Ne budi i ti hrvatski naivac

#SurfajSigurnije

CERT.hr
surfaj sigurnije

Sufinancirano instrumentom Europske unije za povezivanje Europe

**Hrvatska akademska
i istraživačka mreža
- CARNET**

Josipa Marohnića 5,
HR - 10000 Zagreb

tel.: +385 1 6661 616
e-pošta: ured@carnet.hr
www.carnet.hr

Nacionalni CERT

tel.: +385 1 6661 650
e-pošta: ncert@cert.hr
www.cert.hr

CERT.hr je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj, dio je Hrvatske akademske i istraživačke mreže - CARNET.

UVOD

Posjetite www.naivci.hr i kroz zabavu surfajte sigurnije.

Knjižica je nastala u okviru nacionalne kampanje za podizanje svijesti o kibernetičkoj sigurnosti pod nazivom "**Hrvatski naivci**". Kampanja je dio projekta „GrowCERT – Jačanje kapaciteta Nacionalnog CERT-a i poboljšanje suradnje na nacionalnoj i europskoj razini" koji je sufinanciran sredstvima Europske komisije putem Instrumenta za povezivanje Europe (*CEF – Connecting Europe Facility*).

Ova knjižica nastala je u želji da se svim korisnicima približi pojam kibernetičke sigurnosti te ih se pripremi za život u digitalnom dobu. Naša je želja da se ovom knjižicom služite kako biste naučili prepoznati opasnosti koje vrebaju u virtualnoj stvarnosti, zaštititi vaše uređaje te odgovorno rukovati osobnim i povjerljivim podacima.

Danas se internetom gotovo svakodnevno koriste svi, od djece do osoba starije životne dobi, no znaju li oni koje sve opasnosti vrebaju na toj globalnoj mreži i na koji način se od njih zaštititi?

Prema dostupnim podacima istraživanja Eurobarometra iz 2017. godine stavovi građana o kibernetičkoj sigurnosti u Hrvatskoj daju zaključiti kako prosječni korisnici u Hrvatskoj nedovoljno vode brigu o zaštiti vlastitih podataka, ne razmišljaju kako bi upravo oni mogli postati žrtva kibernetičkog napada te im je potrebna edukacija. Korisnici interneta samouki su u snalaženju u online prostoru baš poput samoukih slikara hrvatske naive, a hrvatski naivci ljudi su koji su zahvaljujući svojoj naivnosti postali žrtve internet prevara i neutemeljeno su povjerljivi.

Također, željeli bismo čitatelje osvijestiti kako je kibernetička sigurnost fenomen u kojem svi sudjelujemo zajedno i naglasiti važnosti pravovremenog i primjerenog informiranja i edukacije, ali i komunikacije o izazovima u kibernetičkom prostoru. Kibernetička sigurnost više nije nešto čime se bave isključivo računalni stručnjaci, već bi se njome trebali baviti svi korisnici interneta, a danas se njime svakodnevno služimo gotovo svi.

Nacionalni CERT, odjel Hrvatske akademske i istraživačke mreže – CARNET, zadužen je za kibernetičku sigurnost korisnika interneta u Republici Hrvatskoj te iz tog razloga želimo sve korisnike pripremiti za suočavanje s izazovima digitalnog društva bez straha, oprezno i hrabro, ali odgovorno.

