Sveučilište u Zagrebu
Fakultet organizacije i informatike
Varaždin

Osnove kibernetičke higijene

Mario Harjač,
koordinator za kibernetičku sigurnost

Osnove kibernetičke higijene

Kibernetička higijena odnosi se na skup svakodnevnih digitalnih navika koje pomažu u zaštiti osobnih podataka, uređaja i računa od raznih kibernetičkih prijetnji. Kao što redovita briga o osobnoj higijeni čuva naše fizičko zdravlje, tako i kibernetička higijena štiti naše digitalno okruženje.

U praksi to znači odgovorno ponašanje prilikom korištenja interneta i tehnologije – redovito ažuriranje operacijskog sustava i programa, korištenje snažnih i jedinstvenih lozinki te oprez pri otvaranju sumnjivih poruka i privitaka. Dobar dio kibernetičke higijene čini i korištenje dvostupanjske autentikacije te izrada sigurnosnih kopija važnih podataka, kako bi se smanjile posljedice mogućih incidenata.

Održavanjem dobre kibernetičke higijene smanjuje se rizik od zaraze zlonamjernim programima, krađe identiteta ili financijskih prijevara. Ona ne zahtijeva napredno tehničko znanje – dovoljno je razviti svijest o sigurnom ponašanju i dosljedno primjenjivati osnovna pravila zaštite u svakodnevnom radu i komunikaciji.

Kibernetička higijena, jednostavno rečeno, predstavlja temelj osobne i organizacijske sigurnosti u digitalnom svijetu.

“Basic cyber hygiene prevents 99% of attacks”

Izvor: https://www.microsoft.com/en-us/security/security-insider/risk-management/risk-management-hygiene-guide

Sadržaj

- Upravljanje lozinkama
- Dvostupanjska autentikacija
- Sigurnosno kopiranje (Backup)
- Sigurnost računala (ažuriranja, AV, kriptiranje diska, zaključavanje biosa, admin prava)
- Slanje/čuvanje povjerljivih podataka
- VPN
- Kako prepoznati phishing napade

Što je lozinka?

Lozinka je osobna tajna koju koristimo za prijavu na svoje račune – poput e-pošte, društvenih mreža ili internetskog bankarstva. Ona se sastoji od kombinacije slova, brojeva i simbola te služi kao ključ koji nas štiti od neovlaštenog pristupa. Dobra lozinka pomaže čuvati naše podatke, fotografije i druge važne informacije od hakera i znatiželjnih pogleda.

Baš kao što zaključavamo vrata svog doma, tako i lozinkom „zaključavamo” svoje digitalne prostore. Zato je važno da lozinke budu dovoljno jake, jedinstvene i poznate samo nama.

Kako treba izgledati dobra lozinka?

Svi smo čuli preporuke da dobra lozinka mora sadžavati:

- Minimalna duljina 8 znakova
- Najmanje jedno malo slovo
- Najmanje jedno veliko slovo
- Najmanje jedan broj
- Najmanje jedan poseban znak
- Ne smije biti korištena uobičajena riječ
- Treba se promijeniti svakih 90 dana

Ove smjernice obajvljene su 2004. godine u dokumentu “NIST Special Publication 800-63”.

Kako (ne)treba izgledati dobra lozinka?

Ako primijenimo prethodne smjernice obično naša lozinka izgleda ovako nekako:

Proljece8!

Kako treba izgledati dobra lozinka?

Autor ovih smjernica je g. Bill Burr koji je kasnije izjavio: “Much of what I did I now regret.”

(izvor: https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118)

Ovakve lozinke stvorile su nove probleme:

- Svi izmišljaju lozinke na sličan način
- Teško su pamtljive
- Zapisuju se na papiriće
- Kod obveznih promjena promijeni se samo jedan znak
- Za sve se koristi ista lozinka

Kako treba izgledati dobra lozinka?

2024. godine objavljena je nova verzija preporuka (Second Public Draft of NIST SP 800-63B-4) gdje se stavlja veći naglasak na duljinu lozinke nego na kompleksnost:

- **Minimalna duljina 15 znakova** (do 64 znaka)
- Svi znakovi (uključujući razmak i hrvatske dijaktičke znakove)
- **Promjena samo u slučaju kompromitacije**
- Pružatelj usluge treba ograničiti broj pokušaja prijave

Kako treba izgledati dobra lozinka?

Preporuke također definiraju što ne bi trebalo:

- Dopustiti upotrebu poznatih/popularnih lozinki
- Tražiti nepotrebnu kompleksnost
- Zahtijevati periodičke promjene
- Koristiti “sigurnosna pitanja”
- Pružatelji usluga ne bi trebali skračivati lozinke prilikom spremanja

Što učiniti u praksi?

