Sajber teme se obrađuju kroz:

- IT infrastrukturu
- digitalnu bezbjednost
- razvoj tehnoloških rješenja

➡️ Pogodno za učenje kroz projekte i timski rad.

Kratak zaključak

- Praksa je ključ u sajber bezbjednosti.
- Onlajn laboratorije + tehnološki parkovi = sigurno okruženje za učenje i eksperimentisanje.
- U Crnoj Gori već postoje prostori gdje možeš:
  - učiti
  - testirati
  - graditi karijeru

➡️ Znanje raste najbrže kada ga primijeniš u praksi.

05: Izbor vašeg puta

Zapitajte se:

- Da li želim diplomu (3 godine, akademska + karijerna osnova)?
- Da li više volim kratku, praktičnu obuku (meseci, praktične veštine)?
- Ili želim da kombinujem oba, diplomu i profesionalne sertifikate?

Dobra vest: Crna Gora sada nudi sve **tri opcije.**

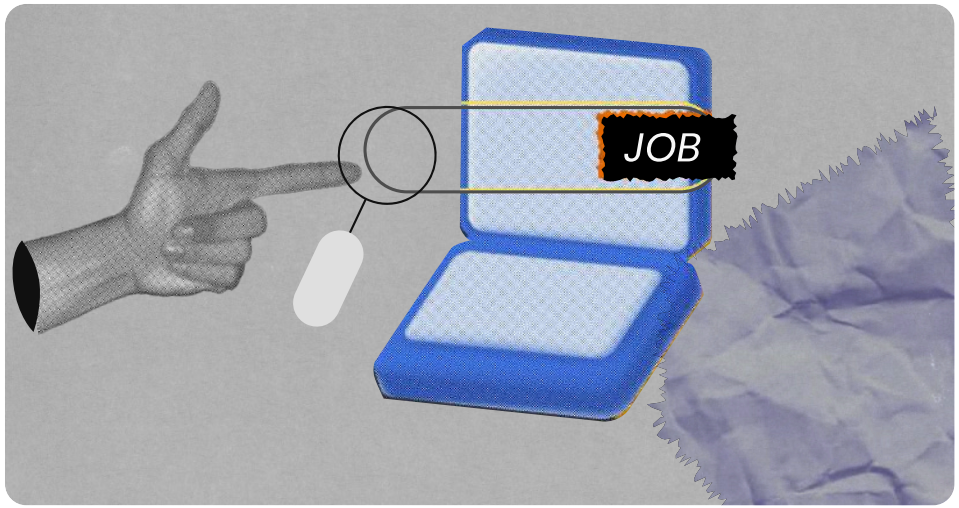
Rezime

Ne morate da napustite Crnu Goru da biste studirali sajber bezbjednost. Mozete da birate:

- Univerziteti:
- Profesionalne škole:
- Specijalizovani centri:
- Onlajn platforme:

Vaš izbor zavisi od toga koliko duboko želite da uđete i koliko brzo. U svakom slučaju, mogućnosti su ovdje.

Gdje raditi u oblasti sajber bezbjednosti u Crnoj Gori



01: Zašto su poslovi u sajber bezbjednosti svuda

Cilj poglavlja: Pokazati vam da sajber bezbjednost nije samo “jedna karijera”. To su stotine uloga raspoređenih u vladi, bankama, tehnološkim kompanijama, nevladinim organizacijama, pa čak i u bolnicama ili aerodromima. Sajber bezbjednost eksplodira. Svaka organizacija koja

koristi računare, mreže ili podatke (što je praktično sve njih) treba zaštitu. To znači da se otvaraju radna mesta širom Crne Gore u vladi, bankama, telekomunikacionim kompanijama, startapima i kritičnoj infrastrukturi. Ako steknete veštine, potražnja vas već čeka.

02: Karijere u javnom sektoru

1. Ministarstvo javne uprave

- Centralna državna institucija nadležna za:
  - digitalizaciju javne administracije
  - informacionu i sajber-bezbjednost državnih IKT sistema
- Koordinira:
  - državne IKT politike
  - implementaciju sajber-mjera u institucijama
- Uključena u:
  - strateške dokumente
  - usklađivanje sa EU (NIS/NIS2)

➡️ Glavna civilna institucija za državnu sajber-politiku.

2. CIRT.me

Nacionalni CSIRT Crne Gore

- Zvanični nacionalni tim za odgovor na računarske incidente.
- Djeluje u okviru Agencije za elektronske komunikacije i poštansku djelatnost (EKIP). Nadležnosti:
  - prijem i obrada sajber-incidenata
  - koordinacija odgovora
  - upozorenja i preporuke institucijama i građanima
  - međunarodna CSIRT/CERT saradnja

➡️ https://www.cirt.me/

➡️ Ključna operativna tačka za sajber-incidente u Crnoj Gori.

3. Agencija za elektronske komunikacije i poštansku djelatnost (EKIP)

- Nacionalni regulator za:
  - elektronske komunikacije
  - telekomunikacione mreže
- Institucionalni „dom“ za CIRT.me.
- Uloga u:

- bezbjednosti telekomunikacione infrastrukture
- nadzoru operatora

➡️ Posebno važna za infrastrukturnu i telekomunikacionu sajber-bezbjednost.