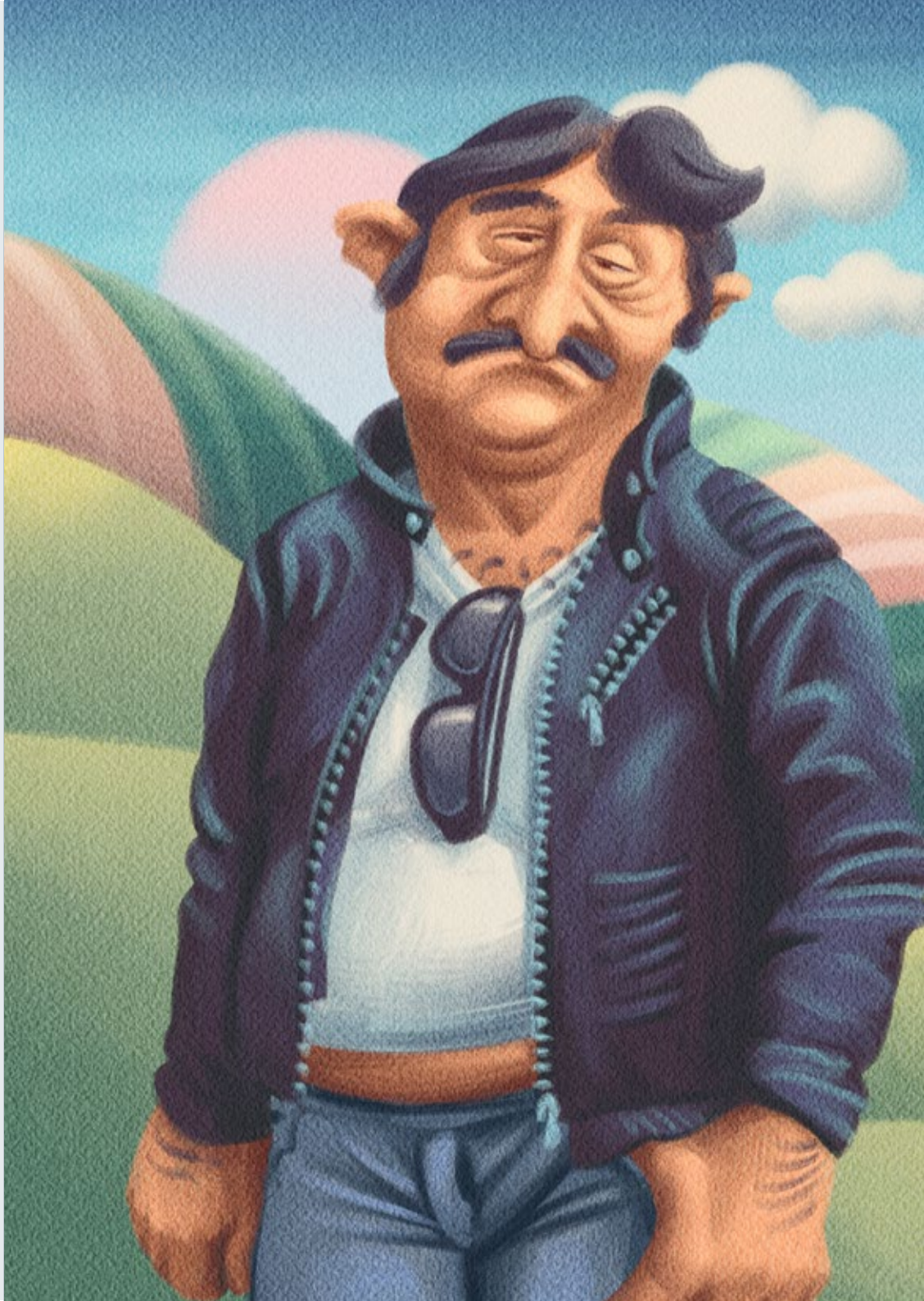
Mnogi od vas ne žele postati računalni stručnjaci koji sate provode ispred računala kako bi ga učinili sigurnim, već se svojim uređajima želite služiti kako biste pristupali internetu, komunicirali te putem i pomoću interneta poslovali.

Upravo zato smo pripremili ovu knjižicu koja će vam putem temeljnih znanja i savjeta olakšati život u digitalnom dobu i omogućiti vam da budete prva linija obrane u vašem kućanstvu ili u poslovnoj okolini te na pravi način podignete razinu kibernetičke sigurnosti.

Iako se do nedavno smatralo kako se najveća opasnost krije u tehničkim propustima unutar uređaja i aplikacija koje koristimo, u posljednje smo vrijeme sve više svjedoci napada koji su usmjereni izravno na čovjeka. Upravo zato želimo osvijestiti kako je najbolji alat u odgovoru na izazove 21. stoljeća znanje i kritičko promišljanje. Svaki vaš postupak na internetu ostavlja neki trag te stvara vaš digitalni otisak koji postaje, htjeli vi to ili ne, dijelom vašeg identiteta u stvarnom svijetu.

