Sufinansira Europska unija

Switzerland.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

VODIČ ZA SAMOSTALNO UČENJE

OSNOVE CYBER SIGURNOSTI ZA ČLANICE BIZNIS UDRUŽENJA I ORGANIZACIJA

Udruženje
e-Transformacija

Sarajevo, 2025.

Sadržaj

Zašto je cyber sigurnost važna 3

Prepoznavanje lažnih e-mailova (phishing) 4

Kako kreirati sigurnu lozinku? 6

Dvofaktorska autentifikacija (2FA):
Zašto je važna i kako se koristi? 8

Redovan backup:
Vaša sigurnosna mreža u digitalnom svijetu 10

Ažuriranja softvera:
Vaš prvi štit protiv digitalnih prijetnji 12

Sigurno korištenje interneta i Wi-Fi mreža:
Pametno povežite, mudro zaštitite 14

Kako zaštititi mobilni uređaj:
Vaš džepni trezor 16

Osnove sigurnog korištenja e-maila:
Pametno klikni, sigurno komuniciraj 18

Kako reagovati u slučaju sigurnosnog incidenta:
Smireno, efikasno, odgovorno 20

Ko je odgovoran za sigurnost? Odgovor: Svi! 22

Uloga menadžmenta i zaposlenih
u jačanju sigurnosne kulture 24

Checklist: Da li je vaša firma spremna za cyber izazove? 26

Kratki test znanja iz oblasti cyber sigurnosti 27

Šta dalje? Gdje učiti više? 27

Zašto je cyber sigurnost važna?

U današnjem digitalnom dobu, poslovni procesi gotovo u potpunosti ovise o informacijskim tehnologijama. Fakturisanje, narudžbe, upravljanje projektima, interna komunikacija, rad sa klijentima – sve se odvija putem interneta, mobilnih aplikacija, cloud servisa i elektronske pošte. I dok digitalizacija donosi brojne prednosti u efikasnosti i dostupnosti, ona istovremeno otvara vrata raznim oblicima prijetnji i zloupotreba.

Šta je cyber sigurnost?

Cyber sigurnost predstavlja skup mjera, procedura i tehnologija koje štite digitalne sisteme, podatke i komunikaciju od neovlaštenog pristupa, krađe, oštećenja ili manipulacije. Njena uloga nije samo tehnička – ona je temelj očuvanja poslovne reputacije, povjerenja klijenata i kontinuiteta rada.

Posljedice ignorisanja sigurnosti

Nezaštićen sistem može biti meta:

- **Ransomware napada,** gdje se podaci šifriraju i zahtijeva novčani otkup
- **Phishing poruka** koje dovode do krađe identiteta ili pristupa finansijskim sredstvima
- **Sabotaže ili grešaka** koje rezultiraju trajnim gubitkom važnih informacija

Primjer iz prakse: Jedna lokalna kompanija doživjela je napad ransomware-om uslijed nepostojanja sigurnosne kopije podataka. Rezultat: gubitak svih poslovnih dokumenata i višesedmični prekid rada, uz finansijski gubitak i narušenu reputaciju među klijentima.

Da li ste spremni na neočekivano?

Razmislite o sljedećem zadatku: Zapišite koje digitalne alate koristite svakodnevno u poslu – e-mail, CRM, fakturisanje, cloud servisi, društvene mreže. Zatim se zapitajte: Šta bi se desilo da im ne možete pristupiti naredna tri dana? Koliko bi to koštalo? Koga bi to pogodilo? Koji su vaši planovi oporavka?

Cyber sigurnost nije pitanje luksuza – ona je neophodna komponenta svakog savremenog poslovanja. Njena primjena počinje od osnovnih koraka: redovne edukacije zaposlenih, sigurnosnih kopija podataka, korištenja provjerenih aplikacija i definisanih procedura u slučaju incidenata. Investicija u sigurnost danas znači stabilnost i otpornost vašeg poslovanja sutra.

Prepoznavanje lažnih e-mailova (phishing)

U digitalnom svijetu, elektronska pošta ostaje jedan od najčešće korištenih oblika komunikacije – kako u poslovnom, tako i u privatnom kontekstu. Nažalost, upravo zbog svoje široke rasprostranjenosti, e-mail je i najčešći kanal putem kojeg se provode cyber napadi. Jedan od najrasprostranjenijih oblika digitalne prevare jeste phishing.

Šta je phishing?

Phishing predstavlja pokušaj obmane u kojem napadač šalje poruku koja izgleda kao da dolazi od pouzdane institucije – banke, kolege, direktora ili čak državnog organa. Cilj napada je navesti korisnika da klikne na sumnjiv link, preuzme zaražen fajl ili upiše lične podatke poput lozinke, broja kreditne kartice ili drugih povjerljivih informacija.

Ovi napadi mogu dovesti do krađe identiteta, gubitka pristupa sistemima, finansijskih gubitaka pa čak i do kompromitacije čitavih organizacija.

Kako prepoznati sumnjiv e-mail?

