CYBERSECURITY NINJA

BORBA S IZAZOVIMA KIBERNETIČKE SIGURNOSTI

IVLP Impact Awards 2023

SADRŽAJ

OBRAZOVANJE MLADIH I RODITELJA O BORBI S KIBERNETIČKIM IZAZOVIMA

CYBERSECURITY NINJA

Cybersecurity Ninja je projekt pokrenut u sklopu "**IVLP Impact Awards**" programa kojeg financira Vlada Sjedinjenih Američkih Država (**U.S. Department of State Bureau of Educational and Cultural Affairs**). Cilj projekta je edukacija djece, roditelja i učitelja o izazovima kibernetičke sigurnosti te kako se od njih zaštititi. Primjena tehnologije sve je raširenija i počinje se koristiti u sve ranijoj dobi. To je zanimljivo napadačima na internetu, takozvanim "hakerima" koji na razne načine pokušavaju izmanipulirati korisnike kako bi stekli korist, najčešće krađom osobnih podataka ili novčanih sredstava. U narednih nekoliko stranica pronađite korisne savjete o tome kako biti sigurniji na internetu.

Projektni partner: CARNET, Nacionalni CERT

VRSTE ZLONAMJERNOG SADRŽAJA

Brojne prijetnje dolaze nam s interneta. Jedna od najčešćih prijetnji je zlonamjerni sadržaj (engl. malware). Upoznajmo se s nekoliko najčešćih prijetnji na internetu.

TROJANSKI KONJ

Poznat i čest zlonamjerni softver koji se lažno predstavlja kao neki drugi, legitiman softver, kako bi ga korisnik pokrenuo. Napadač zatim može koristiti računalo za krađu osjetljivih podataka, kao dio botnet mreže, za špijunažu ili drugu malicioznu aktivnost.

Mreža zaraženih računala koja je pod kontrolom napadača.

Bot je pojedino zaraženo računalo unutar botnet mreže.

BOTNET

VIRUS

Maliciozni softver koji je vezan za druge legitimne datoteke, a širi se **interakcijom čovjeka**. Svojom reprodukcijom može zaraziti računalo tako da sam sebe kopira u datotečni sustav ili memoriju.

Iako se više ne koriste često, obično druge maliciozne softvere poput trojanskog konja ili crva nazivamo zajedničkim nazivom “virusi”.

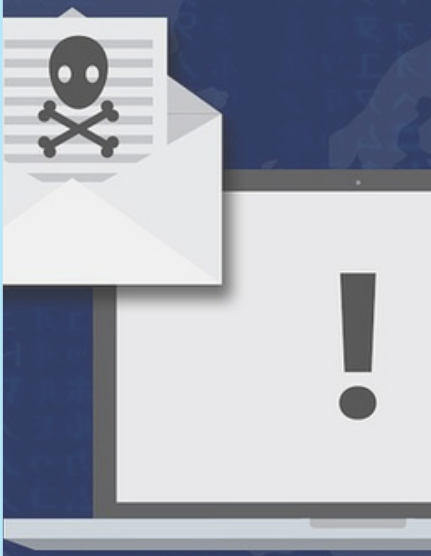
CRV

Maliciozni softver koji se širi mrežom bez interakcije korisnika. Često koriste **ranjivosti** u računalnim sustavima kako bi se umnožili i širili dalje. Za razliku od virusa, oni nisu vezani uz postojeće datoteke.

RANSOMWARE

Vrsta malicioznog softvera koji šifrira korisničke podatke ili zaključava pristup operacijskom sustavu. Kako bi korisnik ponovno ostvario pristup svojim datotekama napadač traži otkupninu, najčešće u kriptovalutama.

Ransomware je sve češća pojava koja najviše cilja poslovne korisnike ili kritičnu infrastrukturu, no cilja i krajnje korisnike. Nerijetko se širi spear phishing metodom, ciljanim phishingom kod kojeg napadač dobro prouči metu i iskorištava prikupljene informacije kako bi kreirao napad specifično za određenu žrtvu. **Najbolja obrana od ransomware napada je redovita izrada sigurnosnih kopija podataka (engl. backup).**



Stručnjaci za kibernetičku sigurnost savjetuju da se **ne plaća otkupnina** napadačima.

KEYLOGGER

Vrsta malicioznog softvera ili hardvera koji bez znanja korisnika snima tipke koje korisnik unosi na računalu, a najčešće se koristi za krađu osjetljivih informacija.

