NAČULJITE UŠI,
SAZNAJTE KAKO SAČUVATI DIGITALNI IMUNITET.

Zajednički projekat sa Intesa Sanpaolo odsekom za sajber bezbednost

SADRŽAJ

KAKO OJAČATI DIGITALNI IMUNITET NAŠE DECE?

Danas, kada svi toliko brinemo o imunitetu i kako da ostanemo zdravi u vanrednim okolnostima koje nam je pandemija donela, zaboravljamo da smo sve više izloženi uticaju velike količine sadržaja sa različitih digitalnih platformi koji itekako utiču na naše i mentalno zdravlje naše porodice. Kako da izgradimo digitalni imunitet i zaštitimo naše klince od štetnih uticaja, toksičnih ljudi i neprimerenih sadržaja, pitanje je koje postavljaju svi roditelji u svetu.

Kao što svoju decu učite da izbegavaju opasnosti na ulici, morate ih naučiti da izbegnu opasnosti koje vrebaju na internetu. Naučite ih da su odgovorni za svoje postupke i da treba da preuzmu odgovornost za sve što na internetu objavljuju i dele. Učite ih da njihovi postupci mogu da pogode ljude sa kojima su u kontaktu, a tako i njih same, pa zbog toga treba da pričaju sa ljudima onlajn na isti način kao da razgovaraju sa njima licem u lice.

PITAJTE I PROVERAVAJTE SVOJU DECU:

- Sa kim četuju?
- Šta rade kad su onlajn?
- Šta posećuju onlajn?
- Ko stupa u kontakt sa njima?

LOZINKA

Lozinke su način pristupa **nečemu** i mogu da se koriste za identifikaciju osobe. Pošto su one jedini način identifikacije osobe, treba da ostanu tajna.

Lozinke treba da sadrže karaktere, slova i brojeve. Treba ih menjati jednom godišnje ili češće kako bi se sprečilo hakovanje.

EVO NEKOLIKO KORISNIH PREDLOGA:

- Osoba može da pogodi lozinku ako je previše jednostavna: savetujte ih da kreiraju složene lozinke pomoću kombinacije slova, brojeva i specijalnih karaktera. Neka koriste barem 8 karaktera (14 karaktera bi bila najbolja opcija).
- Neka ne koriste istu lozinku za više naloga.
- Neka ne uključuju svoje ime u lozinku.
- Ne treba da dele lozinke ni sa kim van svoje porodice.

DIGITALNI SVET I REALNI SVET

OPŠTA PRAVILA KOJA TREBA DA PRENESETE SVOJOJ DECI:

- Uvek razmišljajte o tome ko se krije iza ekrana.
- Čuvajte svoje lične podatke u tajnosti.
- Ne razgovarajte i ne šaljite fotografije nepoznatim osobama.
- Čuvajte svoje naloge na društvenim mrežama bezbednim.

ŠTA MOŽE DA SE DELI NA DRUŠTVENIM MREŽAMA?

- Ime i nadimak.
- Hobiji i interesovanja, bez mnogo detalja.
- Fotografije gde ne mogu da se vide detalji (npr. slike iz škole, slike uniformi sportskih klubova).
- **Lajkovi** za filmove, knjige i hranu.

ŠTA NE TREBA DA SE DELI NA DRUŠTVENIM MREŽAMA?

- Ime i prezime.
- Imena porodice i prijatelja.
- Datum rođenja.
- Naziv škole.
- Fotografije sa detaljima i ličnim podacima.
- Adresa i broj telefona.

MALVERI I ANTIVIRUSI

4

- Saznajte šta su malveri i antivirusi i edukujte svoju decu o tome.
- Malver je kombinacija reči **maliciozni** i **softver**. Malver je vrsta softvera koji hakeri mogu da instaliraju na računar bez saglasnosti vlasnika.
- Postoje različite vrste malvera koji mogu da naštete računarima: verovatno najpoznatiji su kompjuterski virusi, ali ima ih još. Svi ovi maliciozni programi mogu da kradu lozinke, uklanjaju datoteke, prikupljaju lične podatke, a čak i da sprečavaju rad računara.
- Kada se pravilno instalira u računarski sistem, antivirusni softver može da blokira neželjene programe.
- Ako nije instaliran nikakav antivirusni softver, hakeri mogu da pristupe svim informacijama sačuvanim u računaru.
- Instaliranje više od jednog antivirusnog programa nije dobra ideja. Programi mogu da smetaju jedan drugom.