Iako phishing poruke često izgledaju uvjerljivo, postoji nekoliko jasnih pokazatelja koji ih odaju:

- **Neobična e-mail adresa pošiljaoca:** Iako se može činiti da poruka dolazi od poznate organizacije, adresa često sadrži dodatne riječi ili domene (npr. info@banka.support umjesto info@banka.ba)
- **Stvaranje osjećaja hitnosti:** Poruka sadrži zahtjev da odmah reagujete – “Potvrdite svoj račun odmah!” ili “Vaš profil će biti deaktiviran za 24 sata!”
- **Gramatičke greške i loše formatiranje:** Nepravilna struktura rečenica, pogrešan jezik, nedostatak interpunkcije ili zbunjujući sadržaj ukazuju na prevaru
- **Sumnjivi linkovi:** Kada zadržite miš iznad linka, prikazana adresa nije povezana s legitimnim web stranicama
- **Neočekivani dodaci**: Priloženi fajlovi (npr. ZIP, EXE ili nepoznati formati) koje niste tražili ili očekivali

Zadatak za promišljanje

Zavirite u svoj spam folder i pronađite jedan e-mail koji vam djeluje sumnjivo.

Opišite:

- Ko je pošiljalac?
- Šta piše u naslovu i tijelu poruke?
- Da li postoje linkovi ili prilozi?
- Koji elementi čine da sumnjate u njegovu autentičnost?

Prepoznavanje phishing pokušaja nije samo tehničko znanje – to je ključna vještina digitalne pismenosti. Svjesnost, kritičko razmišljanje i oprezno ponašanje mogu spriječiti ozbiljne posljedice. Ako niste sigurni u porijeklo e-maila, bolje je da ga ne otvarate i da ga odmah prijavite IT službi ili označite kao spam. Vaša pažnja je prva linija odbrane.

Kako kreirati sigurnu lozinku?

U digitalnom dobu, lozinke su prva linija odbrane između naših podataka i potencijalnih napadača. Slaba lozinka je kao ostaviti vrata širom otvorena – poziv za neovlašteni pristup vašim nalozima, uređajima i povjerljivim informacijama.

Šta je loša lozinka?

Mnogo korisnika koristi jednostavne lozinke poput 123456, password, qwerty, ili admin jer su brze za unos i lako pamtljive. Nažalost, upravo su one među prvima koje hakeri pokušavaju. Korištenje ličnih informacija, poput imena, prezimena, datuma rođenja ili imena kućnog ljubimca, također je rizično jer se lako mogu pogoditi putem javno dostupnih podataka.

Karakteristike sigurne lozinke

Za snažnu lozinku, preporučuje se:

- Minimalna dužina od 12 karaktera (što duže, to sigurnije)
- Kombinacija velikih i malih slova, brojeva i specijalnih znakova (npr. !, %, @, #)
- Izbjegavanje ponavljanja riječi, uzoraka sa tastature (npr. asdfg) i poznatih izraza

Kreativni savjet

Umjesto nasumičnih nizova slova, koristite fraze koje imaju značenje za vas, ali ih je teško pogoditi. Primjer: Zdravo!Sarajevo_2025% Ova lozinka je dugačka, sadrži više tipova znakova i lako ju je zapamtiti ako ima lični kontekst.

Možete koristiti i tzv. passphrase – niz riječi koje zajedno čine jaku lozinku, poput: MojiPrvi!Koraci@Planine#33

Ukoliko koristite više lozinki, preporučuje se upotreba sigurnog menadžera lozinki, poput Bitwarden, 1Password ili NordPass, koji čuvaju lozinke u šifrovanom obliku.

Zadatak za vježbu

Napravite novu, sigurnu lozinku koristeći preporuke gore. Ne zapisujte je na papirić zalijepljen uz ekran! Umjesto toga, koristite digitalni menadžer lozinki ili zapamtite kroz ličnu asocijaciju.

Razmislite:

- Da li vaša trenutna lozinka ispunjava kriterije sigurnosti?
- Kada ste je posljednji put promijenili?
- Imate li istu lozinku na više servisa?

Lozinka je poput ključa – što je jača i jedinstvenija, to bolje štiti vaš digitalni svijet. Redovna zamjena lozinki, njihova raznolikost i svjesnost o pravilima sigurnosti mogu vas poštedjeti ozbiljnih problema u slučaju napada. Investirajte par minuta u kreiranje kvalitetne lozinke i osigurajte miran san – za vas i vaše podatke.

Dvofaktorska autentifikacija (2FA): Zašto je važna i kako se koristi

U svijetu u kojem se sve više poslovnih i ličnih aktivnosti odvija online, zaštita digitalnih naloga postaje ključna. Lozinka više nije dovoljna da osigura vaš pristup. Cyber napadi, krađe identiteta i upadi u sisteme često se dešavaju zbog kompromitovanih ili predvidljivih lozinki. Tu na scenu stupa dvofaktorska autentifikacija (2FA).

Šta je dvofaktorska autentifikacija?

Dvofaktorska autentifikacija dodaje dodatni sloj zaštite vašem nalogu. Umjesto da se oslanja samo na lozinku (nešto što znate), 2FA zahtijeva i nešto što imate – najčešće jednokratni kod koji dobijete putem SMS-a, mobilne aplikacije (npr. Google Authenticator, Microsoft Authenticator, Authy) ili fizičkog sigurnosnog ključa.

Zamislite to kao dvostruku provjeru identiteta: čak i ako neko sazna vašu lozinku, neće moći pristupiti nalogu bez drugog faktora.

