# **Priručnik o sajber prijetnjama:** identifikacija i borba protiv rizika za korisnike u javnom i privatnom sektoru i građane

**Aleksandar Bratić**

**Oktobar 2022. godina**

DCAF Geneva Centre for Security Sector Governance

# O DCAF-u

DCAF – Ženevski centar za upravljanje sektorom sigurnosti je posvećen poboljšanju sigurnosti država i njihovog stanovništva u okviru demokratskog upravljanja, vladavine prava, poštovanja ljudskih prava i rodnoj jednakosti. Od svog osnivanja 2000. godine, DCAF je pridonio kreiranju održivijeg mira i razvoja pomažući države partnere i međunarodne činioce koji podržavaju te države u poboljšanju upravljanja sektorom sigurnosti kroz inkluzivne i participativne reforme. On kreira inovativne proizvode znanja, promoviše dobre norme i prakse, daje pravne savjete i savjete o politikama i podržava građenje kapaciteta državnih i nedržavnih činioca u sektoru sigurnosti.

DCAF – Ženevski centar za upravljanje sektorom sigurnosti
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Ženeva, Švajcarska
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Design & layout: DTP studio

# Sadržaj

# Sažetak

Svet zavisi od povezanih digitalnih sistema i tehnologija u svakom aspektu svakodnevnog života kao što su trgovanje, finansije, komunikacija, itd.

Mi živimo u digitalnome svetu gde su lični podaci najvažniji. Važno je razumjeti da su lični podaci ranjiviji od bilo kada pre. Stalno čujemo o upadima u podatke i sajber pretnjama koje utiču na milione korisnika. Većina kompanija i institucija se bori da zaštiti svoje podatke od hakera i sajber kriminalaca, a i vi trebate isto tako da igrate ulogu u tome. Sajber sigurnost se ne odnosi samo na organizacije, već i na lične kompjutere, mobilne telefone i tablet uređaje.

Sajber prijetnja ili prijetnja po sajber sigurnost je maliciozna aktivnost osmišljena za krađu ili oštećivanje podataka ili narušavanje sistema jednog pojedinca ili cele organizacije.

U ovom Priručniku biće vam predstavljene različite sajber prijetnje. Sajber prijetnje uključuju široki spektar različitih napada, a najčešće su:

- Društveni inženjering
- Phishing napadi (pecanje – fišing)
- Preuzimanje podatka u prolazu (Drive by downloads)
- Napadi Čovek-u-sredini (MITM napadi)
- Napadi sa odbačenim USB uređajem
- Malware – maliciozni softver

Kako bi zaštitili sebe i svoje sisteme, vi morate naučiti o ovim različitim vrstama sajber prijetnji i različitim načinima kako da ostanete sigurni na internetu.

# Uobičajeni sajber napadi

## Društveni inženjering

Društveni inženjering se koristi da se dovedu u zabludu ili manipuliraju mete, kako bi dobili informacije ili pristup njihovim kompjuterima. Ove vrste napada se pouzdaju u ljudsku interakciju i uobičajeno uključuju manipulaciju korisnika kako bi prekršili sigurnosne procedure i najbolje prakse i dobili neovlašteni pristup sistemima ili dali osjetljive informacije.

Sajber kriminalci koriste pristup preko društvenih mreža da sakriju svoje prave identitete i motive, predstavljajući se kao osobe od povjerenja.

Ovo se vrši varanjem korisnika da kliknu maliciozne linkove ili dobivanjem fizičkog pristupa kompjuteru putem prevare.

**Prevare na internetu**

Prevare na internetu su različite metodologije djela prevare koje vrše sajber kriminalci na internetu. Prevara se može dogoditi putem phishing i-mejlova, društvenih medija, SMS poruka na vašem mobilnom telefonu, lažnih poziva za tehničku podršku i više. Glavni ciljevi ovih vrsta prevara su od krađe kreditnih kartica, snimanja korisničkih akreditiva za prijavljivanje i lozinki, pa do krađe identiteta.[1]

Prevare na internetu funkcionišu jer izgledaju realno i uhvate vas nespremne kada ih ne očekujete. Sajber kriminalci – prevaranti (skemeri) postaju sve pametniji i koriste nove tehnologije, proizvode itd. Savjeti kako da vas ne nagovore da im date vaše lične informacije ili detalje:

- Prevare stvarno postoje, budite obazrivi.
- Ne otvarajte sumnjive tekstualne poruke, pop-up prozore i nemojte kliktati linkove ili privitke u i-mejlovima, već ih obrišite odmah.
- Uvek budite svjesni s kim imate posla.
- Ne odgovarajte na telefonske pozive koji se tiču vaših ličnih informacija ili informacija o kreditnoj kartici; spustite slušalicu.