4. Savjet za informacionu bezbjednost

- Savjetodavno tijelo Vlade Crne Gore.
- Okuplja:
  - državne institucije
  - bezbjednosni sektor
  - stručnjake
- Fokus:
  - nacionalna strategija informacione i sajber-bezbjednosti
  - koordinacija politika

➡️ Strateški i policy nivo sajber-bezbjednosti.

5. Ministarstvo odbrane Crne Gore

- Sajber-bezbjednost u kontekstu:
  - odbrane
  - hibridnih prijetnji
  - NATO standarda

- Rad kroz:
  - odbrambene IKT sisteme
  - međunarodnu vojnu saradnju

➡️ Sajber-bezbjednost kao dio nacionalne odbrane.

6. Državne institucije i operatori ključnih usluga

(elektroenergetika, voda, transport, zdravstvo, telekomi)

- Obaveze u skladu sa:
  - nacionalnim propisima
  - EU NIS direktivama
- Imaju:
  - interne IT/sajber timove
  - ili odgovorna lica za sajber-rizike

➡️ Ovdje se sajber-bezbjednost direktno vezuje za funkcionisanje društva.

Kratak rezime (jako važno za vodič)

U Crnoj Gori NE postoji jedna institucija pod nazivom „Agencija za sajber bezbjednost“.

Kao u nekim drugim državama.

➡️ Sajber-bezbjednost je raspoređena po institucijama, a ključni nosioci su:

- Ministarstvo javne uprave (politike i koordinacija)
- CIRT.me (EKIP) (operativni odgovor)
- Savjet za informacionu bezbjednost (strategija)
- Ministarstvo odbrane (odbrambeni aspekt)

03: Karijere u finansijskom sektoru

Banke su glavne mete hakera, što ih čini velikim poslodavcem za sajber profesionalce.

Banke u Crnoj Gori i tipične sajber uloge

Banke:

- Centralna banka Crne Gore (CBCG)
- Crnogorska komercijalna banka (CKB)
- NLB Banka Podgorica
- Erste Bank AD Podgorica
- Hipotekarna banka

- Lovćen banka
- Adriatic Bank AD Podgorica
- Zapad banka
- Universal Capital Bank (UCB)
- Prva banka Crne Gore
- Ziraat Bank Montenegro

Tipične sajber uloge u bankarskom sektoru:

- CISO (glavni službenik za informacionu bezbjednost)
- Menadžer za IT bezbjednost
- SOC analitičar
- Stručnjak za sajber rizike i usklađenost (Compliance)
- Službenik za digitalnu forenziku
- Specijalista za upravljanje identitetima i pristupima (IAM)
- Analitičar za reagovanje na incidente

➡️ Ove uloge postoje u svim većim bankama, uz razlike u veličini i strukturi timova, ali sa istim fokusom: zaštita novca, podataka i povjerenja klijenata.

04: Privatni sektor i konsalting

Privatni sektor i sajber karijere u Crnoj Gori

(ICT Cortex ekosistem)

Privatni sektor predstavlja **najraznovrsnije polje za**

s**ajber karijere u Crnoj Gori**. Od velikih telekomunikacionih kompanija, preko IT firmi i softverskih kuća, do startapova – svaka organizacija koja obrađuje **osjetljive podatke, digitalne sisteme i onlajn usluge** ima potrebu za stručnjacima iz oblasti sajber bezbjednosti.

ICT Cortex je ključni tehnološki klaster u Crnoj Gori koji okuplja IT, softverske i digitalne kompanije, i predstavlja prirodnu ulaznu tačku za rad u privatnom sajber sektoru.

➡️ https://ictcortex.me/clanice/

Telekomunikacione kompanije u Crnoj Gori

- Crnogorski Telekom
- One Crna Gora
- M:tel Crna Gora

➡️ Tipične sajber uloge:

- Network Security Engineer
- SOC Analyst
- Incident Response Specialist
- Penetration Tester

➡️ Fokus: **zaštita mreža, korisničkih podataka i kritične telekomunikacione infrastrukture.**

IT i tehnološke kompanije (članice ICT Cortex-a)

Kompanije okupljene oko ICT Cortex-a rade u oblastima:

- razvoja softvera
- cloud i infrastrukturnih rješenja
- digitalnih platformi
- data i AI tehnologija

U ovim kompanijama sajber bezbjednost je često integrisana kroz:

- bezbjednost aplikacija
- cloud bezbjednost
- DevSecOps prakse
- zaštitu podataka i sistema

➡️ Tipične uloge:

- Cybersecurity Consultant
- Cloud / DevSecOps Engineer
- Application Security Specialist
- Junior SOC Analyst
- IT Security Engineer

➡️ Često se nude junior pozicije, prakse i rad na projektima, što ih čini pogodnim za ulazak mladih u sajber oblast.