- Minimalna duljina 16 znakova (velika i mala slova, znakovi, brojke)
  - Kompleksnost nije nužna, no nije ni na odmet.
  - Kao pomoć možete koristiti generatore: https://sysportal.carnet.hr/passgen
- Koristite “autentikacijske fraze” duljine 7 riječi (passphrases)
  - Umjesto jedne riječi možete koristiti fraze od nekoliko riječi (5 ili više).
  - Preporuka je da to nisu poznate izreke ili refreni pjesama već da koristite nasumično odabrane riječi (npr.: strangely previous bruising accurate polyester saddlebag botch).
  - Također možete koristiti generatore: https://diceware.rempe.us/#eff

Što učiniti u praksi?

- **NE KORISTITE ISTE LOZINKE VIŠE PUTA** (za različite aplikacije)
  - Izrazito je važno da se pridržavate ovog pravila i da svaka lozinka bude jedinstvena. U slučaju kompromitacije jedne aplikacije napadač može iskoristiti dobivenu lozinku za prijavu na druge aplikacije.
  - Kako bi provjerili je li Vaša lozinka jedinstvena ili je “procurila” na internetu možete koristiti: https://haveibeenpwned.com
- **Ne koristite osobne podatke u lozinkama**
  - “IvanHorvat1963!” nije dobra loznika :)

Što učiniti u praksi?

- Koristite upravitelje lozinkama (password managere) za spremanje.
  - S obzirom na zahtjev da svaka lozinka mora biti jedinstvena, potrebno je koristiti specijalizirane alate za spremanje (nije ih moguće sve zapamtiti).
  - Primjeri ovakvih alata su:
    - Google Password Manager (https://passwords.google.com/)
    - KeePassXC (https://keepassxc.org/)
    - Bitwarden (https://bitwarden.com/)

Što učiniti u praksi?

- **Korisite dvostupanjsku autentifikaciju**
  - Nešto više o ovoj temi u nastvaku.
- Na šaljite lozinke mailom/porukama
  - Za razmjenu lozinki postoje specijalizirani alati kao što je Bitwarden Send (https://bitwarden.com/products/send/).
- **Ne dijelite lozinke s drugima** (**nikada i bez iznimke**)

Korisnički računi na FOI-u

Za pristup uslugama FOI-a (kao što su FOI Nastava, Moodle, Google Workspace i sl.) koristimo samo jedan korisnički račun (elektronički identitet) koji se kreira prilikom zapošljavanja, odnosno upisa. Ovaj korisnički račun dio je AAI@EduHr sustava (https://www.aaiedu.hr/o-sustavu) što nam omogućava prijavu i na druge sustave Sveučilišta ili neke druge akademske institucije (npr. ISVU).

Svoju AAI@Edu lozinku možete promijeniti na:
https://secure.foi.hr/ldap/user

Upravitelji lozinkama - KeepassXC

KeePassXC je **open source** projekt – to znači da je njegov izvorni kod javno dostupan i da ga zajednica može nadograđivati i provjeravati.

Glavna značajka je da se **lozinke pohranjuju isključivo lokalno** na korisnikovom uređaju, bez čuvanja na udaljenim serverima. To može biti prednost (više kontrole, manji rizik od centralnih proboja) ali i nedostatak (ako dođe do kvara ili gubitka uređaja; potreban backup).

KeePassXC podržava **plug-in za web preglednike**, što omogućuje automatsko ispunjavanje lozinki izravno u pregledniku. Također, postoji i verzija za Android – također **open source** – koja omogućuje korištenje iste baze lozinki na mobilnom uređaju.

https://keepassxc.org/

Upravitelji lozinkama - Bitwarden

Bitwarden je popularan upravitelj lozinki koji je **besplatan za osobnu upotrebu**, a nudi i **premium verziju** s dodatnim funkcionalnostima po vrlo pristupačnoj cijeni (oko 10 USD godišnje). Riječ je o **djelomično open source** rješenju, čiji je kod djelomično otvoren i redovito prolazi **neovisne sigurnosne revizije** koje provode treće strane (više na službenim stranicama).

Jedna od glavnih prednosti Bitwardena jest da se **lozinke dekriptiraju isključivo u klijentskoj aplikaciji**, odnosno u pregledniku ili mobilnoj aplikaciji korisnika. To znači da ni Bitwardenovi serveri nemaju pristup stvarnim lozinkama, čime se dodatno povećava sigurnost.

Bitwarden omogućuje **sinkronizaciju lozinki među različitim uređajima**, što korisnicima olakšava pristup podacima bilo gdje. Osim klasičnog rada s lozinkama, podržava i **Passkey tehnologiju**, omogućujući jednostavniju i sigurniju prijavu na moderne web servise.

https://bitwarden.com

Što je Passkey?