## Phishing napadi

Većina svih sajber napada počinje sa phishing (fišing – pecanje) i-mejlom. Phishing je vrsta društvenog inženjeringa u kome sajber kriminalce prevare žrtve da im daju osjetljive informacije ili instaliraju maliciozni softver.

I pored toga što tehničke mere sigurnosti postaju sve bolje, phishing ostaje jedan od najjeftinijih i najlakših načina da sajber kriminalci dobiju pristup osjetljivim i ličnim informacijama.

Ako korisnici kliknu na link, njihova sigurnost može biti ugrožena i mogu postati žrtve krađe identiteta.

Kliktanjem korisnici isto tako mogu da kompromitiraju svoje lične informacije, akreditive za najavu kao što su korisnička imena i lozinke i finansijske informacije kao što su brojevi kreditnih kartica).

1 https://us.norton.com/internetsecurity-online-scams.html#

Često napadači ovo postižu kroz maliciozne i-mejlove koji deluju kao da su od izvora od povjerenja, ali ponekad koriste i druge metode, koji su objašnjeni dole.

## Kako funkcioniše phishing?

Većina phishing kampanja uključuje jedan od dva osnovna metoda:

1. **Maliciozni privitci (attachment)**

   Maliciozni privitci u i-mejlovima, koji uobičajeno imaju alarmantne naslove kao „FAKTURA“. Kada budu otvoreni, ovi privitci instaliraju malware na mašini korisnika.

2. **Linkovi do malicioznih veb sajtova**

   Maliciozni linkovi vode do veb sajtova koji su često klonovi legitimnih sajtova. Prelazak na sajt može da dovede do preuzimanja malicioznog softvera ili strana za najavu na sajtu može da sadrži skripte koje kradu akreditive[2].

## Vrste phishing napada

### Spear Phishing (ciljano pecanje)

Spear phishing je maliciozni napad sa lažnim i-mejlom koji cilja na određenu organizaciju ili osobu, pokušavajući da dobije neovlašteni pristup osjetljivim informacijama[3]. Spear phishing pokušaji se ne vrše od slučajnih napadača, već je vjerovatnije da se vrše od sajber kriminalaca koji žele da postignu finansijsku dobit ili prikupe druge vrijedne informacije.

Spear phishing napad funkcioniše tako da se i-mejl se šalje od pouzdanog izvora, ali vodi do lažnog veb sajta koji je prepun malicioznog softvera. Ovi i-mejlovi najčešće koriste kreativne metode da privuku pažnju korisnika.

Spear phishing je daleko efikasniji od drugih phishing napada, ali zahtjeva od sajber kriminalaca da potroše vreme i resurse na istraživanju pre napada. Sajber kriminalci će biti utoliko uspješniji ako nauče o njihovoj meti pre napada.

### Whale Phishing/Whaling (kitolov)

Whale phishing (lov na kitove) je sličan sa spear phishing (ciljano pecanje), sa nekoliko važnih razlika. Dok je spear phishing uobičajeno usmjeren protiv članova određene grupe, whale phishing je usredsređen na konkretnu osobu – uobičajeno „najveću ribu“ u ciljanoj organizaciji ili pojedinca sa značajnim bogatstvom ili moći koju sajber kriminalci žele da iskoriste.

### Vishing

Vishing ili „glasovni phishing“ uključuje manipulaciju ljudi preko telefona i njihovo zavođenje da otkriju osjetljive informacije. Sajber kriminalci pokušavaju da pokupe podatke žrtve i iskoriste ih za svoju ličnu korist, uobičajeno finansijsku.

2 What is phishing? Everything you need to know | IT Governance UK

3 What is Phishing? (gfidigital.com)

**Smishing**

Termin smishing se odnosi na SMS phishing i uključuje tekstualnu poruku umesto i-mejla. Mete uobičajeno dobiju tekstualnu poruku koja sadrži obmanu i koja ih tjera da daju lične ili finansijske informacije. Sajber kriminalci se pretvaraju da su organ vlasti, banka ili druga kompanija kako bi djelovali legitimni u svojim zahtjevima.