Startap i inovacioni ekosistem

Kroz ICT Cortex i povezane inicijative:

- startapovi razvijaju digitalne proizvode
- sajber bezbjednost se ugrađuje od samog početka (security-by-design)

➡️ Sajber vještine se ovdje kombinuju sa:

- programiranjem
- QA i testiranjem
- cloud i API bezbjednošću

➡️ Idealno okruženje za one koji traže dinamičnu karijeru i brzo učenje.

Zašto je ovo važno

U privatnom IT sektoru u Crnoj Gori:

- sajber bezbjednost nije izolovana funkcija
- ona se prirodno povezuje sa:
    - razvojem softvera
    - cloud tehnologijama
    - QA procesima
    - data i AI rješenjima

➡️ Ako te zanimaju tehnologija, programiranje i rad na realnim projektima – privatni sektor je najbrži put u sajber karijeru.

05: NVO i civilno društvo u Crnoj Gori

Nije svaki posao u oblasti sajber bezbjednosti korporativni ili tehnički. U Crnoj Gori, organizacije civilnog društva sve više angažuju stručnjake iz oblasti sajber bezbjednosti za rad na podizanju svijesti, istraživanju, digitalnim pravima i javnim politikama.

Relevantne organizacije i inicijative u Crnoj Gori:

- Women4Cyber Montenegro – dio evropske inicijative za osnaživanje žena u oblasti sajber bezbjednosti, edukacije i karijernog razvoja.
- Digital Forensic Center (DFC) – bavi se istraživanjem dezinformacija, hibridnih prijetnji, sajber uticaja i digitalne bezbjednosti.
- Centar za demokratsku tranziciju (CDT) – radi na pitanjima izbora, digitalnog integriteta, transparentnosti i sajber rizika u demokratskim procesima.
- Institut Alternativa – istraživanja javnih politika, uključujući digitalnu upravu, bezbjednost institucija i upravljanje rizicima.
- Human Rights Action (HRA) – digitalna prava, privatnost, zaštita podataka i sloboda izražavanja u digitalnom prostoru.

- Western Balkans Cyber security Center - Podgorica - training center - regional initiative

Tipične sajber uloge u NVO sektoru:

- Cybersecurity trener / edukator
- Istraživač javnih politika
- Analitičar digitalnih prijetnji i dezinformacija
- Dizajner kampanja za podizanje sajber svijesti
- Zagovornik digitalnih prava i privatnosti

➡️ Ovaj sektor je posebno pogodan za one koji žele da spoje sajber znanje sa pravom, politikom, edukacijom i društvenim uticajem.

06: Kritična infrastruktura u Crnoj Gori

Kritična infrastruktura = kičma države.
Njena zaštita predstavlja **pitanje nacionalne bezbjednosti** i ključnu oblast za razvoj sajber karijera u Crnoj Gori.

Energetika

- Elektroprivreda Crne Gore (EPCG) – proizvodnja električne energije
- CGES (Crnogorski elektroprenosni sistem) – prenosna mreža

- CEDIS – distribucija električne energije

Transport

- Aerodromi Crne Gore (Podgorica i Tivat)
- Željeznički prevoz Crne Gore (ŽPCG)
- Uprava za saobraćaj / putne vlasti

Zdravstvo

- Klinički centar Crne Gore (KCCG)
- Institut za javno zdravlje Crne Gore
- Privatne bolnice i zdravstvene ustanove

Vodosnabdijevanje

- Regionalna vodovodna preduzeća (npr. Vodovod Podgorica, Regionalni vodovod Crnogorsko primorje)
- Komunalna preduzeća za upravljanje otpadnim vodama

Digitalna infrastruktura

- Crnogorski Telekom
- One Crna Gora
- M:tel Crna Gora

Javna uprava

- Ministarstva
- Opštine

- Skupština Crne Gore
- Državne agencije i regulatorna tijela

Proizvodnja i distribucija hrane

- Veće prehrambene kompanije i prerađivači
- Distributivni centri, logistika i skladišta

Tipični sajber poslovi u kritičnoj infrastrukturi:

- Bezbjednost industrijskih sistema (ICS / SCADA)
- Nadzor mreža i sistema u realnom vremenu
- Upravljanje i odgovor na sajber incidente u vitalnim uslugama
- Sajber otpornost i krizni menadžment

➡️ Ovdje sajber bezbjednost nije samo IT posao, već direktna zaštita zdravlja, energije, saobraćaja i funkcionisanja države.

07: Vaša mapa sajber karijere

Evo pregleda Gdje možete raditi na Kosovu:

- Vlada – branite zemlju.
- Banke – Štite novac i Povjerenje.
- Privatne kompanije – Izgradite i Obezbjedite tehnologiju.
- NVO – Zastupanje i edukacija.

- Kritična infrastruktura – Obezbediti nesmetano funkcionisanje društva.

Sajber bezbjednost nije jedan put. To je ekosistem. I Crna Gora ga brzo gradi.

➡️ Pitanje nije da li ima mjesta za tebe.

➡️ Pitanje je gdje ti želiš da budeš u tome.