S boljim razumijevanjem o tome što sve napadač može učiniti s vašim osobnim i povjerljivim podacima, lakše ćete se snaći na internetu te znati u pravom trenutku prepoznati prijetnju te na pravi način reagirati. Želimo vam ugodno surfanje i dobre valove!

Vaš CERT.hr tim



NACIONALNI CERT

Nacionalni CERT (eng. Computer Emergency Response Team) odjel je Hrvatske akademske i istraživačke mreže – CARNET, čiji je osnovni zadatak obrada incidenata na internetu odnosno očuvanje kibernetičke sigurnosti u Republici Hrvatskoj. Nacionalni CERT bavi se incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj (odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru), osim tijela državne uprave za koje je nadležan CERT ZSIS (CERT Zavoda za sigurnost informacijskih sustava).

Nacionalni CERT osnovan je 30. listopada 2007. godine kada je Upravno vijeće CARNET-a prema obvezama Zakona o informacijskoj sigurnosti donijelo izmjene statuta kojima je uspostavljen Odjel za Nacionalni CERT. Do tada, jedini CERT u Republici Hrvatskoj bio je CARNET CERT koji je osnovan 1996. godine. 2013. godine Nacionalni CERT preuzima sve poslove koje je obavljao CARNET CERT. Tako je CARNET omogućio bolju brigu o sigurnosti javnih informacijskih sustava kroz djelatnost Nacionalnog CERT-a te pružio kvalitetniju uslugu korisnicima u sustavu znanosti i obrazovanja kroz aktivnosti tadašnjeg CARNET-ovog Odjela za računalnu sigurnost (2016. godine i taj je odjel pripojen Odjelu za Nacionalni CERT). Nakon ustrojstva Nacionalnog CERT-a započinje uspostava hijerarhijski ustrojene infrastrukture CERT timova koja je nužna za preventivno djelovanje i učinkovitu koordinaciju pri rješavanju računalno-sigurnosnih incidenata vezanih uz informacijsko-komunikacijske sustave.

Kibernetička sigurnost

Kibernetička sigurnost je temelj sigurnog djelovanja i poslovanja u ovom digitalnom, informacijskom dobu u kojem živimo te joj se posvećuje sve više pažnje i sve se više o njoj govori. Iako smo svjesni nekih opasnosti i prijetnji, često ne znamo dovoljno o njima da bismo ih mogli prepoznati i zaštititi se. Međutim, korištenje zdravog razuma te kritičko promišljanje o kibernetičkoj sigurnosti podiže razinu vaše sigurnosti, a time i razinu sigurnosti vaših bližnjih, prijatelja i poslovnih kolega.

Zlonamjerni korisnici

Kada govorimo o kibernetičkoj sigurnosti, uvijek si moramo postaviti pitanje: „Kako bi **napadač** mogao ostvariti svoj naum i doći do mojih podataka ili ostvariti pristup do mojeg računala?“. Odgovora na ovo pitanje je mnogo i zasigurno ih ovdje ne možemo nabrojati sve, ali vam možemo prikazati neke koje najčešće susrećemo i koji korisnicima predstavljaju najveću prijetnju.

Black hat – pojedinci koji svoje znanje o informacijsko-komunikacijskim sustavima koriste na zlonamjeran način. Često su tvorci zlonamjernih sadržaja kojima žele ukrasti neke podatke ili ih izmijeniti, a mnogi od njih rade isključivo zbog novčane dobiti.

White hat – etički hakeri koji svoje znanje koriste kako bi povećali razinu sigurnosti nekog sustava. Iz nesebičnih i dobronamjernih razloga pronalaze sigurnosne propuste te ih prijavljuju. Svojim radom brinu o sigurnosti mnogih sustava te razvijaju inovativna sigurnosna rješenja.

Grey hat – pojedinci s velikim znanjem o načinu rada informacijsko-komunikacijskih sustava koji su kombinacija black i white hat-a. Iako vlastite vještine i znanja često ne koriste za osobni dobitak, mogu imati dobre i loše namjere.