Prednosti korištenja 2FA

- **Zaštita od neovlaštenog pristupa:** Sprječava upade u naloge čak i kada je lozinka ukradena.
- **Smanjenje rizika od phishing napada:** Hakeri teže dolaze do pristupa jer im nedostaje dodatni kod.
- **Povećanje povjerenja klijenata i korisnika:** Sigurni sistemi znače sigurnije poslovanje.

Gdje se koristi 2FA?

Dvofaktorska autentifikacija je dostupna i preporučena u mnogim digitalnim okruženjima:

- E-mail servisi: Gmail, Outlook, Yahoo
- Bankarstvo: Mobilne i online aplikacije za plaćanje i transakcije
- Poslovni alati: CRM sistemi, Slack, Microsoft Teams, ERP platforme
- Cloud servisi: Dropbox, Google Drive, OneDrive
- Platforme za kupovinu: Amazon, eBay, PayPal

Kako aktivirati 2FA?

1. Uđite u podešavanja vašeg naloga
2. Pronađite sekciju „Sigurnost“ ili „Autentifikacija“
3. Aktivirajte 2FA i odaberite način (SMS, aplikacija, sigurnosni ključ)
4. Sačuvajte rezervne kodove u slučaju gubitka pristupnog uređaja

Zadatak za vas

Provjerite da li je 2FA aktivirana na vašem e-mail nalogu. Ako nije, slijedite korake za uključivanje i osigurajte svoj digitalni identitet. Zapišite: Na kojim još aplikacijama biste mogli aktivirati 2FA?

Dvofaktorska autentifikacija je jednostavna, ali izuzetno efikasna mjera koja može značajno smanjiti rizik od cyber napada. Uložite nekoliko minuta i zaštitite ono što je najvrijednije: vaše podatke, komunikaciju i poslovanje.

Redovan backup: Vaša sigurnosna mreža u digitalnom svijetu

U današnje vrijeme kada su naši poslovni i lični podaci sve više oslonjeni na digitalne uređaje, gubitak podataka može imati ozbiljne posljedice. Od tehničkih kvarova i krađe uređaja, pa sve do sofisticiranih napada poput ransomware-a – rizici su brojni. Upravo zato, redovan backup predstavlja osnovni korak u zaštiti vaše digitalne imovine.

Šta je backup?

Backup je sigurnosna kopija vaših važnih datoteka i podataka, koja vam omogućava da u slučaju gubitka ili oštećenja originalnog sadržaja brzo i jednostavno vratite podatke. Bilo da se radi o radnim dokumentima, fotografijama, e-mailovima ili aplikacijama, backup vam daje mirnu savjest da ništa neće biti nepovratno izgubljeno.

Vrste backup-a

Postoje različite metode backup-a koje možete prilagoditi vlastitim potrebama:

- **Lokalni backup** Spremanje podataka na eksterni hard disk, USB stick ili drugo fizičko skladište. Prednost: potpuna kontrola nad podacima. Nedostatak: rizik od fizičkog oštećenja ili krađe uređaja.
- **Cloud backup** Pohranjivanje podataka na internetu putem servisa kao što su Google Drive, OneDrive ili Dropbox. Prednost: pristup s bilo kojeg uređaja i automatska sinhronizacija. Nedostatak: zavisnost od internetske konekcije.
- **Automatski backup softver** Aplikacije kao što su Duplicati, Acronis ili Mac Time Machine omogućavaju zakazano i automatsko pravljenje sigurnosnih kopija bez potrebe za ručnim upravljanjem.
-

Najbolje prakse

- Radite backup najmanje jednom sedmično, a po potrebi i češće – posebno ako često radite na važnim dokumentima.
- Testirajte backup kopije: nije dovoljno da podaci budu sačuvani, važno je da ih možete i uspješno vratiti.
- Koristite kombinaciju lokalnog i cloud backup-a za maksimalnu sigurnost.
- Ne zaboravite backup e-mailova, kontakata, fotografija i konfiguracijskih datoteka softvera.

Zadatak za vas

Provjerite kada ste posljednji put napravili sigurnosnu kopiju važnih dokumenata. Ako je prošlo više od sedmicu dana – vrijeme je da to uradite sada. Razmislite i o automatizaciji tog procesa uz softver koji radi u pozadini.

Backup nije samo tehnički postupak – to je osiguranje vaše digitalne svakodnevice. Ne čekajte da se desi gubitak podataka; uložite nekoliko minuta sedmično i zaštitite ono što vam je važno. Jer kad se dogodi nepredviđeno, backup je ono što pravi razliku između stresa i brzog oporavka.

Ažuriranja softvera:
Vaš prvi štit protiv digitalnih prijetnji

U digitalnom svijetu gdje se prijetnje razvijaju brže nego ikada, ažuriranja softvera više nisu samo dodatak – ona su neophodna zaštita. Redovno ažuriranje softvera predstavlja jednu od najjednostavnijih, a najefikasnijih mjera za očuvanje sigurnosti vaših uređaja, podataka i privatnosti.

Zašto su ažuriranja važna?

Ažuriranja (tzv. update-i) ne donose samo nove funkcije i poboljšanja u performansama. Njihova ključna uloga je otklanjanje sigurnosnih propusta koje hakeri mogu iskoristiti da neovlašteno pristupe vašem sistemu.
Zastarjeli softver je poput otključanih vrata na vašem digitalnom domu – pozivnica za cyber napade.