Passkey je nova, sigurnija i jednostavnija zamjena za lozinke. Umjesto da korisnici moraju pamtiti i unositi nizove znakova, passkey koristi naprednu tehnologiju temeljenu na **kriptografiji javnog ključa**. Ova tehnologija omogućuje da se korisnik prijavi na račun ili uslugu bez potrebe za klasičnom lozinkom.

Passkey standard razvijen je u sklopu inicijative **FIDO Alliance**, u kojoj sudjeluju najveće tehnološke tvrtke poput Googlea, Microsofta, Amazona, Facebooka, PayPala i Cisca. Danas ga podržavaju gotovo svi važni **operativni sustavi** i **internetski preglednici**.

Ključevi koji omogućuju prijavu pohranjuju se sigurno na uređaju korisnika – računalu, mobitelu ili čak u specijaliziranom **upravitelju lozinkama** poput Bitwardena. Tijekom prijave **privatni ključ** nikada se ne šalje putem interneta, što dodatno povećava sigurnost.

Za mobilne uređaje, passkey koristi **Bluetooth vezu** kako bi potvrdio da je korisnik fizički prisutan u trenutku prijave. Zahvaljujući ovakvom pristupu, passkey se smatra ne samo sigurnijim, već i jednostavnijim za korištenje od tradicionalnih lozinki.

Dodatne informacije

- How to use a Password Manager: https://www.youtube.com/watch?v=ugeLoJNjfPk
- NIST Password Guidelines Made Easy | Password Security Tips: https://www.youtube.com/watch?v=e_NecL4-OMU
- Have I Been Pwned Review - Legit or Scam Platform: https://www.youtube.com/watch?v=MqHiyx95-Sc
- Nešto više o Passkeyu: https://safety.google/authentication/passkey/
- Popis usluga/stranica koje podržavaju Passkey: https://passkeys.directory/
- Testna stranica: https://passkeys.eu

Dvostupanjska autentifikacija (2FA)

Dvostupanjska autentikacija, poznata i kao **2FA (two-factor authentication)**, dodatna je zaštita koja čuva naše račune čak i ako netko sazna našu lozinku. Osim što unosimo lozinku, traži se i drugi način potvrde identiteta – najčešće **jednokratni kod** koji dobijemo SMS-om, putem **autentifikacijske aplikacije** ili pomoću **sigurnosnog ključa**.

Ovaj dodatni korak značajno smanjuje rizik od neovlaštenog pristupa, jer napadač ne može ući u račun bez oba dijela provjere. Dvostupanjska autentikacija jednostavan je, ali vrlo učinkovit način da povećamo sigurnost svojih digitalnih identiteta.

Dvostupanjska autentifikacija (2FA)

Često se ovakva dodatna provjera vrši na jedan od načina:

- Mailom
- SMS-om
- Kroz mobilne aplikacije (npr. Certilia)
- Hardverski uređaji (https://www.yubico.com/products/yubikey-5-overview/)
- Passkey

Dvostupanjska autentifikacija (2FA)

- Vremenski ograničene jednokratne lozinke (TOTP)
  - Google Authenticator (https://www.youtube.com/watch?v=seyOjyJGsxY)
  - Authy (https://www.authy.com)

Kod upotrebe dvostupanjske autentikacije potrebno je dodatno obratiti pažnju kako ne bi izgubili mogućnost prijave zbog npr. gubitka mobitela na kojem Vam se nalazi TOTP generator ili sl.

Sigurnosno kopiranje (Backup)

Schofield's Second Law of Computing:

> **“Data doesn't really exist unless you have at least two copies of it.”**

Izvor: https://www.zdnet.com/article/follow-schofields-three-laws-of-computing-and-avoid-disasters/

Sigurnosno kopiranje (backup)

Izrada sigurnosnih kopija podataka (**backup)**, jedan je od najvažnijih koraka u zaštiti osobnih i poslovnih informacija. Najpoznatije pravilo za sigurnu pohranu podataka je takozvana **3-2-1 strategija**.

Prema tom pristupu, potrebno je imati **tri kopije podataka**: jednu glavnu i **dvije sigurnosne**. Te kopije trebaju biti pohranjene na **najmanje dva različita medija** – primjerice, na tvrdom disku računala i na vanjskom disku ili NAS uređaju. Osim toga, **jedna kopija mora biti dislocirana**, odnosno čuvana na drugoj lokaciji (primjerice u oblaku ili kod druge osobe), kako bi bila sigurna u slučaju fizičkog oštećenja (požar, poplava i sl.) ili krađe uređaja.

Važno je da sigurnosna kopija ima i **“vremensku komponentu”** – znači da se čuva više verzija datoteka kroz vrijeme, što omogućuje povratak na stariju verziju ako dođe do pogreške ili zlonamjerne izmjene.