OPASNOSTI NA INTERNETU

Pristupajući internetu otvaramo prozor u globalni virtualni svijet u kojem u djeliću sekunde možemo pristupiti gotovo beskonačnoj količini informacija, vijesti, slika, filmova, glazbe i ostalih sadržaja. Također, internet nam omogućava da neposredno i u stvarnom vremenu komuniciramo s bilo kime bez obzira na mjesto ili vrijeme jer je osmišljen kao globalna, javno dostupna mreža koja bi trebala biti svima slobodna za korištenje. Nažalost, ne razmišljaju svi korisnici interneta na taj način, a upravo su zlonamjerni korisnici interneta razlog iz kojeg je važno promišljati o kibernetičkoj sigurnosti.

Socijalni inženjering – skup tehnika i metoda kojima se zlonamjerni korisnik služi kako bi ostvario neku korist koja nama nije u interesu.

Zlonamjerni korisnici nas pokušavaju ili prevariti korištenjem **socijalnog inženjeringa** kako bi od nas dobili neke povjerljive ili osobne podatke ili nam čak ukrali novac ili na naše uređaje pokušavaju isporučiti zlonamjerni sadržaj. Važno je za osvijestiti kako se zlonamjerni sadržaj može nalaziti i u datotekama za koje smatramo da su sigurne kao što su dokumenti (.pdf, .docx, .xlsx...) čak i kada nam ti dokumenti djeluju legitimno i dobronamjerno.

Kako bismo se zaštitili, moramo sve aplikacije koje dolaze u kontakt s datotekama što ih preuzimamo s interneta redovito ažurirati kako bi se na vrijeme primijenile sigurnosne zakrpe njihovih proizvođača.

Kako danas najviše vremena na računalu provedemo surfajući putem internetskog preglednika, sigurnost te aplikacije predstavlja važan dio u osobnoj sigurnosti korisnika. Pokušajte što češće ažurirati vaš internetski preglednik kako biste umanjili mogućnost da zlonamjerni korisnik ostvari pristup do vašeg računala.

Prijevare

U posljednje vrijeme sve češće govorimo o internetskim prijevarama. Kako se danas sve transakcije mogu obaviti korištenjem određenih osobnih informacija, te su informacije zlonamjernim korisnicima vrlo zanimljive, a upravo je prikupljanje informacija cilj velikog broja kibernetičkih napada. Zlonamjerni korisnici s tako prikupljenim informacijama mogu, u naše ime, naručivati proizvode putem interneta, ugovarati usluge, upravljati našim bankovnim računalima, ali ih mogu i iskoristiti za daljnje napade.

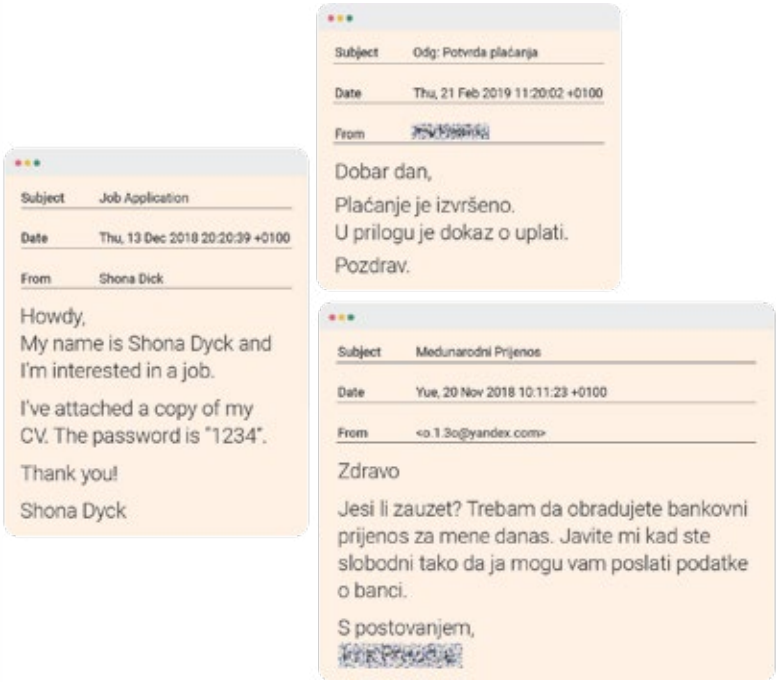
Najčešći način kojim se prikupljaju te informacije zove se **phishing** i temelji se na slanju poruka elektroničke pošte velikom broju korisnika u kojima ih se nastoji nagovoriti da svoje osobne podatke pošalju u povratnoj poruci, da ih pošalju na neku drugu adresu ili da ih upišu na nekoj internetskoj stranici čija je adresa dostavljena u tekstu poruke.

Phishing –
od engleskog *fishing* što znači pecanje. Jednostavno rečeno, zlonamjerni korisnici pecaju naše podatke.

Tipovi phishing-a

1. Vishing
Vishing se odnosi na krađu identiteta putem telefonskih poziva. Budući da se glas koristi za ovu vrstu krađe identiteta, ona se naziva vishing → voice + phishing = vishing.

2. Smishing
SMS phishing je jedan od najlakših vrsta phishing napada. Korisnik je ciljan pomoću SMS obavijesti koja sadrži izravnu poruku ili detalj iz lažne narudžbe s poveznicom za otkazivanje. Na poveznici se nalazi lažna stranica dizajnirana za prikupljanje osobnih podataka.



3. Catphishing
Catphishing je vrsta online obmane / prevare u kojoj osoba stvara lažni profil na društvenim mrežama odnosno izmišlja postojanje neke osobe s ciljem mamljenja neke stvarne osobe u vezu - obično romantičnu - kako bi izmamila novac, darove ili samo pažnju. No, može poslužiti i kao lažni odnos s ciljem dobivanja informacija ili pristup određenim resursima na koje osoba žrtva ima pravo.

4. Spear phishing
Spear phishing se razlikuje od klasičnog phishinga u kojem se jedna e-poruka šalje milijunima nepoznatih korisnika, u spear phishingu napad cilja određenog korisnika uz pažljivo osmišljen tekst e-poruke.

Ovi napadi imaju veći rizik jer napadači prvo dobro istražuju sve dostupne informacije o korisniku (putem društvenih mreža, organizacijskih podataka, web stranica).

Ova vrsta phishinga se najviše koristi pri napadu na korisnika pojedinca ili na organizaciju.

5. Whaling
Whaling phishing ili tzv. kitolov se ne razlikuje mnogo od spear phishinga, no ciljana skupina je specifičnija / posebnija te ograničena za ovakav tip napada. Ova vrsta napada cilja na direktorske / upravljačke radne pozicije kao što su izvršni direktor, financijski direktor za koje se smatra da su veliki igrači - "kitovi" u informacijskom lancu organizacije. Ovom vrstom napada najviše ciljani sektori su tehnologija, bankarstvo i zdravstvo zbog dva glavna faktora: velikog broja korisnika i veće ovisnosti o podacima.

Phishing je kao metoda iznimno popularan jer od napadača ne iziskuje visoku razinu tehničkog znanja i izvođenje složenih napada. Umjesto toga, napadač koristi socijalni inženjering kako bi žrtvu nagnao da napravi nešto što joj nije u interesu.

Phishing poruke u nekom obliku primamo gotovo svakog dana. Bilo da je riječ o porukama u kojima stoji kako ste osvojili veliki dobitak na lutriji koju niste igrali, bilo da je riječ o porukama u kojima vas kontaktira bogati princ neke afričke države i traži od vas pomoć za koju će vas velikodušno nagraditi ili da je riječ o tome da ste primili poruku u kojoj se napadač predstavlja kao djelatnik vaše banke ili čak poslovni suradnik, phishing se temelji na povjerenju što ga žrtva neopravdano ukazuje napadaču.