Smishing napadači često traže lične ili bankovne podatke, kao što su akreditivi korisničkih naloga, brojeve kreditnih kartica i brojeve za identifikaciju. Potom, oni koriste te informacije kako bi provodili različite vrste napada, uključujući finansijske prevare, prevare sa poklonima i prevare sa podrškom za klijente.

## Preuzimanje podataka u „prolazu“ (drive-by downloads)

Napad sa preuzimanjem podataka u „prolazu“ je sajber napad gde se preuzimaju maliciozne skripte na kompjutere ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim sajber napadima. To može da se dogodi na svakom uređaju na bilo kojem operativnom sistemu. Uobičajeno se događa kada korisnik pređe na i pretražuje kompromitovani veb sajt.

## Napadi čovek-u-sredini (man in the middle (MITM))

MITM napad se događa kada se sajber kriminalac tajno ubaci između dva uređaja, ili između uređaja i nesigurne wi-fi mreže, kako bi presretao komunikacije koje potom on može da čita i/ili mijenja. U takvom slučaju, korisnik može da nenamjerno pošalje sajber kriminalcu akreditive ili druge informacije.

## Napad sa odbačenim USB

U napadu sa odbačenim USB, USB uređaj koji sadrži maliciozni kod se uključuje na kompjuter.

Najuobičajenija sajber prijetnja predstavljana ovim napadom je infekcija malicioznim softverom ili virusom. Infekcije preko USB diska mogu biti i namjerne i nenamjerne, ovisno o dotičnome malicioznom softveru.

Najpametnije  je da organizacije prekinu vjerovati zastariloj USB tehnologiji i počnu koristiti moć sigurnih digitalnih mreža koristeći cloud spremanje podataka (na internetu).

## MALWARE (MALICIOZNI SOFTVER)

Malware je opšti termin koji se koristi za definisanje svake datoteke ili programa koji ima za cilj da ošteti ili naruši rad kompjutera:

- **Botnet softver**

  Botnet softver je osmišljen da inficira veliki broj uređaja koji su povezani na internet. Neki botnet (mreže botova) su sačinjene od velikog broja uređaja, od kojih svaki koristi relativno malu procesorsku snagu. Time se otežava otkrivanje ove vrste malicioznog softvera, čak i kada je botnet u funkciji.

- **Ransomware napadi (napadi sa softverom za otkupninu)**

  Ransomware je vrsta malicioznog softvera koji šifrira informacije korisnika i zahtijeva plaćanje za ključ za dešifriranje, kako bi se povratile informacije. Međutim, plaćanje otkupnine ne garantuje uvek da ćete vratiti šifrirane podatke.

- **Spyware (špijunski softver)**

  Spyware je vrsta malicioznog softvera koji se koristi za nezakonito praćenje aktivnosti korisnika na kompjuteru i prikupljanje ličnih podataka.

- **Trojanski virus**

  Trojanski virusi su vrsta malicioznog softvera koji deluju kao legitiman softver, ali vrše maliciozne aktivnosti kada budu izvršeni.

- **Virusi i crvi**

  Kompjuterski virus je maliciozni kod instaliran bez znanja korisnika. Virusi se mogu množiti i širiti na druge kompjutere time što se pripijaju na druge kompjuterske datoteke.
  Crvi su slični virusima jer se množe sami, ali ne moraju da se prikače na drugi program kako bi to uradili[4].

4 Types of Cyber Threat in 2019 | IT Governance USA

# Kako ostati siguran na internetu

## Budite pažljivi sa svojim ličnim informacijama i digitalnim identitetom

Mi, kao pojedinci, možemo da se identifikujemo na različite načine. Naša imena, adrese, uzrast, profesija i više. Naši identiteti su sadržani u različitim oblicima na našim vozačkim dozvolama, karticama za osiguranje, izvodima iz matične knjige rođenih, karticama za posao ili školu, itd.