Treba naglasiti da **sinkronizacija datoteka u oblaku nije isto što i sigurnosna kopija** – ako se datoteka slučajno izbriše ili ošteti, ta promjena se često automatski prenese i u oblak. Zato je klasični backup i dalje nezamjenjiv dio dobre sigurnosne prakse.

Na kraju, **sigurnosne kopije treba redovito provjeravati** – testirati da se mogu otvoriti i vratiti – jer neispravan backup ne vrijedi ništa kad je najpotrebniji.

Sigurnosno kopiranje (Backup)

Sigurnosne kopije mogu se izrađivati na **različitim razinama**, ovisno o potrebama i tehničkom znanju korisnika:

- **Na razini diska** – radi se **kopija cijelog diska**, odnosno svih blokova podataka. Ova metoda omogućuje potpunu obnovu sustava u slučaju ozbiljnog kvara, ali zahtijeva više prostora za pohranu.
- **Na razini operacijskog sustava** – izrađuje se **backup datoteka i postavki** iz samog sustava, što olakšava vraćanje računala u prethodno stanje bez potpunog reinstaliranja.
- **Na razini datoteka** – najjednostavniji oblik sigurnosne kopije, gdje se kopiraju samo odabrane mape i dokumenti, poput fotografija, radnih datoteka ili važnih projekata.

Podaci se mogu pohraniti na različitim mjestima, ovisno o željenoj razini sigurnosti:

- U oblaku (primjerice OneDrive, Google Drive, Dropbox i slične usluge).
- Na lokalnoj mreži, primjerice pomoću NAS uređaja (Network Attached Storage).
- Lokalno, na vanjskom disku ili USB memoriji.

Kombiniranjem više rješenja i lokacija dobiva se veća pouzdanost i otpornost na gubitak podataka, što je i cilj svake dobre backup strategije.

Sigurnosno kopiranje (Backup) - Alati

U nastavku su opisani neki alati s kojima možete napraviti sigurnosno kopiranje podataka na svojim računalima:

- Windows backup
  - Backup podataka i postavki na OneDrive (potreban account)
- Backup and Restore (Windows 7)
  - Backup na vanjski disk
  - Mogućnost izrade slike sustava (na razini diska)
  - Dostupan kroz Control Panel
- File History
  - Periodičko kopiranje datoteka na vanjski disk (samo libraries)
  - Dostupan kroz Control Panel

Sigurnosno kopiranje (Backup) - Alati

- Google Drive for desktop
  - Backup na Google Drive
  - Obrisane dokumente seli u Trash (automatski se brišu nakon 30 dana)
  - Limiti:
    - Maksimalno 100 verzija pojedinog dokumenta
    - Verzije se čuvaj maksimalno 30 dana

Sigurnosno kopiranje (Backup) - Alati

- Veeam Agent for Microsoft Windows FREE
  - https://www.veeam.com/products/free/microsoft-windows.html
  - Potrebna registracija kod preuzimanja
  - https://www.veeam.com/veeam_agents_feature_comparison_ds.pdf
  - Backup na vanjski disk
  - Cijeli disk, particija ili dokumenti

Sigurnosno kopiranje (Backup) - Alati

- Backblaze Personal Computer Backup
  - https://www.backblaze.com/cloud-backup/personal
  - Neograničena količina podataka
  - Neograničen broj računala
  - Verzije dokumenata 30 dana / 1 godina (moguća doplata za trajno)
  - Cijena 9$/mj.

Sigurnosno kopiranje (Backup) - Alati

- Duplicati
  - https://duplicati.com
  - Open source
  - Backup na razini datoteka
  - Na vanjski disk ili cloud po odabiru
  - Web sučelje
  - Mogućnost automatske provjere datoteka

Sigurnosno kopiranje (Backup) - Alati

- Syncthing
  - https://syncthing.net/
  - Open source
  - Direktna sinkronizacija datoteka između dva ili više računala
  - Podržava verzioniranje

Sigurnost (osobnog) računala

Održavanje sigurnosti osobnog računala ključni je korak u zaštiti osobnih podataka i privatnosti. Postoji nekoliko osnovnih mjera koje svatko može primijeniti kako bi smanjio rizik od zlonamjernih programa, krađe podataka i drugih prijetnji.

Prvi i najvažniji korak su redovita ažuriranja operacijskog sustava i aplikacija. Ažuriranja često sadrže zakrpe za novootkrivene sigurnosne propuste, pa njihovo odgađanje povećava rizik od napada.

Instalacija i redovito korištenje antivirusnog programa dodatno pomaže u otkrivanju i uklanjanju zlonamjernog softvera. Uz antivirus, važnu zaštitu pruža i vatrozid (firewall), koji nadzire mrežni promet i sprječava neovlaštene pokušaje pristupa računalu.