U ovakvim je situacijama dobro „stati na loptu" i zapitati se: „Imam li stvarno dalekog rođaka u Africi i čini li mi se izglednim da sam jedini nasljednik njegovog ogromnog bogatstva?", „Bi li me moja banka zaista tražila da im presliku svoje kartice i PIN dostavim putem e-pošte?", „Jesam li zaista mogao biti dobitnik na lutriji, iako ju nisam nikada igrao?". Iako ova pitanja možda djeluju smiješno, i mnogi od nas vjeruju da ne bi mogli biti žrtve phishing napada, napadači iz dana u dan usavršavaju svoju tehniku i pronalaze nove načine napada. Nekada su poruke nigerijskih princeva bile prepune nezgrapno i nepravilno napisanog engleskog jezika, ali danas više nije tako. Jasno napisane poruke bez jezičnih pogrešaka su danas postale standard za phishing poruke, a napadači sve vještiji u prikrivanju svojeg pravog identiteta.

Upravo je zato teško iznijeti neku formulu ili popis indikatora prema kojima bi se **phishing** mogao prepoznati. Najbolje je koristiti zdrav razum te se zapitati koliko je vjerojatno da je poruka koju smo primili legitimna te stoji li iza te poruke stvarna osoba ili zlonamjerni napadač.

ZLONAMJERNI SADRŽAJ

Do sada smo već spominjali zlonamjerni kod, no treba razjasniti o čemu se zapravo radi i u kakvim ga oblicima danas susrećemo. Internet kriminal usko je povezan sa zlonamjernim sadržajem jer je on sredstvo putem kojega zlonamjerni korisnici nanose financijsku i druge oblike štete običnim korisnicima i tvrtkama. Neka istraživanja pokazala su da ritam izdavanja zlonamjernog sadržaja premašuje ritam izdavanja legitimnog sadržaja. Napadači šire velike količine zlonamjernog sadržaja te računaju da će, zbog različitih razloga, uvijek uspjeti zaraziti djelić korisnika koji na neki način dođu u doticaj sa zlonamjernim sadržajem. Skupno, sve oblike svrstavamo pod kategoriju zlonamjernog sadržaja (eng. malware – malicious software), a najzastupljeniji oblici su:

Crypto Ransomware - U zadnje vrijeme sve je više slučajeva u kojima se pojavljuje zlonamjerni ransomware sadržaj koji šifrira korisničke podatke i u zamjenu za njihovo dešifriranje traži uplatu određenih novčanih sredstava.

1. **Zlonamjerni ransomware sadržaj**

Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze zlonamjerni ransomware sadržaj može šifrirati datoteke ili onemogućiti njihovo korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala.

2. **Cryptominer**

Zlonamjerni sadržaj za neovlašteno rudarenje elektroničkih kriptovaluta je relativno nova vrsta zlonamjernog sadržaja čiji je glavni zadatak preuzimanje resursa računala te trošenje istih na rudarenje elektroničkih kriptovaluta bez odobrenja vlasnika računala. Ova je vrsta zlonamjernog sadržaja veoma popularna jer napadači korištenjem resursa mnogih računala stječu novčanu dobit.

3. **Zlonamjerni wiper sadržaj**

Ovoj vrsti zlonamjernog sadržaja primarni je zadatak uništavanje sustava i/ili podataka te ih zbog toga možemo nazivati i brisačima. Napadi ovom vrstom zlonamjernog sadržaja obično uzrokuju velike financijske i reputacijske

štete tvrtkama žrtvama. Akteri koji stoje iza ove vrste napada su najčešće motivirani slanjem političke poruke, sabotiranjem ili jednostavno prikrivanjem vlastitih tragova nakon uspješnog prikupljanja podataka.

4. **Zlonamjerni kod bez datoteke**

Zlonamjerni kod bez datoteke ne ostavlja artefakte/dokaze na lokalnom tvrdom disku prilikom zaraze ciljanog računala zbog čega lako zaobilazi tradicionalne sigurnosne i forenzičke alate temeljene na sigurnosnom potpisu. Tipični napadi iskorištavaju ranjivosti u preglednicima i povezanim programima (Java, Flash ili PDF čitači) ili ih napadači isporučuju koristeći phishing.

5. **Trojanski konj**

Trojanski konj oblik je zlonamjernog sadržaja koji se lažno predstavlja kao neki koristan program kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Termin je, zbog analogije, preuzet iz grčke mitologije. Trojanski konj može izmijeniti operacijski sustav na zaraženom računalu kako bi on prikazivao oglase ili skočne prozore u svrhu ostvarivanja novčane koristi od strane napadača. Opasniji je slučaj kada trojanski konj omogući napadaču potpunu kontrolu nad zaraženim računalom.