Primjeri rizika neažuriranog softvera

- Otvaranjem starog Word dokumenta moguće je aktivirati skriveni zlonamjerni kod koji se izvršava bez vašeg znanja
- Neažurirani operativni sistem može omogućiti napadaču da preuzme kontrolu nad uređajem, pristupi vašim fajlovima ili instalira ransomware
- Nezaštićeni web pretraživači postaju meta phishing kampanja i zlonamjernih ekstenzija

Šta treba redovno ažurirati?

Redovno provjeravajte da su svi vaši programi ažurirani, naročito:

- **Operativni sistemi:** Windows, macOS, Linux
- **Internet pretraživači:** Chrome, Firefox, Safari, Edge
- **Antivirusni softver:** Obavezno za zaštitu od malware-a i virusa
- **Aplikacije** koje svakodnevno koristite: e-mail klijenti, uredski paketi, softver za komunikaciju (Teams, Zoom), specijalizirani poslovni alati

Savjet: *Omogućite automatska ažuriranja kad god je to moguće – tako će softver sam instalirati najnovije zakrpe bez vaše intervencije.*

Zadatak za vas

Otvorite podešavanja vašeg uređaja i provjerite:

- Da li su operativni sistem i aplikacije ažurirani?
- Kada je posljednji put instaliran sigurnosni patch?
- Imate li uključenu opciju automatskog ažuriranja?

Zabilježite ove odgovore i postavite podsjetnik za redovne provjere svakih 7 do 14 dana.

Digitalna sigurnost počinje s malim, ali ključnim korakom – ažuriranjem softvera. Svako ažuriranje je zapravo zakrpa kroz koju zatvarate rupu u sistemu i otežavate napadačima da pronađu put do vas. Uložite minut, kliknite na „Update“ i dajte svom uređaju štit koji zaslužuje.

Sigurno korištenje interneta i Wi-Fi mreža: Pametno povežite, mudro zaštitite

U današnje vrijeme brzog pristupa internetu, javne Wi-Fi mreže postale su neizostavan dio svakodnevnice – u kafićima, hotelima, aerodromima i tržnim centrima. Iako praktične, javni Wi-Fi može predstavljati ozbiljan sigurnosni rizik. Podaci koje šaljete ili primate putem takvih mreža mogu lako biti presretnuti od strane cyber kriminalaca.

Zašto je javni Wi-Fi nesiguran?

Javne mreže najčešće nemaju adekvatnu enkripciju i zaštitu, što omogućava napadačima da:

- Prisluškuju vašu komunikaciju i kradu lozinke
- Presretnu osjetljive podatke poput brojeva kartica ili poslovnih dokumenata
- Simuliraju lažne Wi-Fi mreže („evil twin“) kako bi vas prevarili i dobili pristup vašem uređaju

Pravila sigurnog ponašanja na internetu

Da biste umanjili rizik i zaštitili svoju privatnost, primijenite sljedeće savjete:

- Izbjegavajte osjetljive aktivnosti putem javnog Wi-Fi-a. Ne prijavljujte se na bankovne, poslovne ili druge osjetljive naloge dok ste povezani na javnu mrežu.
- Koristite VPN (Virtual Private Network) VPN šifrira vaš internet saobraćaj i stvara siguran kanal između vašeg uređaja i interneta – odlična zaštita kada ste na nepoznatim mrežama.
- Isključite automatsko povezivanje na Wi-Fi mreže Vaš uređaj se može automatski spojiti na nesigurne mreže bez vašeg znanja. Onemogućite ovu opciju u podešavanjima.
- Preferirajte mobilnu mrežu Kada je sigurnost prioritet, mobilni internet (4G/5G) je sigurnija opcija od otvorenih Wi-Fi mreža.
- Redovno ažurirajte uređaje i aplikacije Sigurnosne zakrpe i update-i mogu spriječiti iskorištavanje poznatih ranjivosti.

Zadatak za vas

Otvorite postavke Wi-Fi na svom telefonu, laptopu ili tabletu i provjerite:

- Da li je uključena opcija automatskog povezivanja na mreže?
- Imate li instaliran i aktivan VPN alat?
- Koristite li mogućnost obavijesti pri povezivanju na nepoznatu mrežu?

Ako ste odgovorili „da“ na automatsko povezivanje – vrijeme je da tu postavku isključite radi sigurnosti.

Korištenje interneta treba biti praktično, ali prije svega sigurno. S nekoliko jednostavnih koraka možete zaštititi svoje podatke, komunikaciju i uređaje od neželjenih pogleda. Javni Wi-Fi neka bude kratkoročno rješenje, a ne stalna praksa. Vaša digitalna privatnost ovisi o vašim svakodnevnim navikama – zato ih učinite mudrim.

Kako zaštititi mobilni uređaj: Vaš džepni trezor

U današnjem svijetu, mobilni telefon nije samo sredstvo komunikacije – to je lični i poslovni digitalni centar. Sadrži e-mailove, kontakte, dokumente, aplikacije, fotografije i često i pristup bankovnim računima. Zbog toga je njegova zaštita ključna, ne samo za privatnost već i za sigurnost poslovanja.