Sigurnost (osobnog) računala

Kako bi se spriječio gubitak važnih podataka, potrebno je provoditi redovito sigurnosno kopiranje – idealno prema 3-2-1 strategiji.

Također, treba biti oprezan pri otvaranju datoteka iz nepoznatih ili sumnjivih izvora. Ako niste sigurni u sigurnost neke datoteke, možete je provjeriti putem servisa poput VirusTotal koji analizira sumnjive datoteke i poveznice pomoću više antivirusnih programa.

Dodatnu razinu zaštite pruža postavljanje lozinke na BIOS/UEFI. Time se sprječava neovlašteno pokretanje ili izmjena osnovnih postavki računala, što može biti važno u slučaju fizičkog pristupa uređaju.

Sigurnost (osobnog) računala

Enkripcija diska je proces šifriranja podataka pohranjenih na računalu tako da postanu nečitljivi bez odgovarajuće autorizacije. Ovo je posebno važna mjera zaštite koja sprječava neovlašteni pristup podacima u slučaju gubitka, krađe ili otpisa računala.

Na Windows operativnim sustavima postoje dvije glavne opcije za enkripciju diska:

- **Device Encryption** – jednostavno rješenje dostupno na modernim Windows uređajima koje automatski šifrira podatke.
- **BitLocker Drive Encryption** – naprednija opcija koja omogućuje potpunu kontrolu nad procesom enkripcije i dodatnim postavkama zaštite.

Glavna prednost enkripcije diska jest što štiti podatke od **offline pristupa**, čak i ako napadač fizički dođe do diska ili uređaja. Ipak, važno je imati na umu da je enkripcija samo dio sigurnosne strategije.

Također, pri korištenju ovih tehnologija nužno je **spremiti Recovery Key izvan računala**. Ovaj ključ omogućuje vraćanje podataka u slučaju problema s pristupom šifriranom disku, a ako se izgubi, pristup podacima može postati nemoguć (**backup, backup, backup**).

Sigurnost (osobnog) računala - Device Encryption

Device Encryption je ugrađena opcija u modernim Windows uređajima koja automatski šifrira kompletan disk kako bi zaštitila podatke od neovlaštenog pristupa. Ova značajka radi u pozadini i često se uključuje automatski kada uređaj zadovoljava potrebne uvjete.

Za korištenje Device Encryptiona potrebno je imati određenu **hardversku podršku -** TPM čip (Trusted Platform Module), koji omogućuje sigurno upravljanje kriptografskim ključevima. Osim toga, korisnik mora biti prijavljen na **Microsoftov korisnički račun**.

Kada se Device Encryption aktivira, kompletan disk postaje šifriran, čime se sprječava čitanje podataka bez odgovarajuće autorizacije. Recovery key, ključ za vraćanje pristupa disku u slučaju problema, automatski se sprema u Microsoftov korisnički račun. Ipak, važno je napraviti i **backup ovog ključa na zasebno sigurno mjesto**, jer bez njega pristup podacima može postati nemoguć ako se dogodi problem s računom ili uređajem.

Sigurnost (osobnog) računala - BitLocker

BitLocker je napredna opcija enkripcije diska dostupna u Windows operativnim sustavima koja omogućuje šifriranje podataka radi zaštite od neovlaštenog pristupa. Za razliku od Device Encryptiona, BitLocker se može koristiti čak i **bez TPM čipa**, što ga čini fleksibilnijim rješenjem za različite uređaje i situacije.

Jedna od prednosti BitLockera jest mogućnost odabira što će biti šifrirano – moguće je kriptirati **cijeli disk ili samo pojedine particije**, ovisno o potrebama korisnika. Također, BitLocker **ne zahtijeva Microsoft korisnički račun** - recovery key može se spremiti na USB stick ili isprintati.

BitLocker nudi i dodatne razine zaštite. Primjerice, moguće je postaviti **PIN kod prije pokretanja sustava** ili koristiti **ključ pohranjen na USB sticku**. Ove opcije omogućuju dodatnu sigurnost, posebno na uređajima koji sadrže osjetljive podatke ili se često koriste u javnim okruženjima (više informacija ovdje).

BitLocker predstavlja snažnu zaštitu podataka, ali zahtijeva pažljivo upravljanje postavkama i recovery ključevima kako bi se osigurala potpuna sigurnost i dostupnost podataka.