Kada razmislimo o svim različitim identifikacijama koje koristimo u svakodnevnom životu na internetu i van njega, da li možemo sa sigurnošću da kažemo koliko naših privatnih podataka se koristi bez naše saglasnosti i koliko od tih podataka se čuva na lokacijama koje su nama nepoznate i koje možda imaju pristup njima i koriste ih.

Nepotrebno je pominjati da nikada ne trebate deliti vaše lozinke, bankovne detalje ili lične informacije na internetu ili sa drugom osobom. Informacije o vašim ličnim odnosima ili imena ljubimca mogu biti iskorištene kao odgovori na vaša sigurnosna pitanja ili mogu dati sajber kriminalcima ideju kada napadaju vaše lozinke.

Hakeri stalno traže nove načine za zloupotrijebu ličnih podataka. Krađa identiteta iz evidencija i upad u podatke su velike prijetnje koje kompromituju to što smo, jer identitet je naše osnovno sredstvo za interakciju:

- Vratite nazad kontrolu nad vašim podacima
- Nemojte koristiti vaše lične podatke kada kreirate profile na internetu
- Nemojte davati vaše lične podatke kako bi dobili popust u prodavnici
- Nemojte nepotrebno deliti vaše privatne informacije na društvenim medijima
- Uvek provjerite kako će biti obrađeni vaši lični podaci kada koristite neku aplikaciju
- Provjerite da li je sajt siguran pre nego što ostavite lične informacije

Ako je besplatna usluga koju koristite, budite ekstra obazrivi. Ako je besplatno, uobičajeno vi ste roba (vaši podaci).

## Kreirajte i koristite složene lozinke

**Uvek trebate koristiti složene lozinke**. Ako vaša lozinka sadrži očigledne ili lake za pogađanje kombinacije brojeva (12345, 111111, 123321), popularna ženska imena (Nikolina, Džesika, Hana) ili samo nizove slova koji formiraju horizontalnu ili vertikalnu liniju na QWERTY tastaturi (asdfghjkl, qazwsx , 1qaz2wsx, itd.), trebate je promjeriti ODMAH! Iznenađuje što je najočiglednija lozinka – „password“ – još uvek vrlo popularna. I nju trebate promjeriti odmah (ili ako je vaša lozinka slična bilo čemu gore navedenom).

Ako vam je potrebna pomoć da izmislite sigurne lozinke, evo nekoliko savjeta:

- Treba da bude najmanje 15 karaktera — duža, ako je moguće.
- Pomiješajte slova (velika i mala), brojeve i simbole.
- Ne koristite sekvencu brojeva ili slova, kao „qwerty“.
- Izbjegavajte zamjene kao „štreberski govor“ (gde se slova mijenjaju brojevima ili simbolima sličnog izgleda).

**Koristite različite lozinke za različite korisničke naloge**. Na taj način, ako je jedan nalog kompromitovan, bar drugi neće biti pod rizikom.

Ako ne možete da sjetite vaših lozinki, definitivno trebate probati program za upravljanje lozinkama. Lozinke je teško zapamtiti same po sebi, osobito ako vam je potrebna posebna lozinka za svaki sajt. Savjetuje se korišćenje renomiranih programa za upravljanje lozinkama kao što su LastPass ili 1Password[5].

## Dvaput proverite linkove pre kliktanja

Kada provjeravate vaš i-mejl ili posjećujete internet strane, provjerite da li poznajete i vjerujete linku pre nego što kliknete na njega.

Jedan način da provjerite da li je link siguran je da pređete mišem preko njega. To će vam pokazati prikaz celog linka u status polju vašeg internet pretraživača. Provjerite da vidite da li prikazani link odgovara veb sajtu sa kojeg bi trebao da dolazi. Isto tako, možete da provjerite link do tačnog sajta ako potražite njegovo ime.

Ako dobijete i-mejl koji od vas zahtjeva da se prijavite, sigurnije je da ne kliknete link u i-mejlu i umesto toga da odete na zvanični sajt i prijavite se tamo. Možete preći na zvanični sajt ili pretražujući njegovo ime ili, ako znate napamet, unošenjem adrese u URL polje vašeg pretraživača. Ovaj savjet uključuje i linkove koje su vam poslali prijatelji u aplikacijama za društvene mreže.

Ako i-mejl ili sajt zahtjeva od vas da se prijavite na vaš bankovni račun, uvek možete da se javite i provjerite zahtjev.