Zašto je važno štititi mobilni uređaj?

Mobilni telefoni su česte mete napada zbog ogromne količine osjetljivih informacija koje sadrže. Gubitak, krađa ili kompromitacija uređaja može imati:

- Pristup povjerljivim dokumentima
- Neovlaštene finansijske transakcije
- Krađu identiteta ili zloupotrebu korisničkih računa

Osnovne mjere zaštite

Primijenite sljedeće sigurnosne korake da zaštitite svoj uređaj:

- **Zaključavanje ekrana** Koristite PIN, lozinku, otisak prsta ili prepoznavanje lica kako biste spriječili neovlašteni pristup.
- **Preuzimajte aplikacije samo iz provjerenih izvora** Google Play i App Store imaju sigurnosne mehanizme – aplikacije iz nepoznatih izvora mogu sadržavati malware.
- **Aktivirajte funkciju „Find My Device“** ili sličnu U slučaju gubitka ili krađe, moći ćete locirati, zaključati ili obrisati podatke s uređaja na daljinu.
- **Šifrirajte podatke na uređaju** Većina modernih telefona ima opciju enkripcije – uključite je kako bi svi podaci bili dodatno zaštićeni.
- **Ne otvarajte sumnjive linkove i privitke** Phishing napadi sve češće ciljaju mobilne korisnike putem SMS-a, e-maila i društvenih mreža.

Napredne postavke privatnosti

- Pregledajte dozvole aplikacija: Provjerite koje aplikacije imaju pristup mikrofonu, kameri, lokaciji i kontaktima – onemogućite nepotrebne.
- Isključite Bluetooth i lokaciju kada ih ne koristite.
- Redovno ažurirajte sistem i aplikacije radi zaštite od poznatih sigurnosnih propusta.

Zadatak za vas

Uđite u postavke telefona i provjerite sljedeće:

- Da li je aktivirano zaključavanje ekrana?
- Koje aplikacije imaju pristup mikrofonu, kameri i kontaktima?
- Da li je opcija „Find My Device“ uključena?

Ako otkrijete da je neka od ovih opcija neaktivna – aktivirajte je odmah. Vaša sigurnost počinje s vašom pažnjom.

Mobilni telefon je više od uređaja – to je proširenje vašeg digitalnog identiteta. Bez odgovarajuće zaštite, izložen je rizicima koji mogu ugroziti privatnost i sigurnost. Uzmite nekoliko minuta i osigurajte da vaš džepni trezor zaista ostane neprobojan.

Osnove sigurnog korištenja e-maila: Pametno klikni, sigurno komuniciraj

E-mail je temeljni alat savremene poslovne komunikacije. Pomaže nam da šaljemo poruke, dijelimo dokumente i obavljamo svakodnevne zadatke. No, upravo zbog svoje široke upotrebe, e-mail je i jedan od najčešćih vektora cyber napada. Napadači koriste lažne poruke, privitke i linkove kako bi prevarili korisnike, ukrali podatke ili instalirali zlonamjerni softver.

Koje prijetnje dolaze putem e-maila?

- **Phishing** – poruke koje izgledaju kao da dolaze iz pouzdanih izvora, a zapravo vas navode da otkrijete lozinke, kliknete na zlonamjerne linkove ili preuzmete štetan sadržaj
- **Malware putem privitaka** – Word, PDF ili ZIP datoteke koje sadrže skriveni zlonamjerni kod
- **Spoofing** – manipulacija e-mail adresama pošiljaoca tako da izgledaju poznato i pouzdano

Savjeti za sigurnu upotrebu e-maila

Zaštitite sebe i svoj tim primjenom ovih osnovnih pravila:

- Ne otvarajte sumnjive privitke ili linkove, čak ni od osoba koje poznajete ako poruka djeluje neuobičajeno (npr. „Hitno! Pogledaj ovo odmah!“)
- Nikada ne šaljite lozinke putem e-maila – za dijeljenje osjetljivih informacija koristite sigurne komunikacione kanale
- Provjerite adresu pošiljaoca – klikom na ime možete vidjeti stvarnu e-mail adresu (često se kriju sumnjive domene poput @secure-mail.net umjesto službene domene)
- Obratite pažnju na pravopis i ton poruke – mnoge lažne poruke sadrže gramatičke greške i neobične zahtjeve
- Koristite dvofaktorsku autentifikaciju (2FA) za pristup svom e-mail nalogu kako biste dodatno zaštitili svoj račun

Zadatak za vas

Otvorite svoj inbox i potražite e-mail koji vam djeluje sumnjivo. Analizirajte sljedeće:

- Ko je pošiljalac i je li adresa autentična?
- Da li poruka ima neuobičajen ton, pravopisne greške ili hitne zahtjeve?
- Sadrži li linkove ili privitke koji vam nisu poznati?

Zapišite ili podijelite s kolegom što taj e-mail čini opasnim i kako biste reagovali da ga dobijete ponovo.

Sigurno korištenje e-maila počinje sa sviješću i oprezom. Jedan nepromišljen klik može ugroziti čitav sistem. Prije nego što otvorite privitak, kliknete na link ili odgovorite – zastanite, razmislite i procijenite. Vaša informacija je vrijedna, zato je štitite kao profesionalac.