6. **Botnet**

Jedna od najvećih prijetnji internetu je prisutnost velike količine kompromitiranih računala. Mreže takvih računala često se nazivaju botnet mreže ili "zombi vojske", a računala koja su njihov dio prisutna su u kućanstvima, školama, poslovnim zgradama i vladama diljem svijeta. Uglavnom se nalaze pod kontrolom jednog (ili nekolicine) hakera, a koriste se za izvođenje raznih oblika napada – od distribuiranih napada uskraćivanja usluga (eng. Distributed Denial-of-Service, DDoS), slanja neželjenih poruka elektroničke pošte, iskorištavanja alata za praćenje pritisaka tipki (eng. keylogger) do širenja tzv. malware programa i sl.

7. **APT (*eng. Advanced persistent threat*) Malware**

Advanced persistent threat (APT) je ciljani kibernetički napad kod kojeg zlonamjerna skupina ili osoba stekne neovlašteni pristup mreži i ostaje nezapažena dulje vrijeme. Namjera APT napada uglavnom je praćenje aktivnosti na mreži i krađa informacija, a ne prouzrokovanje štete na mreži ili u organizaciji. Meta ovih napada su organizacije iz sektora nacionalne obrane, proizvodnje ili financijskog sektora koje obrađuju vrijedne podatke, npr. intelektualno vlasništvo, vojne planove i druge podatke vrijedne za državu ili veliku organizaciju. Ovakve vrste napada velikih su razmjera, s naprednim tehnikama i točno određenim ciljem, a motivi za izvođenje ovakvih napada uglavnom su poslovni ili politički. Kako bi "upali" u mrežu, napadači se koriste naprednim metodama napada, iskorištavaju "zero-day"

ranjivosti, koriste se socijalnim inženjeringom, npr. vrlo dobro pripremljenim ciljanim (*spear phishing*) napadom itd. Kako bi što dulje nezapaženo ostali u mreži napadači koriste napredne metode poput mijenjanja zlonamjernog koda, neprestanog nadziranja i izvlačenja informacija iz mreže korištenjem naredbenog i kontrolnog sustava i sl.

8. Stegware - korištenje steganografije za sakrivanje zlonamjernog koda

Jedna od novijih vrsta širenja zlonamjernog sadržaja je takozvani "stegware" - zlonamjerni program koji se sakrije u sliku, dokument ili čak piksel korištenjem steganografije. Steganografija je znanstvena disciplina koja proučava metode skrivanja informacija u naizgled bezazlene objekte. Iako se donedavno koristila uglavnom u vojne svrhe kako bi se osigurala tajnost podataka jer osoba kojoj podaci nisu namijenjeni nije svjesna postojanja istih, napadači su steganografiju prepoznali kao odličnu priliku za sakrivanje zlonamjernog sadržaja. Velika je prednost za napadače što tradicionalna antivirusna zaštita neće prepoznati zlonamjerni sadržaj.

9. Zlonamjerno oglašavanje (eng. *Malvertising – Malicious advertising*)

Zlonamjerno oglašavanje je korištenje internetskog oglašavanja u svrhu širenja zlonamjernog sadržaja. Najčešće se zasniva na ubacivanju zlonamjernog koda u reklame koje se potom šire putem legitimnih oglašivačkih servisa i internetskih stranica. Oglašivački servisi i reklame pružaju dobar temelj za širenje zlonamjernih sadržaja jer su prilagođene korisnicima i pokušavaju ih privući.

10. Neželjena pošta (eng. *Spam*)

Spam je neželjena elektronička poruka poslana s namjerom oglašavanja raznog reklamnog sadržaja, u svrhu phishing napada ili kao sredstvo distribucije zlonamjernih poveznica. Najčešće se šalje putem elektroničke pošte. Osim u slučaju e-pošte, spam se koristi još i kod elektroničkih foruma, blogova, socijalnih mreža, servisa za izravnu komunikaciju i drugih sustava za razmjenu poruka ili drugih podataka. Širitelji spama nazivaju se spameri (eng. *spammers*).