SPYWARE

Vrsta malicioznog softvera koji prikuplja podatke o korisniku bez njegova pristanka, primjerice osjetljive i osobne informacije, lozinke ili podatke bankovnih kartica. Napadači obično prikupljene podatke šalju trećim stranama za krađu identiteta, prijevare ili ciljane oglase.

SOCIJALNI INŽENJERING

Osim zlonamjernih sadržaja, s interneta nam često dolaze prijetnje koje na neki način manipuliraju korisnikovim odlukama. Te vrste prijevara zajednički se nazivaju socijalni inženjering. Socijalni inženjering je manipulacija ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator ne može sam doći. Manipulator korisnika prijevarom "namami" da otkrije povjerljivu informaciju ili za njega obavi neku radnju.

Najpoznatija vrsta socijalnog inženjeringa je phishing. Phishing (varijanta engleske riječi za pecanje, fishing) je vrsta socijalnog inženjeringa koja se odnosi na prijevare u kojima napadač lažnim predstavljanjem i naizgled legitimnim zahtjevom pokušava potencijalnu žrtvu natjerati da učini nešto u napadačevu korist. Phishingom se kradu različiti osobni podaci: korisnička imena i lozinke za pristup servisima kao što su e-mail, društvene mreže, u opasnijem slučaju brojevi i CVV oznake naših bankovnih kartica itd.

Phishing je popularan jer prevaranti ne moraju tražiti propuste u sigurnosnoj zaštiti računala, već korisnik svojevoljno upisuje informacije.

NEKE OD PRIJETNJI NA DRUŠTVENIM MREŽAMA:

- Napadi povezani sa socijalnim inženjeringom;
- Krađa identiteta;
- Curenje podataka;
- Dijeljenje neprikladnih informacija;
- Rudarenje podataka i profiliranje;
- Narušavanje privatnosti;
- Širenje malicioznog sadržaja;
- Internetsko nasilje i uznemiravanje;
- Lažne vijesti i dezinformacije;
- Kompromitacija korisničkog računa;
- Zlonamjerno praćenje lokacije, kamere, mikrofona.

10 ZLATNIH PRAVILA KIBERNETIČKE SIGURNOSTI

REDOVITO AŽURIRAJTE SOFTVER

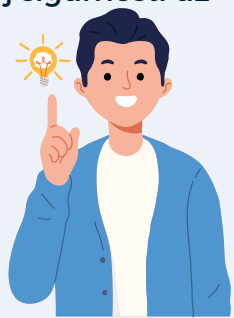
Redovito ažurirajte operacijske sustave, aplikacije i antivirusne programe. Ažuriranja često sadrže ispravke sigurnosnih ranjivosti.

KORISTITE SNAŽNE I JEDINSTVENE LOZINKE

Kreirajte kompleksne lozinke za svoje korisničke račune i koristite različite lozinke za svaku pojedinu uslugu. Razmislite o korištenju upravitelja lozinkama kako bi ih jednostavno i sigurno pohranjivali.

KORISTITE VIŠEFAKTORSKU AUTENTIFIKACIJU

Gdje god je moguće, uključite višefaktorsku autentifikaciju (engl. multifactor authentication - MFA) za svoje online korisničke račune. To dodaje još jedan sloj sigurnosti uz kompleksnu lozinku.



PRIPAZITE NA PHISHING

Budite oprezni kod otvaranja sumnjivih e-mail poruka, poveznica i priloga. Uvjerite se u legitimnost pošiljatelja prije nego kliknete na poveznice i podijelite osjetljive informacije.

ZAŠTITITE SVOJE OSOBNE INFORMACIJE

Ograničite količinu osobnih podataka koje dijelite na internetu. Budite oprezni što dijelite na društvenim mrežama i s kime dijelite informacije.

OSIGURAJTE SVOJU WI-FI MREŽU

Koristite snažne lozinke za svoju Wi-Fi mrežu i redovito ažurirajte ugrađeni softver usmjernika (engl. firmware routera). Onemogućite udaljenu administraciju i koristite snažne metode enkripcije ako je moguće.

REDOVITO IZRAĐUJTE SIGURNOSNE KOPIJE

Redovito izrađujte sigurnosnu kopiju (engl. backup) svojih podataka i držite ih na sigurnoj lokaciji, odvojeno od sustava. To će vam pomoći u slučaju gubitka podataka ili ransomware napada.