Kako reagovati u slučaju sigurnosnog incidenta: Smireno, efikasno, odgovorno

U digitalnom okruženju, sigurnosni incidenti se mogu dogoditi svakome – od sumnjivog e-maila i neobične aktivnosti na računaru, do otkrivanja zlonamjernog softvera ili neovlaštenog pristupa. Ključ uspješne reakcije je brzina, smirenost i koordinacija. Pravilan odgovor može spriječiti širenje štete, zaštititi podatke i pomoći u identifikaciji uzroka.

Šta je sigurnosni incident?

Incident može biti bilo koji događaj koji ugrožava sigurnost podataka, uređaja ili korisnika. Primjeri uključuju:

- Otkriće zlonamjernog softvera (ransomware, trojanac, keylogger)
- Neautorizovan pristup korisničkim računima
- Gubitak uređaja s osjetljivim podacima
- Sumnjiva aktivnost u e-mailu, mreži ili aplikacijama

Kako postupiti korak po korak

1. **Izolirajte uređaj** Odmah isključite zaraženi ili kompromitovani uređaj sa mreže (internet i lokalna mreža). Time se sprječava daljnje širenje potencijalne prijetnje.
2. **Obavijestite nadležnu osobu ili IT podršku** Ne pokušavajte sami rješavati situaciju ako niste stručnjak. Kontaktirajte IT tim, sigurnosnog oficira ili odgovornu osobu za incidente u vašoj organizaciji.
3. **Ne preduzimajte neovlaštene radnje** Ne brišite datoteke, ne pokrećite antivirus na svoju ruku i ne mijenjajte konfiguraciju sistema – time možete nehotice uništiti dokaze ili pogoršati situaciju.
4. **Zabilježite sve relevantne informacije** Napravite kratak zapis: šta ste primijetili, kada, kako ste reagovali i ko je bio uključen. Ovaj zapis pomaže IT timu u analizi i prijavi incidenta ako je potrebno.
5. **Obavijestite nadređene ako je incident ozbiljan** U situacijama koje uključuju osjetljive podatke (npr. informacije klijenata, finansijske dokumente), važno je obavijestiti rukovodstvo i slijediti internu politiku o informisanju.

Preventivne mjere koje olakšavaju reakciju

- Održavajte redovne sigurnosne treninge
- Upoznajte se s internim procedurama za upravljanje incidentima
- Osigurajte da svi zaposleni znaju koga kontaktirati u kriznim situacijama

Zadatak za vas

Napravite lični plan reagovanja:

- Koga biste prvo kontaktirali u firmi ako sumnjate na incident?
- Gdje možete pronaći kontakt IT podrške?
- Koji su naredni koraci prema internim pravilima?

Zapišite odgovore i držite ih dostupnima – na vašem radnom mjestu, u telefonu ili e-mailu, tako da u slučaju hitnosti ne gubite dragocjeno vrijeme.

Reagovati na sigurnosni incident ne znači paničariti – znači prepoznati problem, izolovati prijetnju i obavijestiti stručne osobe. Brza, koordinirana i smirena reakcija može biti razlika između manjeg tehničkog izazova i ozbiljnog gubitka podataka. Budite spremni – jer sigurnost počinje informisanošću.

Ko je odgovoran za sigurnost? Odgovor: Svi!

U savremenom digitalnom okruženju, cyber sigurnost više nije isključiva nadležnost IT sektora. Od trenutka kada uključimo računar, pristupimo e-mailu ili kliknemo na link — svi mi postajemo aktivni učesnici u zaštiti digitalne imovine organizacije.

Cyber napadi se sve češće oslanjaju na ljudsku grešku, nepažnju ili nedovoljno znanje zaposlenih. Zbog toga je kolektivna odgovornost temelj svakog održivog i sigurnog poslovnog okruženja.

Ko nosi koji dio odgovornosti?

Menadžeri i rukovodioci

- Definišu sigurnosne politike i procedure
- Osiguravaju resurse za edukaciju i alate za zaštitu
- Potiču sigurnosnu kulturu kroz primjer i komunikaciju

Zaposleni na svim nivoima

- Poštuju sigurnosne smjernice i interne pravilnike
- Pažljivo postupaju s osjetljivim informacijama
- Odmah prijavljuju sumnjivu aktivnost ili nesigurne situacije

IT administratori i tehnički timovi

- Implementiraju i održavaju sigurnosne mjere
- Upravljaju pristupima, sistemima i alatima
- Reaguju na incidente i prate moguće prijetnje

Poruka je jasna: Svaki klik, poruka ili odluka može pomoći u očuvanju sigurnosti — ili je ugroziti.

Kako doprinositi sigurnosti na svom radnom mjestu?

- Redovno se edukujte o najnovijim prijetnjama i sigurnosnim praksama
- Ne dijelite lozinke — čak ni kolegama
- Koristite jake lozinke i uključite dvofaktorsku autentifikaciju
- Ne ignorišite sumnjive e-mailove ili ponašanje uređaja — reagujte odmah
- Pratite interne procedure za prijavu incidenata

Zadatak za vas

Razgovarajte sa svojim kolegama:

- Znaju li kome se obratiti ako primijete nešto sumnjivo?
- Gdje se nalazi dokument s internim sigurnosnim kontaktima?
- Da li tim zna koje korake treba preduzeti u slučaju digitalnog incidenta?