Slanje/čuvanje povjerljivih podataka

Osim enkripcije diska, važno je koristiti dodatne metode za zaštitu pojedinačnih datoteka ili poruka koje sadrže povjerljive informacije. Postoji nekoliko učinkovitih rješenja, ovisno o vrsti datoteke i načinu prijenosa:

- Zip arhiva zaštićena lozinkom – jednostavan način za šifriranje datoteka. 7-Zip omogućuje stvaranje komprimiranih arhiva koje su zaštićene lozinkom, čime se sprječava neovlašten pristup sadržaju.
- VeraCrypt – besplatan i open-source alat za naprednu enkripciju datoteka, mapa ili čak cijelih diskova (veracrypt.eu). VeraCrypt pruža visoku razinu sigurnosti i često se koristi za zaštitu osjetljivih podataka.
- age – jednostavan alat za enkripciju datoteka, pogodan za korisnike koji žele brzo i sigurno šifrirati pojedinačne datoteke prije prijenosa (link).
- GnuPG – moćan open-source sustav za šifriranje i potpisivanje e-pošte i datoteka. Gpg4win pruža jednostavan način za implementaciju GnuPG tehnologije na Windows računalima.
- Gmail Confidential mode – opcija u Gmailu koja omogućuje slanje poruka s dodatnom zaštitom, uključujući mogućnost postavljanja isteka poruka, zahtjeva za lozinkom i sprječavanja preuzimanja sadržaja (link).

VPN

VPN (**Virtual Private Network**) je tehnologija koja omogućava siguran pristup mrežnim resursima putem interneta, kao da ste fizički povezani na lokalnu mrežu. To znači da možete pristupiti internim dokumentima, serverima ili aplikacijama čak i kada niste radnom mjestu.

Osim toga, VPN dodaje **dodatni sloj enkripcije** vašoj internetskoj vezi. To znači da je promet između vašeg uređaja i interneta zaštićen od prisluškivanja i neovlaštenog pristupa. Ova značajka posebno je važna kada koristite nesigurne mreže.

Zbog svoje sigurnosne funkcije, **korištenje VPN-a preporučuje se na javnim Wi-Fi mrežama** – poput onih u kafićima, restoranima, hotelima ili na konferencijama. Time se značajno smanjuje rizik od krađe podataka i prisluškivanja vaše komunikacije.

VPN je jednostavan alat koji može pružiti veću privatnost i sigurnost pri korištenju interneta, posebno u situacijama kada je mreža javna ili nesigurna.

Kako prepoznati phishing napade

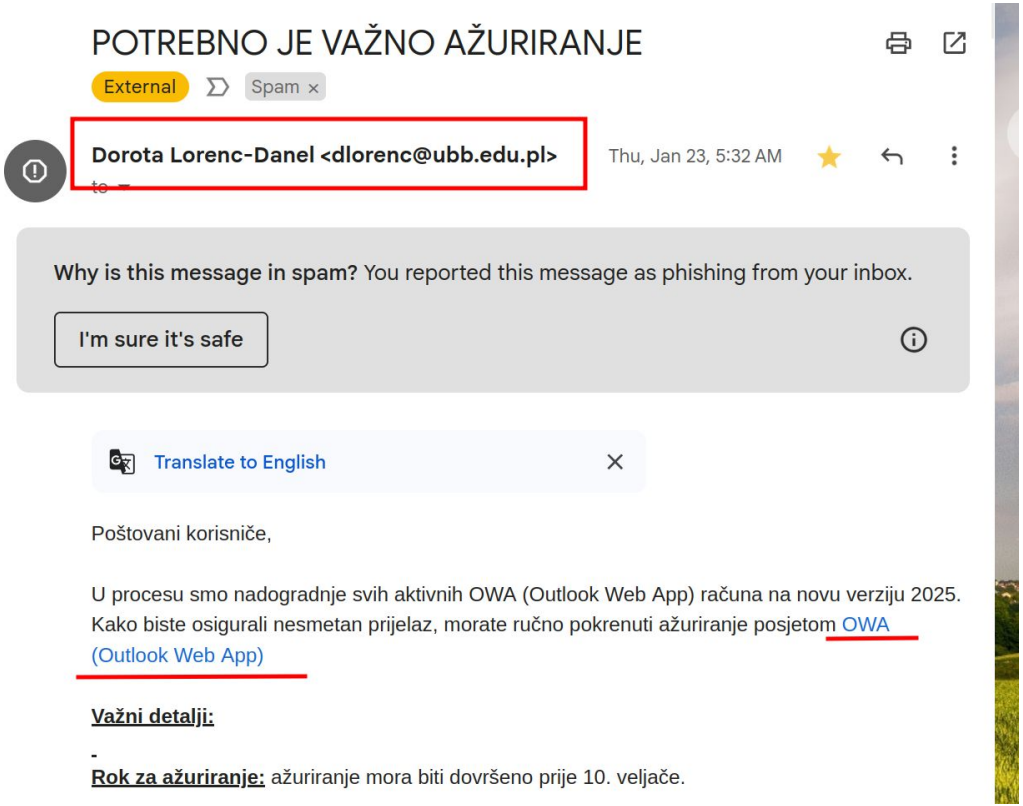
“Phishing se odnosi na internetske prijevare u vidu lažnih e-poruka koje izgledaju kao da su ih poslale legitimne organizacije (primjerice banka, tijelo javne vlasti ili internet stranica za kupovinu), a koje primatelja navode na dijeljenje osobnih, financijskih ili sigurnosnih podataka.”