Što se tiče preuzimanja podataka, trebate razmisliti dvaput pre nego što to uradite. Određeni sajber kriminalcu imaju za cilj da inficiraju vaš uređaj malicioznim softverom time što će vas prevariti da preuzmete kompromitovane aplikacije i drugi softver. Pre nego što preuzmete podatke, provjerite sajt sa koga skidate novu igru ili aplikaciju i jednostavno nemojte preuzimati ništa što djeluje sumnjivo.

## Koristite sigurne WI-FI mreže

Nikada ne trebate koristiti nesigurnu, otključanu ili wi-fi mrežu bez lozinke, osim ako stvarno ne morate. Ako koristite takvu mrežu, nemojte se prijavljivati na nijedan korisnički nalog onlajn ili u aplikacijama i nemojte unositi lične ili finansijske informacije.

Sajber kriminalci često postave lažne wi-fi mreže kako bi namamili korisnike. Čim osoba poveže svoj telefon na wi-fi, sajber kriminalci u suštini vide sve što ta osoba radi.

Ako tražite wi-fi mrežu, najsigurniji način je da pitate zaposlenog kako se zove njihova wi-fi mreža.

Isto tako, osigurajte se da vaši uređaji nisu postavljeni da se automatski povezuju na wi-fi mreže, osim na poslu ili kod kuće. Namjestite uređaj da vas pita pre nego što se poveže. Na ovaj način ćete biti sigurni na šta se povezujete.

## Koristite VPN

VPN, ili virtualna privatna mreža, sigurno povezuje važe uređaje na internet kako niko ne bi mogao da sledi

5 How to Stay Safe Online: Internet Safety Tips and Resources (reviews.org)

aktivnosti ili pristupi vašim informacijama preko internet veze. VPN može biti dobar način za sigurnu vezu kod kuće ili čak i kada ste vani i koristite javnu wi-fi mrežu.

Jedini nedostatak povećanoj sigurnosti koju daje VPN je da može usporiti vašu internet vezu. Ovo je često rezultat toga što VPN preusmjerava vaše podatke kroz drugi server kako bi osigurao vaše informacije.

Sve više ljudi radi od kuće u zadnje vreme, što kaže da mnogi od nas mogu postati meta sajber kriminalaca. Metod za održavanje zaštite je korišćenje VPN mreže i njeno ažuriranje po preporuci.

Kako bi dobili VPN, trebate odabrati davaoca VPN usluga, preuzeti i instalirati VPN i povezati se na server.

## Koristite sajtove koji počinju sa https//

Ako želite da se prijavite na bilo koji sajt, provjerite da li adresa na vrhu vašeg pretraživača počinje sa https://, a ne sa http://. Možda ćete i vidjeti simbol katanca pored adrese sajta.

“S” znači “secure” - sigurno i znači da sajt šifrira vaše podatke.

Internet kupovina znači da vi dajete vaše lične informacije, kao što su bankovni računi i informacije o kreditnim karticama. Uvek provjerite dva puta da li je veb sajt na kome se nalazite siguran, a potom popunite podatke.

## Isključite vaš Bluetooth

Bluetooth komunikacije se mogu kompromitirati ili čak manipulirati. To ne znači da nikada ne trebate koristiti Bluetooth, ali ako niste povezani sa drugim uređajem i aktivno ga koristite, najbolje je da ga isključite.

## Koristite antivirus i antimalware softver

Ne preporučuje se pretraživanje interneta bez zaštite. Ako si ga ne možete priuštiti, bar nađite besplatni i jeftini antivirus softver na internetu. Odaberite pažljivo i mudro.

Plaćanje male svote za softver vrijedi kako bi izbjegli glavobolju od suočavanja sa malware ili ransomware. Ako već imate antivirus ili antimalware softver, ažurirajte ga stalno.

Neki preporučeni antivirus i antimalware softveri uključuju sledeće:

- Microsoft Defender (dolazi sa Windows, ali ga morate uključiti i ažurirati)
- Norton AntiVirus Plus
- Bitdefender
- AVG
- Malwarebytes
- Avast
- SpyBot Search and Destroy

## Napravite bekap (rezervne kopije) vaših podataka

Naši kompjuteri i drugi uređaju su dom svih naših važnih podataka. Ali, ako je taj uređaj kompromitovan, oštećen, izgubljen ili ukraden, vaši važni podaci mogu biti izgubljeni. Bez razlike da li se radi o hardverskom

defektu, krađe, prirodne katastrofe ili infekcije vašeg uređaja sa malicioznim softverom, povratak podataka može biti skup ili nemoguć.

**Bekap je digitalna kopija vaših najvažnijih informacija**.

Kada pravite rezervne kopije podataka, kopije vaših datoteka (pr. fotografije, dokumenti, videa itd.) se snimaju na spoljašnji uređaj za čuvanje podataka ili na onlajn servis kao što je cloud.

Ako imate bekap to znači da možete vratiti svoje podatke ako nešto krene po zlu. To je preventivna mjera kako bi vaši podaci bili dostupni u slučaju da se nešto dogodi vašem kompjuteru. Savjetujemo vas da redovno radite bekap vaših datoteka[6].

Postoji mnogo načina za bekap vaših podataka, od korišćenja eksternih diskova do spremanja podataka na udaljenom serveru preko interneta. Ovo su prednosti i nedostaci svakog metoda:

- **Bekap na eksterni disk**: kako bi izvršili bekap podataka na eksterni hard disk, možete iskoristiti ugrađene bekap opcije kompjutera. S vremena na vreme povežite disk na vaš kompjuter i iskoristite alat za bekap, ili ostavite disk uključen i bekap će se raditi automatski.
  **Pozitivne strane**: bekap je brz i jeftin.
  **Negativne strane**: eksterni disk može biti izgubljen ili ukraden.
- **Bekap vaših podataka na vaš kompjuter**: ovo su neka uputstva o različitim načinima za bekap vaših podataka na Mac, iOS uređajima ili PC:
  * iCloud (iOS uređaji)
  * Time Machine (Mac)
  * Windows 8.1 (PC)
  * Windows 10 (PC)

  **Pozitivne strane**: bekap je brz i jeftin.
  **Negativne strane**: bekap može biti izgubljen ili ukraden.
- **Koristite uslugu za čuvanje podataka na internetu (cloud)**: umesto da čuvate vaše podatke na hard disku vašeg kompjutera, vi ih možete čuvati i na servisu kao Dropbox, Google Drive, Microsoft OneDrive, ili sličnoj usluzi za čuvanje podataka na internetu - cloud. Oni će se onda automatski sinhronizirati sa vašim onlajn korisničkim nalozima i vašim drugim uređajima. Ako se vaš hard disk pokvari ili vam ukradu kompjuter, još uvek će te imati kopije datoteka koje se čuvaju onlajn i na vašim drugim uređajima.
  **Pozitivne strane**: ovaj je metod brz i lak i u mnogim slučajevima besplatan, a zbog toga što je onlajn, štiti vas od svih vrsta gubitka podataka.
  **Negativne strane**: Većina cloud servisa nudi samo nekoliko besplatnih gigabajta podataka, tako da ovo funkcioniše samo ako imate mali broj datoteka koje želite staviti na bekap ili ako ste voljni da platite za dopunski prostor[7].

Na kraju, trebati razmisliti o tome gde se nalaze vaši važni podaci i da provjerite/testirate da imate nekoliko kopija u svakom trenutku. Idealno, te kopije trebaju biti na nekoliko fizičkih lokacija. Sve dok mislite o tome šta ako se nešto loše dogodi uređaju, trebali bi biti ispred većine ljudi.

6 Back Up and Restore - Microsoft Windows | Cyber.gov.au

7 Best ways to backup your computer. • Nerds in a Flash

# Zaključak

Sve veće prijetnje se otkrivaju u novim tehnologijama kao što su društveni mediji, cloud kompjuterski rad, tehnologija pametnih telefona ili kritične infrastrukture, a te prijetnje često zloupotrebljavaju njihove jedinstvene karakteristike.

Umesto pokušaja za rješavanje problema na internetu i u kompjutorskim sistemima, bolji je pristup da na vaš uređaj primjenite neke od savjeta iz ovog Priručnika i da slijedite preporučeno ponašanje kako bi ostali sigurni na internetu.