Zapišite odgovore, osvježite ih ako je potrebno — jer brza reakcija počinje jasnim informacijama.

Cyber sigurnost je timski sport. Svako u organizaciji ima svoju ulogu, a zajednički cilj je isti: zaštita podataka, korisnika i sistema. Kad svi preuzmemo odgovornost, organizacija postaje otpornija na prijetnje, spremnija za izazove i sigurnija za sve.

Uloga menadžmenta i zaposlenih u jačanju sigurnosne kulture

U današnjem digitalno povezanom poslovnom okruženju, cyber sigurnost više nije isključiva briga IT sektora – ona je kolektivna odgovornost svakog pojedinca unutar organizacije. Ključna uloga u oblikovanju sigurnosne svijesti i ponašanja zaposlenih pripada upravo menadžmentu.

Ako je sigurnost jasno prepoznata kao strateški prioritet – kroz politiku, obuku i svakodnevnu komunikaciju – zaposlenici će je ozbiljnije shvatiti i u skladu s tim postupati.

Menadžment: lideri sigurnosne kulture

- Postavljaju pravila i definiraju standarde sigurnosnog ponašanja
- Osiguravaju sredstva za edukaciju i tehnološku zaštitu
- Potiču transparentnost i otvorenu komunikaciju o sigurnosnim rizicima
- Vode primjerom u primjeni sigurnosnih mjera

Sigurnost počinje s vrha – kada menadžment demonstrira odgovornost, zaposleni slijede taj primjer.

Zaposleni: prvi red odbrane

- Primjenjuju sigurnosne smjernice u svakodnevnom radu
- Prepoznaju i prijavljuju sumnjive situacije ili potencijalne prijetnje
- Brinu o svojim pristupnim podacima, uređajima i e-mailovima
- Aktivno se uključuju u sigurnosne obuke i testiranja

Dobre prakse koje grade otpornu organizaciju

- **Obuka prilikom zapošljavanja** Uvođenje novozaposlenih u osnove digitalne sigurnosti od prvog dana
- **Povremeni testovi i simulirani napadi** Provjera reakcije i spremnosti zaposlenih na potencijalne prijetnje (npr. phishing simulacije)
- **Prepoznavanje pozitivnog ponašanja** Nagrađivanje pojedinaca koji prijave ranjivosti, predlože poboljšanja ili se istaknu u obukama
- **Kontinuirano usavršavanje** Redovna edukacija kroz prezentacije, radionice i digitalne materijale

Zadatak za vas

Predložite menadžmentu da uvede "10 minuta sigurnosti" u mjesečne sastanke. To može biti kratka prezentacija, analiza slučaja ili podsjetnik na aktuelne prijetnje. Na ovaj način, sigurnost ostaje svježa tema i postaje dio organizacijske rutine.

Jačanje sigurnosne kulture je proces koji zahtijeva angažman svih nivoa organizacije. Menadžment postavlja temelje, ali pravi uspjeh dolazi kada svaki zaposleni prepozna svoju ulogu i aktivno doprinosi sigurnosti. Zajedno čuvamo podatke, povjerenje i ugled naše organizacije.

Checklist: Da li je vaša firma spremna za cyber izazove?

Cyber sigurnost više nije rezervisana samo za IT sektor – ona je sastavni dio poslovanja svake moderne organizacije. Bilo da ste mala firma, startup ili međunarodna kompanija, određeni elementi zaštite moraju biti ugrađeni u vašu svakodnevnu praksu. Ova lista služi kao brza samoprocjena sigurnosne zrelosti vaše firme.

Osnovni elementi digitalne zaštite

- ☐ **Koristimo dvofaktorsku autentifikaciju (2FA)** Dodatni sloj zaštite za korisničke naloge putem SMS-a, aplikacije ili sigurnosnog ključa.
- ☐ **Svi uređaji su ažurirani i zaštićeni lozinkom** Aktivna zaštita uz jake lozinke i redovno ažuriranje softvera smanjuje rizik od napada.
- ☐ **Postoji plan reagovanja u slučaju sigurnosnog incidenta** Definisan tok koraka, kontakt osobe i procedure za brzo djelovanje u kriznoj situaciji.
- ☐ **Redovno pravimo backup-e i znamo kako ih vratiti** Sigurnosne kopije kritičnih podataka čuvamo lokalno i u oblaku, s redovnim testiranjem oporavka.
- ☐ **Zaposleni su informisani o osnovama sigurnosti** Obuka, interni vodiči i podsjetnici o opasnostima poput phishinga, loših lozinki i upotrebe javnih mreža.

Napomena: Idealno je da se ova lista popunjava zajedno sa sigurnosnim timom ili menadžmentom. Svaka označena stavka predstavlja jednu prepreku manje za potencijalne napadače.

Zadatak za tim

Razgovarajte sa kolegama, menadžmentom i IT podrškom:

- Šta već imamo na ovoj listi?
- Gdje postoje rupe ili nejasnoće u primjeni?
- Ko može preuzeti odgovornost za unapređenje preostalih stavki?

Možda će vam trebati dodatni alati, edukacija ili promjena u internim procedurama – važno je da se koraci preduzmu proaktivno.