Izvor: https://azop.hr/phishing-napadi-kako-ih-prepoznati-i-zastititi-se/

Kako prepoznati phishing napade

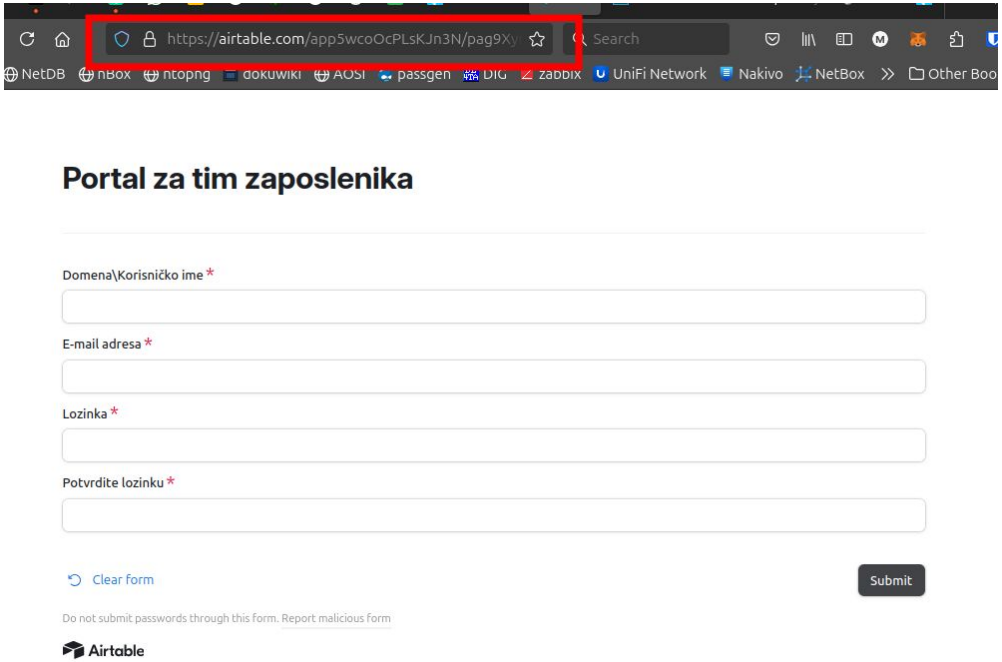
- lažna adresa/domena pošiljatelja (ne nužno!)
- ističu važnost ili traže hitnu reakciju
- nudi se novac ili neka druga primamljiva prilika
- pravopisne i gramatičke pogreške
- sadrže privitke, zahtjevaju otvaranje linkova ili skeniranje QR kodova
- traže uplatu u kriptovalutama

Kako prepoznati phishing napade



- Neobična adresa pošiljatelja.
- Ističe se važnost i postavlja rok.
- Traži se otvaranje linka.