BUDITE OPREZNI PRILIKOM PREUZIMANJA SADRŽAJA S INTERNETA

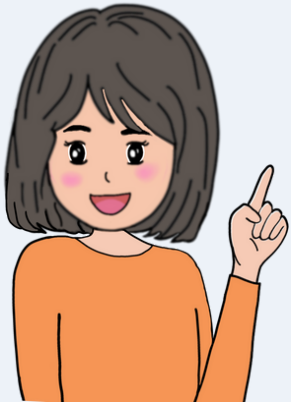
Preuzimajte softver i datoteke samo iz pouzdanih izvora. Izbjegavajte preuzimanje piratskog sadržaja i softvera jer može sadržavati maliciozni sadržaj.

VODITE BRIGU O MREŽNOJ SIGURNOSTI

Koristite vatrozid (engl. firewall), sustav za otkrivanje upada (engl. intrusion detection system) i antivirusni softver kako biste zaštitili svoju mrežu od kibernetičkih prijetnji.

EDUCIRAJTE SEBE I DRUGE

Informirajte se o najboljim praksama u području kibernetičke sigurnosti i informirajte svoju obitelj, prijatelje i kolege. Samo zajedno možemo učiniti internet sigurnijim.



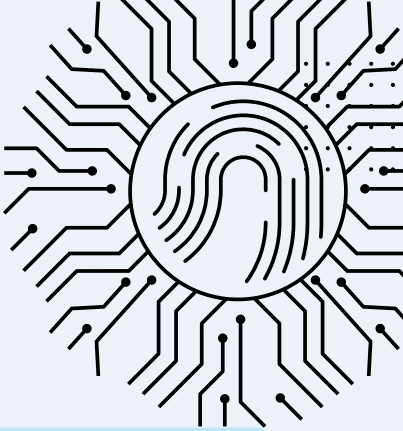
Za sigurnije surfanje primjenjuj zlatna pravila svaki put kada se koristiš internetom!

Tu su kako bi te zaštitila!

SAVJETI ZA DOBRU LOZINKU

- Stavite prioritet na **duljinu lozinke** (što dulja to bolja)
- Koristite **velika i mala slova, brojeve i specijalne znakove** (poželjno dijakritike)
- Koristite **upravitelje lozinkama**
- Koristite **višefaktorsku autentifikaciju** gdje god je to moguće
- Možete koristiti **fraze** ili **stihove** pjesama
- Kod korištenja fraza i riječi **zamijenite slovo brojem i obrnuto** (npr. 3=E, i=1, A=4, T=7 i slično)
- Kako bi lozinka bila sigurnija primijenite sve gore navedene savjete.

DIGITALNI TRAG



Digitalni trag, otisak ili sjenu čini jedinstven skup digitalnih aktivnosti, akcija, doprinosa te komunikacije putem interneta i digitalnih uređaja kojoj se može ući u trag. Svaki digitalni trag treba tretirati kao **neizbrisiv.**

Uključuje sve **naše objave**, sve objave koji su **drugi objavili o nama**, ali i sve podatke o nama koje smo **dopustili** da se prikupljaju. Na primjer to su fotografije, videi, tekstualne poruke i objave, reakcije, kolačići i osobni podaci koje svjesno ili nesvjesno objavljujemo i šaljemo putem interneta.

Napadači imaju mnoge koristi od našeg digitalnog traga, uključujući krađu identiteta, marketinške oglase, ucjene i povrede privatnosti.

Iz tog razlog bitno je paziti što, kada i gdje **objavljujemo**, **šaljemo** i na koji način **reagiramo.**

SIGURNOST ŠKOLSKOG RAČUNALA

Školsko računalo potrebno je tretirati **kao vlastito** i koristiti se njime, kao što se koristimo i onim kod kuće - **na siguran način:**

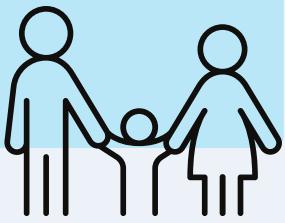
- kad smo završili s nekim zadatkom ili korištenjem neke usluge na internetu, potrebno se **odjaviti iz korisničkog računa;**
- kad se moramo udaljiti od računala ili napustiti učionicu, a prijavljeni smo na neke online usluge, računalo je potrebno zaključati kombinacijom tipki **Windows tipka + L**;
- ne uključivati **neprovjerene** uređaje za pohranu podataka (npr. USB flash memoriju)
- kad smo završili s korištenjem **USB-a**, potrebno ga je na **siguran način isključiti** i spremiti;
- kad preuzimamo datoteke, one moraju biti samo iz **provjerenih izvora** i ne bismo trebali **otvarati sumnjive poveznice i privitke;**
- osobe odgovorne za administraciju školskih računala moraju **redovito ažurirati** operacijski sustav i antivirusni program.