Bez obzira na veličinu tima ili sektor poslovanja, sigurnosna pripremljenost je ključna. Ova checklista vam pomaže da razjasnite prioritete, identifikujete slabosti i ojačate ukupnu otpornost na digitalne prijetnje.

Kratki test znanja iz oblasti cyber sigurnosti

Testirajte svoje poznavanje ključnih principa digitalne zaštite. Ako niste sigurni u odgovor – ne brinite! Cilj je učenje, a za dodatnu pomoć vratite se na odgovarajući dio sigurnosnog vodiča.

Pitanja

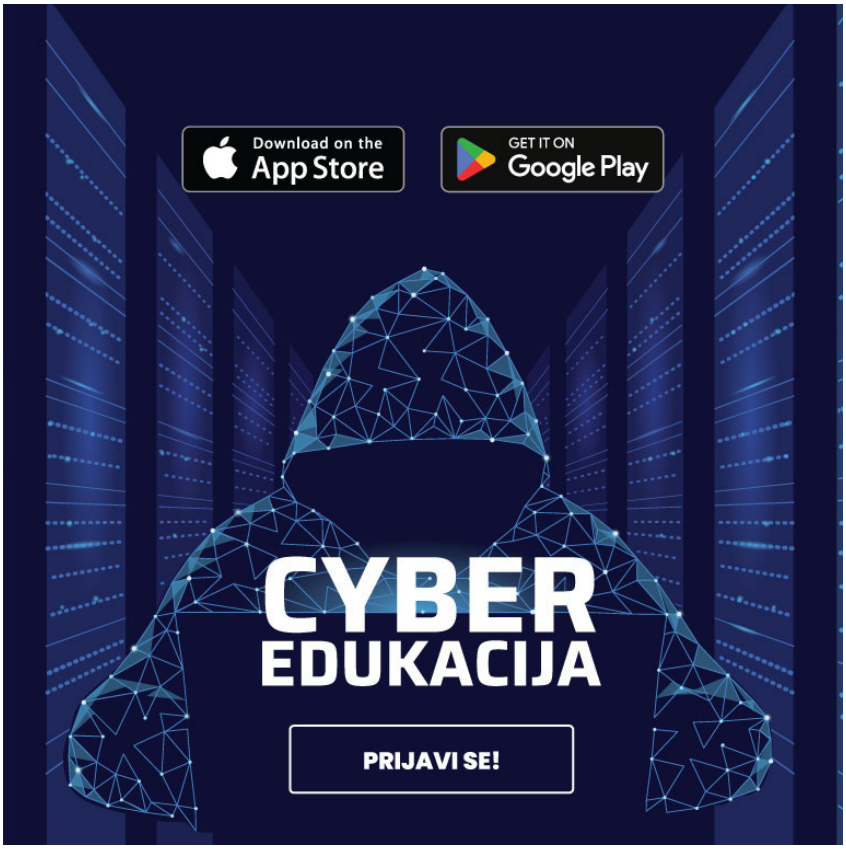
1. **Šta je phishing?** Objasnite kako izgledaju lažne poruke koje pokušavaju izvući vaše podatke.
2. **Zašto je važno redovno ažurirati softver?** Koje sigurnosne rizike možete izbjeći pravovremenim update-ima?
3. **Šta znači dvofaktorska autentifikacija (2FA)?** Kako dodatni sloj zaštite štiti vaš korisnički nalog?
4. **Kako izgleda snažna lozinka?** Navedite karakteristike koje čine lozinku otpornom na hakovanje.
5. **Da li je javni Wi-Fi siguran za poslovnu komunikaciju?** Kada ga izbjegavati i koje su alternative?
6. **Kako se ponašati u slučaju digitalnog napada ili incidenta?** Koji su prvi koraci koje treba preduzeti?
7. **Ko je odgovoran za sigurnost unutar firme?** Da li postoji jedinstvena osoba ili je to zajednička odgovornost?
8. **Koliko često treba praviti sigurnosne kopije (backup)?** Koji ritam je preporučen u profesionalnom okruženju?
9. **Kako prepoznati sumnjiv e-mail?** Navedite barem tri znaka koji mogu ukazivati na pokušaj prevare.
10. **Gdje možete dalje učiti o cyber sigurnosti?** Preporučite interne vodiče, online resurse ili sigurnosne treninge.

Zadatak za vas

Odgovorite na sva pitanja iskreno i samostalno. Ako ste sigurni – bravo, vaše znanje je na visokom nivou! Ako ste neodlučni ili ne znate – vratite se na odgovarajuću stranicu vodiča, edukujte se i zabilježite ono što ste naučili.

Napomena: Ovaj test nije ocjena – to je alat za razvoj. Svaka osoba u firmi igra ulogu u zaštiti podataka, uređaja i reputacije. Znanje = sigurnost.

Šta dalje? Gdje učiti više?



Udruženje
e-Transformacija

https://e-transformacija.ba/

Ova publikacija je objavljena u sklopu implementacije projekta Cyber Security education program a u okviru SEDEP programa, koji sufinansiraju Njemačko savezno ministarstvo za ekonomsku saradnju i razvoj (BMZ), Evropska unija i Švicarska vlada. Sadržaj ove publikacije isključiva je odgovornost Udruženja e-Transformacija i ne odražava nužno stavove njemačke vlade, švicarske vlade ili Evropske unije.