Kako prepoznati phishing napade

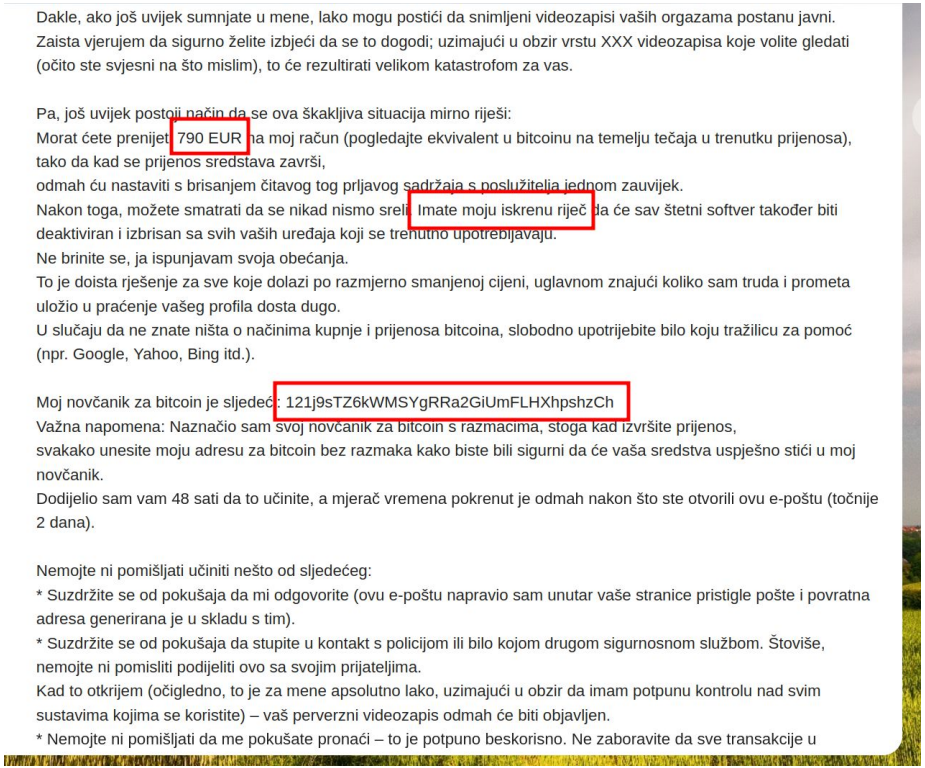


Ova stranica otvara se klikom na link iz prethodnog primjera. Provjerite na kojoj domeni se nalazi “Portal za tim zaposlenika”. Ova domena (airtable.com) ne pripada FOI-u.

Kako prepoznati phishing napade

U ovom primjeru primatelj je ujedno i pošiljatelj! “Haker” tvrdi kako mu “uopće nije bilo teško prijaviti se” na račun primatelja. Ovo je nedostatak SMTP mail protokola koji omogućava slanje mailova s bilo koje adrese bez autentikacije.

Kako prepoznati phishing napade



Dakle, ako još uvijek sumnjate u mene, lako mogu postići da snimljeni videozapisi vaših orgazama postanu javni.
Zaista vjerujem da sigurno želite izbjeći da se to dogodi; uzimajući u obzir vrstu XXX videozapisa koje volite gledati (očito ste svjesni na što mislim), to će rezultirati velikom katastrofom za vas.

Pa, još uvijek postoji način da se ova škakljiva situacija mirno riješi:
Morat ćete prenijeti 790 EUR na moj račun (pogledajte ekvivalent u bitcoinu na temelju tečaja u trenutku prijenosa), tako da kad se prijenos sredstava završi,
odmah ću nastaviti s brisanjem čitavog tog prljavog sadržaja s poslužitelja jednom zauvijek.
Nakon toga, možete smatrati da se nikad nismo sreli. Imate moju iskrenu riječ da će sav štetni softver također biti deaktiviran i izbrisan sa svih vaših uređaja koji se trenutno upotrebljavaju.
Ne brinite se, ja ispunjavam svoja obećanja.
To je doista rješenje za sve koje dolazi po razmjerno smanjenoj cijeni, uglavnom znajući koliko sam truda i prometa uložio u praćenje vašeg profila dosta dugo.
U slučaju da ne znate ništa o načinima kupnje i prijenosa bitcoina, slobodno upotrijebite bilo koju tražilicu za pomoć (npr. Google, Yahoo, Bing itd.).

Moj novčanik za bitcoin je sljedeći: 121j9sTZ6kWMSYgRRa2GiUmFLHXhpshzCh
Važna napomena: Naznačio sam svoj novčanik za bitcoin s razmacima, stoga kad izvršite prijenos,
svakako unesite moju adresu za bitcoin bez razmaka kako biste bili sigurni da će vaša sredstva uspješno stići u moj novčanik.
Dodijelio sam vam 48 sati da to učinite, a mjerač vremena pokrenut je odmah nakon što ste otvorili ovu e-poštu (točnije 2 dana).

Nemojte ni pomišljati učiniti nešto od sljedećeg:
* Suzdržite se od pokušaja da mi odgovorite (ovu e-poštu napravio sam unutar vaše stranice pristigle pošte i povratna adresa generirana je u skladu s tim).
* Suzdržite se od pokušaja da stupite u kontakt s policijom ili bilo kojom drugom sigurnosnom službom. Štoviše, nemojte ni pomisliti podijeliti ovo sa svojim prijateljima.
Kad to otkrijem (očigledno, to je za mene apsolutno lako, uzimajući u obzir da imam potpunu kontrolu nad svim sustavima kojima se koristite) – vaš perverzni videozapis odmah će biti objavljen.
* Nemojte ni pomišljati da me pokušate pronaći – to je potpuno beskorisno. Ne zaboravite da sve transakcije u

Traži se uplata u kriptovalutama.

Dodatne informacije

- What is Phishing and How to Protect Yourself from it: https://www.youtube.com/watch?v=qdpReVgpQhc
- Phishing: https://www.cert.hr/phishing/
- Phishing napadi – kako ih prepoznati i zaštititi se: https://azop.hr/phishing-napadi-kako-ih-prepoznati-i-zastititi-se/
- Phishing Defenses: Top Cybersecurity Strategies to Protect Your Data: https://www.youtube.com/watch?v=nSGQkE67jcg