VODIČ ZA RODITELJE I UČITELJE

Otvorena komunikacija - uspostavite otvorenu i ne osuđujuću komunikaciju s djecom u vezi njihovih online aktivnosti. Potaknite ih da razgovaraju s vama ako naiđu na probleme ili se osjećaju nelagodno online.

Postavite prikladne dobne granice za korištenje interneta - kod društvenih mreža, video igara i drugih sadržaja različite dobne skupine nailaze na različite prijetnje i ranjivosti. Razmislite o korištenju alata za postavljanje dobnih granica.

Podučite djecu bontonu na internetu - razgovarajte o internet bontonu (engl. netiquette), odgovornom ponašanju na internetu i posljedicama internetskog nasilja i uznemiravanja. Potaknite empatiju i poštovanje prema drugim korisnicima na internetu.



VODIČ ZA RODITELJE I UČITELJE

Privatnost na internetu - naučite djecu o važnosti online privatnosti, savjetujte im da ne dijele informacije kao što su ime i prezime, adresa, škola ili telefonski broj nepoznatim ljudima na internetu. Objasnite im rizik dijeljenja slika i videa online te važnost dobivanja dozvole prije nego objave sliku ili video druge osobe.

Osnove kibernetičke sigurnosti - naučite djecu o važnosti korištenja snažnih lozinki i MFA, opasnosti otvaranja sumnjivih poveznica ili preuzimanja sumnjivog sadržaja te kako prepoznati phishing sadržaj.

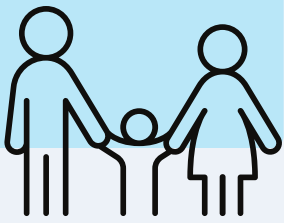
Budite svjesni online aktivnosti - pratite što djeca rade online bez zadiranja u njihovu privatnost! Važno je da razumijete platforme koje koriste i koje prijatelje imaju online. Budite svjesni aplikacija koje preuzimaju, pročitajte recenzije te se upoznajte s dobnom granicom kako biste procijenili jesu li te aplikacije primjerene.

VODIČ ZA RODITELJE I UČITELJE

Sigurno korištenje društvenih mreža - raspravite o važnosti podešavanja pravila privatnosti kako bi djeca mogla odrediti tko može vidjeti njihov online sadržaj i komunicirati s njima. Potaknite ih da prihvate online prijateljstva samo od onih ljudi koje poznaju u stvarnom životu.

Prepoznajte znakove internetskog nasilja - Naučite djecu kako prepoznati znakove internetskog nasilja i dajte im do znanja da vam se mogu obratiti ako postanu žrtva ili budu svjedoci maltretiranja drugih.

Online reputacija - Objasnite da njihove online radnje, objave i komentari mogu utjecati na njihovu budućnost, uključujući upis na fakultet i prilike za posao. Potaknite ih da zadrže pozitivnu online prisutnost.



VODIČ ZA RODITELJE I UČITELJE

Vodite primjerom - Budite uzor za odgovorno ponašanje na internetu. Djeca često uče promatrajući postupke svojih roditelja. I sami vježbajte dobre navike vezane uz kibernetičku sigurnost, kao što su korištenje snažnih lozinki i oprez kod otvaranja e-pošte i poveznica.

Ostanite informirani - Budite u toku s najnovijim online trendovima, aplikacijama i društvenim mrežama koje vaša djeca mogu koristiti. Upoznajte se s potencijalnim rizicima povezanim s novim tehnologijama.

Podržite njihove interese - Potaknite interes svoje djece za tehnologiju i internet, ali ih usmjeravajte da koriste te alate sigurno i odgovorno.

IVLP Impact Awards program provodi se pod pokroviteljstvom U.S. Department of State Bureau of Educational and Cultural Affairs u partnerstvu s Meridian International Center. Navedeni subjekti nisu odgovorni za sadržaj ove brošure. Za više informacija posjetite: https://www.meridian.org/project/u-s-department-of-state-ivlp-impact-awards/

Za više sadržaja o kibernetičkoj sigurnosti pratite projektnog partnera CARNET - Nacionalni CERT: