SAVJETI ZA ZAŠTITU OSOBNIH UREĐAJA OD KIBERNETIČKIH NAPADA

Ovi savjeti odnose se na postupanje s osobnim uređajima (računala, dlanovnici, pametni telefoni, pametni satovi i sl.) koji imaju mogućnost povezivanja s internetom. Svaki takav uređaj može biti kompromitiran i rizik od kibernetičkog napada uvijek je prisutan. Kako bi takve rizike što više smanjili, nužno je biti svjestan njihova postojanja, znati kakva postupanja ili nepostupanja rizike povećavaju te prilagoditi način korištenja ili konfiguriranja osobnih uređaja na način koji će mogućnost kibernetičkog napada što više smanjiti. Neke od mjera koje preporučamo poduzeti su sljedeće:

KORISTITE ANTIVIRUSNE PROGRAME

Instalirajte i redovito ažurirajte antivirusne programe na svim Vašim osobnim uređajima, uključujući i pametne telefone.

KORISTITE VATROZID

Koristite programski ili sklopovski vatrozid, i osigurajte da je isti na odgovarajući način konfiguriran i uključen.

INSTALIRAJTE REDOVNO SIGURNOSNE NADOGRADNJE

Ako je to moguće, na svojim uređajima omogućite automatsko preuzimanje programskih i sigurnosnih nadogradnji.

ISKLJUČITE MOGUĆNOST NEPOTREBNOG PRISTUPA PODACIMA O VAŠOJ LOKACIJI (TJ. LOKACIJI UREĐAJA), TE UGRAĐENOJ KAMERI I MIKROFONU

Provjerite sva dopuštenja koja pojedina aplikacija zahtijeva od uređaja, posebno ona koja se odnose na pristup podacima o Vašim kontaktima, lokaciji, kameri ili mikrofonu uređaja. Ako takav pristup nije opravdan funkcionalnošću aplikacije, takva dopuštenja isključite.

UKLONITE APLIKACIJE KOJE VAM NISU POTREBNE

Svaka aplikacija u određenoj mjeri predstavlja rizik od kibernetičkog napada. U tom smislu, što više instaliranih aplikacija imate na Vašem uređaju – i rizik kojim ste izloženi je veći. Ako Vam neka aplikacija više nije potrebna, uklonite je (deinstalirajte) s uređaja.

PRIJE INSTALIRANJA SVAKE NOVE APLIKACIJE NA VAŠ UREĐAJ – SAGLEDAJTE RIZIK NJEZINA KORIŠTENJA

Aplikacije s lošim ocjenama korisnika i aplikacije koje su razvile nepoznate tvrtke ili razvojni programeri predstavljaju veći rizik od onih s boljim ocjenama korisnika ili onih koje je razvio pouzdani izvor. Mnoge aplikacije mogu sadržavati i dijelove s malicioznim kodom. Budite svjesni takvih rizika i odgovorno procijenite što želite instalirati na svoj uređaj, što ćete uistinu koristiti te koliko vjerujete pojedinoj aplikaciji. Budite dodatno oprezni s aplikacijama za čije korištenje/instaliranje na uređaj je

nužno omogućiti pristup podacima o Vašoj lokaciji, kameri ili mikrofonu uređaja.

PAŽLJIVO I ODGOVORNO KORISTITE DRUŠTVENE MREŽE

Razmislite o postavkama sigurnosti na svakom Vašem profilu na bilo kojoj društvenoj/socijalnoj mreži. Budite svjesni rizika kojem se izlažete te mogućnosti kompromitacije osobnih podataka koje na takvim mrežama pohranjujete te svjesno i odgovorno odlučite o svakoj mogućoj sigurnosnoj postavci. Preporuka je odabrati sigurnosne postavke koje u najvećoj mogućoj mjeri štite Vašu privatnost te ne iznositi nikakve podatke koji bi u trenutku objavljivanja, ili bilo kada kasnije, mogli naškoditi Vašem ugledu ili ugledu osoba/organizacija koje spominjete ili s kojima ste povezni.

KORISTITE SLOŽENE ZAPORKE

Koristite zaporke koje sadrže velika i mala slova, brojeve i posebne znakove te su dovoljno duge (npr. 10 i više znakova). Preporučena zaporka, koja je dovoljno duga i složena da ju je teško pogoditi i istovremeno lakša za zapamtiti, je fraza sastavljena od nasumičnih (ili čak nepostojećih) riječi uz dodavanje specijalnih znakova po želji. U internetskim preglednicima nemojte koristiti mogućnost pamćenja zaporke (opcija „*remember password*“) i nemojte koristiti jednaku zaporku ili jednak PIN za više različitih računa, aplikacija ili web usluga. Zaporke redovito mijenjajte, svakih 3 ili najviše 6 mjeseci. Možete koristiti i programe koji upravljaju zaporkama (tzv. *password manager* programe). Takav program pamti i pohranjuje sve Vaše zaporke, a pristupate mu korištenjem jedne tzv. glavne zaporke. Vodite računa da ćete u ovom slučaju morati zapamtiti samo jednu zaporku koja mora biti uistinu vrlo složena što na prvi pogled može djelovati kao povećani rizik. No, ako koristite veliki broj zaporki, i ako su sve složene, teško ćete ih moći zapamtiti i vjerojatno ćete zaporke ili negdje zapisati ili koristiti istu zaporku za više usluga/računa ili na neki drugi način doskočiti objektivnoj teškoći pamćenja velikog broja složenih zaporki. U tom slučaju, ako ste svjesni da ne možete zapamtiti sve svoje zaporke, korištenje programa koji upravlja zaporkama predstavlja manji rizik od korištenja zaporki koje ste negdje zapisali ili korištenje lako predvidljivih jednostavnih zaporki.

PAŽLJIVO IZBERITE PREGLEDNIK I PRETRAŽIVAČ ZA INTERNET

Nisu svi preglednici i pretraživači interneta jednaki. Osim korisničkog iskustva koje može biti različito, bitno je sagledati i razinu sigurnosti i privatnosti koju jamče. Najčešće se veća razina sigurnosti ostvaruje na račun manje razine privatnosti, i obratno. Ako postavke pretraživača kojeg koristite omogućuju isključivanje praćenja povijesti pretraživanja, izradu audio zapisa ili pristup podacima o Vašoj lokaciji, iskoristite tu mogućnost i tako smanjite rizike.

IZBJEGAVAJTE JAVNE/NEPOZNATE BEŽIČNE MREŽE

Razina sigurnosti na javnim bežičnim mrežama nije pod našom kontrolom, i ako je ikako moguće, izbjegavajte korištenje takvih mreža. Pristupanjem takvoj mreži izlažete se riziku i raznim zlonamjernim korisnicima dajete mogućnost za pokušaj kibernetičkog napada na Vaš uređaj. Ako želite bežično pristupiti Internetu s uređajem koji nema funkcionalnost GSM-a, tj. morate koristiti bežični wi-fi pristup, jedna od opcija je i da sami napravite/uključite pristupnu točku koristeći drugi pouzdan uređaj (npr. vlastiti pametni telefon) te tako umjesto javne bežične mreže, koristite mrežu svog uređaja.

ZAŠTITITE SE OD TZV. *PHISHING* NAPADA

Phishing je vrsta kibernetičkog napada u kojem napadač socijalnim inženjeringom pokušava doći do Vaših zaporki, korisničkih imena i sl. podataka. Najčešće se realizira na način da korisnik (potencijalna žrtva napada) zaprimi poruku elektroničke pošte s uputom da na poveznici (*link*-u) koji je dio poruke provjeri ili ponovo upiše pristupne podatke za korištenje nekog servisa/usluge. Odabirom (klikanjem) na takvu poveznicu korisnik stiče dojam da je na legitimnoj stranici npr. banke, portala za on-line kupovinu i sl. Međutim, niti jedan pružatelj usluga neće nikada od Vas tražiti da pristupite njihovoj usluzi kroz poveznicu koju ste zaprimili elektroničkom poštom, niti će na takav način tražiti da „provjerite“ svoju zaporku i sl. Takve poveznice Vas preusmjeravaju na maliciozne stranice koje su oblikovane na način da nalikuju službenim stranicama neke tvrtke/servisa, no one su u vlasništvu napadača. Svrha *phishing* napada je krađa i iskorištavanje Vaših podataka za razne maliciozne radnje ili ostvarivanje koristi na Vaš račun. Ne vjerujte neprovjerenim porukama

elektroničke pošte, ne odgovarajte na njih, **ne otvarajte sumnjive i neprovjerene privitke niti poveznice**. Uslugama koje koristite pristupajte preko preglednika za internet korištenjem službene web adrese pružatelja usluge.

ONEMOGUĆITE PRIKAZIVANJE OGLASA ILI SKOČNE PROZORE S OGLASIMA

Koristite aplikacije, antivirusne programe ili internet preglednike koji korisniku omogućuju blokiranje odnosno onemogućavanje prikazivanja oglasa.

APLIKACIJE ZA KOMUNIKACIJU I RAČUNI ELEKTRONIČKE POŠTE

Aplikacije za komunikaciju porukama (tzv. messaging aplikacije, npr. WhatsApp, Viber, javni servisi elektroničke pošte i sl.) mogu kriptirati Vaše poruke na način da su nečitljive trećim stranama, tj. samo ih pošiljatelj i primatelj mogu pročitati. Međutim, Vaše poruke nisu uvijek skrivene od pružatelja usluge. Servis kojeg koristite može prikupljati različite podatke o Vama (iz poruka koje šaljete i zaprimate te iz uređaja na kojem je usluga instalirana) i koristiti ih bilo za povećanje vlastitog profita, ili može Vaše podatke ustupiti tvrtkama s kojima su povezani. Vaše ime, prezime, broj telefona, popis Vaših kontakata, lokacija, detalji o provedenim plaćanjima i kupovinama, vrijeme i učestalost kojom razmjenjujete poruke itd. samo su dio podataka koje su dostupne messaging aplikacijama na Vašem uređaju. Vodite računa o svojoj privatnosti i sigurnosti te provjerite postavke aplikacije koje koristite. Prilikom samog odabira aplikacije, tj. kada odlučujete koju ćete aplikaciju koristiti, informirajte se kakav pristup sigurnosti i privatnosti svojih korisnika ima tvrtka koja je vlasnik aplikacije.

BUDITE OPREZNI S POVEZNICAMA, SMS PORUKAMA, FOTOGRAFIJAMA I VIDEO MATERIJALIMA

Ne otvarajte sumnjive poveznice, poruke, fotografije i video klipove. Pazite na poruke koje su Vam proslijeđene. Pošiljatelj, koji nije stvaratelj poruke, ne mora biti svjestan što Vam je proslijedio i radi li se o sumnjivom ili malicioznom privitku. U aplikacijama za komunikaciju porukama onemogućite automatsko preuzimanje privitaka.

NE ZABORAVITE

FIZIČKI PREKRIJTE OTVOR KAMERE

Jedini način da budete potpuno sigurni da vaša kamera neće moći biti upotrijebljena bez Vašeg znanja i dopuštenja, čak i u slučaju kompromitacije uređaja ili kibernetičkog napada jest fizičko prekrivanje otvora kamere. Možete koristiti kupovni poklopac za kameru ili zalijepiti *post it* papirić ili nešto slično preko otvora kamere.

PAŽLJIVO ODABERITE KADA I GDJE PUNITE SVOJE UREĐAJE

Spajanje vašeg uređaja na stanicu za punjenje na javnom mjestu (npr. u javnom prostoru, zrakoplovnoj luci i sl.) predstavlja rizik i postoji mogućnost neovlaštenog pristupa Vašem uređaju i podacima na njemu. Koristite vlastite punjače ili razmislite o korištenju aplikacija koje mogu onemogućiti prijenos podataka preko ulaza za punjenje uređaja.

ISKLJUČITE WI–FI I *BLUETOOTH* KAD VAM NE TREBAJU

Hakeri mogu pristupiti Vašem uređaju korištenjem uključenog wi–fi ili *bluetooth* prijemnika. Isključite ih u postavkama uređaja za vrijeme dok Vam nisu potrebni.

BUDITE OPREZNI PRILIKOM SPAJANJA NEPOUZDANIH PRIJENOSNIH UREĐAJA/MEMORIJA NA VAŠ UREĐAJ

Prijenosne memorije, punjači i slični uređaji mogu biti inficirani računalnim virusima ili nekim drugim zlonamjernim sadržajem. Ako ne vjerujete uređaju, mislite da bi mogli biti inficirani ili ne poznate onoga tko Vam je uređaj dao, ne koristite ga. Ako nepouzdani prijenosni uređaj/memoriju ipak odlučite priključiti na svoj uređaj, rizik možete u određenoj mjeri smanjiti ako sadržaj nepouzdanog uređaja/memorije provjerite antivirusnim programom.

IZRADITE KOPIJE SVOJIH PODATAKA

Za slučaj gubitka ili kvara uređaja, ili nekih vrsta kibernetičkih napada (npr. tzv. *ransomware* napad u kojem zlonamjerni softver kriptira podatke korisnika i u zamjenu napadač traži otkupninu), kopija podataka na nekoj vanjskoj prijenosnoj memoriji ili u oblačnom servisu kojem vjerujete može vam omogućiti brži i jednostavniji nastavak rada te spriječiti plaćanje otkupnine.

Ne postoji popis proizvođača, usluga ili uređaja kojima možete sa 100% sigurnošću vjerovati. Niti jedna od predloženih mjera ne može u potpunosti ukloniti rizik niti Vam jamčiti da nećete biti predmet kibernetičkog napada. Međutim, svaka od predloženih mjera, ako je primjenjiva za pojedinu vrstu uređaja, može i hoće smanjiti rizik kojem se izlažete, a u slučaju da se napad ipak dogodi, posljedice tj. prouzročena šteta bit će manja. Na Vama je odgovornost da osobne uređaje koristite savjesno, pažljivo i odgovorno i da ne ignorirate rizike kojima se izlažete. Cilj svake od prethodno opisanih mjera nije otežavanje korištenja nekog uređaja niti je cilj izbjegavanje interneta i on-line servisa. Kibernetički napadi su dio naše svakodnevnice i ne možemo ih izbjeći. Ono što možemo i moramo je smanjiti rizike u najvećoj mogućoj mjeri te biti odgovoran sudionik kibernetičkog prostora.

REPUBLIKA HRVATSKA
Ured Vijeća za nacionalnu sigurnost
Jurjevska 34, 10000 Zagreb
www.uvns.hr

REPUBLIKA HRVATSKA
Zavod za sigurnost informacijskih sustava
Fra Filipa Grabovca 3, 10000 Zagreb
www.zsis.hr