DEFINICIJE MALVERA

VIRUS

Virusi su među najvažnijim i najpoznatijim malverima. U pitanju su programi koji zaražavaju računar ili računarski sistem radi uništavanja podataka, oštećenja datoteka ili modifikacije radnih karakteristika.

Za razliku od drugih malvera, virusi mogu da se replikuju i ulaze u druge računare, tablete i pametne telefone upotrebom internet veze ili drugih komunikacionih sistema.

SPAJVER

„Spajver" je kombinacija reči „spaj" (spy – špijun) i „ver" (ware) (deminutiv reči „softver"). Ovaj malver zaražava računar, tablet, pametni telefon ili računarske sisteme radi špijuniranja ljudi koji ih koriste, krađe informacija koje se čuvaju u memoriji njihovog uređaja i njihovog slanja drugim uređajima kojima upravljaju hakeri, odnosno kreatori spajvera.

RANSOMVER

Ovo je jedan od najopasnijih i najskorijih malvera. Ransomveri, koji su softveri za „otkup" (ransom), koriste pecanje kako bi zarazili uređaj u cilju infiltracije u računarsku mrežu. Kada uđu u računar, tablet ili pametni telefon, vlasnik ne može ništa da uradi: ransomveri brzo sakrivaju sve podatke skladištene u memoriji i restartuju uređaj. Kada se restartuje, vlasnik uređaja će primetiti poruku sa zahtevom za otkup, u kojoj se od njega traži da plati određenu sumu novca kako bi ponovo pristupio svojim datotekama.

DEFINICIJE MALVERA

CRV

Crvi su malveri koji koriste zaražene uređaje da se replikuju i šalju sami sebe drugim uređajima. U većini slučajeva, oni to čine tako što šalju sebe putem imejlova. Crvi obično ne deluju sami, već omogućavaju drugim malverima da se šire, poput spajvera.

TROJANAC

Baš kao što je Odisej ušao u Troju pomoću drvenog konja, **hakeri se često infiltriraju u sigurnosne sisteme na računarima, tabletima, pametnim telefonima i računarskim sistemima upravo upotrebom „Trojanskog konja“.** Kada uđe u uređaje, softver kreira daljinski pristup koji prevaranti koriste za krađu podataka, ali i za daljinsko upravljanje uređajima.

ADVER

Adveri su verovatno najmanje štetni malveri, pošto su u pitanju maliciozni programi koji ulaze u računare, tablete i pametne telefone samo radi prikaza video reklama i banera. U ovom slučaju, cilj nije krađa ili uništavanje podataka, već samo zarada kroz oglašavanje, koja se povećava vizuelizacijama vlasnika zaraženih uređaja.

SAVETI ZA RODITELJE

- Ne ostavljajte svoju decu samu kada koriste internet! Podesite vaše uređaje tako da vaša deca zaborave lozinku Wi-Fi veze, da ne mogu da budu onlajn bez vas. Takođe, proveravajte njihova preuzimanja aplikacija i aktivnosti na društvenim mrežama.
- Razgovarajte sa svojom decom o sajber bezbednosti! Važno je da deca razumeju implikacije onoga što objavljuju (šta se otprema onlajn, ostaje onlajn...), rizike deljenja ličnih podataka, sajber nasilje, prisustvo malicioznih ljudi i način na koji se kriju na internetu (princip „ne razgovaraj sa nepoznatima“ važi i za virtuelnu stvarnost), itd.
- Koristite prikladnije pretraživače za decu.
- Verifikujte podešavanja privatnosti na uređajima vaše dece.
- Podesite vaš pretraživač tako da blokira sve iskačuće prozore (pop-ups) i isključite Javu.
- Uvek prijavite štetne, uznemirujuće, uvredljive, nametljive i opasne poruke i sadržaje!

ZAKLJUČAK

Najčešće se roditelji ne ustručavaju da preuzmu brigu i odgovornost za ponašanje svoje dece u igri, školi ili u tuđoj kući. Ne mora biti drugačije ni kad je reč o onome što se događa posredstvom moderne tehnologije. Roditelji treba da se edukuju o savremenoj tehnologiji, a zatim da razgovaraju sa svojom decom o kompjuterskoj etici, da dogovore pravila ponašanja na internetu i, kao najvažnije, definišu posledice kršenja tih pravila. Prisutnost odraslih koji nadgledaju situaciju u stvarnom životu umanjuje incidente i ublažava posledice, ukoliko do nasilja i dođe. Isto se može primeniti i na elektronsko nasilje.