# Reference

Online Scams, Avoiding Internet Scams, Norton

What is phishing? Everything you need to know, IT Governance UK

What is Phishing?, gfidigital.com

Types of Cyber Threat in 2019, IT Governance USA

What Is Cyberbullying, StopBullying.gov

Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Back Up and Restore - Microsoft Windows, Cyber.gov.au

Best ways to back up your computer, Nerds in a Flash

# Aneks: Kontrolna lista dobrih praksi

| UOBIČAJENI SAJBER NAPADI | |
|---|---|
| DRUŠTVENI INŽENJERING | - Društveni inženjering se koristi da se dovedu u zabludu ili manipuliraju mete, kako bi dobili informacije ili pristup njihovim kompjuterima. Ove vrste napada se pouzdaju u ljudsku interakciju i uobičajeno uključuju manipulaciju korisnika kako bi prekršili sigurnosne procedure i najbolje prakse i dobili neovlašteni pristup sistemima ili dali osjetljive informacije. |
| PHISHING NAPADI | - Phishing je vrsta napada u kome sajber kriminalci prevare žrtve da im daju osjetljive informacije ili instaliraju maliciozni softver:<br>• Spear Phishing (ciljano pecanje) – maliciozni i-mejl koji cilja na određenu organizaciju ili osobu sa ciljem dobijanja pristupa osjetljivim informacijama.<br>• Whale Phishing / Whaling (kitolov) – usredsređen je na konkretnu osobu – uobičajeno „najveću ribu“ u ciljanoj organizaciji ili pojedinca sa značajnim bogatstvom ili moći koju sajber kriminalci žele da iskoriste.<br>• Vishing – je pokušaj za dobijanje podataka žrtve i njihovo korišćenje za finansijsku dobit, a ljudi se prevare preko telefona.<br>• Smishing – je tekstualna SMS poruka koja sadrži obmanu da privuče primače da daju lične ili finansijske informacije (akreditivi korisničkih naloga, brojeve kreditnih kartica, itd...), gde se sajber kriminalci pretvaraju da su organ vlasti, banka ili druga kompanija kako bi djelovali legitimni u svojim zahtjevima. |
| PREUZIMANJE PODATAKA U „PROLAZU“ | - Napad sa preuzimanjem podataka u „prolazu“ je sajber napad gde se preuzimaju maliciozne skripte na kompjutere ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim sajber pretnjama i događa se kada korisnik pređe na i pretražuje kompromitovane veb sajtove. |
| MITM (čovek u sredini) NAPADI | - MITM napad se događa kada se sajber kriminalac tajno ubaci između dva uređaja, ili između uređaja i nesigurne wi-fi mreže, kako bi presretao komunikacije koje potom on može da čita i/ili mijenja, što može da dovede do toga da korisnik nenamjerno pošalje sajber kriminalcu akreditive ili druge informacije. |
| NAPAD SA ODBAČENIM USB | - Napad sa odbačenim USB se događa kada se uključi na kompjuter USB uređaj koji sadrži maliciozni kod. |
| MALICIOZNI SOFTVER - MALWARE | - **Botnet softver** – on inficira veliki broj uređaja koji su povezani na internet.<br>- **Ransomware napad (napad sa softverom za otkupninu)** – on šifrira informacije korisnika i zahtijevaju plaćanje za ključ za dešifriranje, kako bi se povratile informacije.<br>- **Spyware** - je vrsta malicioznog softvera koji se koristi za nezakonito praćenje aktivnosti korisnika na kompjuteru i prikupljanje ličnih podataka.<br>- **Trojanski virus** – je vrsta malicioznog softvera koji djeluje kao legitiman softver, ali vrši maliciozne aktivnosti kada budu izvršen.<br>- **Virusi i crvi** –<br>- Virus je maliciozni kod instaliran bez znanja korisnika. Virusi se mogu množiti i širiti na druge kompjutere time što se pripijaju na druge kompjuterske datoteke.<br>- Crvi su slični virusima jer se množe sami, ali ne moraju da se prikače na drugi program kako bi to uradili. |

| KAKO OSTATI SIGURAN NA INTERNETU | |
|---|---|
| NEMOJTE DELITI SVOJE LIČNE INFORMACIJE | - **Nikada ne trebate ni sa kim ili onlajn deliti informacije o:**<br>• vašim lozinkama<br>• bankovne detalje<br>• lične informacije<br>- **Vratite nazad kontrolu nad vašim podacima**<br>- **Nemojte koristiti vaše lične podatke kada kreirate profile na internetu**<br>- **Nemojte davati vaše lične podatke kako bi dobili popust u prodavnici**<br>- **Nemojte nepotrebno deliti vaše privatne informacije na društvenim medijima**<br>- **Uvek provjerite kako će biti obrađeni vaši lični podaci kada koristite neku aplikaciju:**<br>• Provjerite da li je sajt siguran pre nego što ostavite lične informacije |
| KREIRAJTE I KORISTITE SLOŽENE LOZINKE | - **Uvek trebate koristiti složene lozinke:**<br>• Treba da bude najmanje 15 karaktera — duža, ako je moguće.<br>• Pomiješajte slova (velika i mala), brojeve i simbole.<br>• Ne koristite sekvencu brojeva ili slova, kao „qwerty“.<br>• Izbjegavajte zamjene kao „štreberski govor“ (gde se slova mijenjaju brojevima ili simbolima sličnog izgleda).<br>- **Koristite različite lozinke za različite korisničke naloge**<br>- **Probajte softver za upravljanje lozinkama** |
| DVAPUT PROVERITE LINKOVE PRE KLIKTANJA | - **Kada provjeravate vaš i-mejl ili posjećujete internet strane, provjerite da li poznajete i vjerujete linku pre nego što kliknete na njega**:<br>• Pređite mišem preko linka i provjerite da li ste dobili prikaz celog linka u status polju vašeg internet pretraživača.<br>• Ako dobijete i-mejl koji od vas zahtjeva da se prijavite, sigurnije je da ne kliknete link u i-mejlu i umesto toga da odete na zvanični sajt i prijavite se tamo.<br>• Ako i-mejl ili sajt zahtjeva od vas da se prijavite na vaš bankovni račun, uvek možete da se javite i provjerite zahtjev.<br>• Pre nego što preuzmete podatke, provjerite sajt sa koga skidate novu igru ili aplikaciju i jednostavno nemojte preuzimati ništa što djeluje sumnjivo. |
| KORISTITE SIGURNE WI-FI MREŽE | - Nikada ne trebate koristiti nesigurnu, otključanu ili wi-fi mrežu bez lozinke, osim ako stvarno ne morate.<br>- Dok ste na wi-fi mreži nemojte se prijavljivati na nijedan korisnički nalog onlajn ili u aplikacijama i nemojte unositi lične ili finansijske informacije.<br>- Osigurajte se da vaši uređaji nisu postavljeni da se automatski povezuju na wi-fi mreže. |
| KORISTITE VPN | - VPN, ili virtualna privatna mreža, sigurno povezuje važe uređaje na internet kako niko ne bi mogao da sledi aktivnosti ili pristupi vašim informacijama preko internet veze.<br>- Kako bi dobili VPN, trebate odabrati davaoca VPN usluga, preuzeti i instalirati VPN i povezati se na server. |
| AKO POČINJE SA HTTPS, SIGURNO JE | - Ako želite da se prijavite na bilo koji sajt, provjerite da li adresa na vrhu vašeg pretraživača počinje sa https://, a ne sa http://.<br>- Možda ćete i vidjeti simbol katanca pored adrese sajta. |
| ISKLJUČITE VAŠ BLUETOOTH | - Ako ponekad koristite Bluetooth isključite ga kad ga aktivno ne koristite, kako bi izbjegli njegovo kompromitiranje ili manipulaciju. |
| KORISTITE ANTIVIRUS I ANTIMALWARE SOFTVER | - Ako si ga ne možete priuštiti, bar nađite besplatni i jeftini antivirus softver na internetu kako bi izbjegli suočavanje sa malware ili ransomware. |
| NAPRAVITE BEKAP (REZERVNE KOPIJE) VAŠIH PODATAKA | - Kada pravite rezervne kopije podataka, kopije vaših datoteka (pr. fotografije, dokumenti, videa itd.) se snimaju na spoljašnji uređaj za čuvanje podataka ili na onlajn servis kao što je cloud.<br>- Postoji mnogo načina za bekap vaših podataka<br>• Bekap na eksterni disk<br>• Bekap podataka na vašem kompjuteru<br>- Koristite uslugu za čuvanje podataka na internetu (cloud) |

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

**www.dcaf.ch**

@DCAF_Geneva