11. Hoax

Scam je ozbiljniji oblik hoaxa, često s ozbiljnim financijskim, pravnim ili drugim posljedicama za žrtvu.

Hoax je poruka elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja. Želja osobe koja je poslala hoax je njegovo prosljeđivanje na što veći broj adresa. Pri tome ih primatelji doista i prosljeđuju internetom jer su uvjereni da time pomažu drugima. Hoax ne može uzrokovati oštećenja računalnih programa i operacijskih sustava, ali zabilježeni su brojni slučajevi gdje je hoax svojim sadržajem i vještom psihologijom naveo korisnike da sami oštete svoje programe i sustave. Drugi oblik štete koju hoax može nanijeti je zavaravanje korisnika te narušavanje njihovog ugleda, kao i ugleda određenih organizacija, tvrtki i poznatih osoba.

BEŽIČNE MREŽE

Današnja prijenosna računala standardno dolaze s opremom za povezivanje na bežične mreže. Oprema koju dobivate kada preuzimate priključak na internet također uglavnom dolazi s bežičnom pristupnom točkom. Bežične su mreže svuda oko nas i omogućavaju nam veću mobilnost i udobnost. Također, ako nisu ispravno podešene, omogućavaju svakome u našoj blizini da se u njih uključi, prisluškuje i pristupa internetu koristeći naš priključak.

Ako koristimo samo jedno stolno računalo u kući, lako se zaštititi od bežičnih opasnosti - jednostavno spojimo računalo na uređaj za pristup internetu koristeći običan mrežni kabel te isključimo bežični primopredajnik na pristupnom uređaju i na računalu. Upute za isključenje bežičnog primopredajnika dobivamo s uređajem, a ako smo ih izgubili možemo se savjetovati s korisničkom podrškom.

WEP standard sadrži propuste zbog kojih je moguće "ukrasti" ključ unatoč šifriranju i nije preporučljiv za korištenje. Svakako izbjegavajte korištenje WEP standarda!

Ako nam je bežična mreža potrebna, prvo trebamo osigurati ispravnu kontrolu pristupa i šifriranje informacija koje se radio-valovima šire kada računalo komunicira s pristupnom točkom. Većina pristupnih uređaja i računala nudi WEP, WPA i WPA2 standarde šifriranja te korištenje kraćeg ili dužeg ključa za kontrolu pristupa.

Preporuka je korištenje WPA2 protokola uz AES metodu šifriranja koja se u slučaju nekih proizvođača naziva WPA2 Personal. Svakako koristite potpuno nasumičan ključ - bez riječi, imena, datuma ili bilo čega drugog smislenog. Računalo će pohraniti vaš ključ i više vas za njega neće pitati te nema potrebe da bude lako pamtljiv. Uz dovoljno dugu lozinku vrlo je teško dešifrirati bežičnu komunikaciju prilikom korištenja WPA-AES protokola.

Koristimo li tuđe pristupne točke,
potrebno je obratiti pažnju na dvije stvari:

1. Radi li se o nezaštićenoj (nešifriranoj ili šifriranoj WEP protokolom) mreži?

2. Znamo li kome mreža pripada i možemo li mu vjerovati?

Kada pristupamo nezaštićenoj bežičnoj mreži, sva računala u dometu mogu "preslušavati" informacije koje naše računalo odašilje i prima. Na ovaj način mogu se ukrasti lozinke i drugi važni podaci, a u nekim slučajevima moguće je pristupiti i sadržaju tvrdog diska vašeg računala. Ako je vaše računalo pritom još i ranjivo, moguće je potpuno preuzimanje kontrole bez vašeg znanja.

Web stranice, klijenti za dopisivanje i druge aplikacije koje već koriste šifriranje odgovarajuće su zaštićene čak i ako mreža na kojoj ih koristimo nije. Svakako provjerite koristi li vaša omiljena aplikacija za razmjenu poruka šifriranje!

Pristupamo li bežičnoj mreži čijeg vlasnika ne poznajemo, izlažemo se istom riziku kao i u slučaju nezaštićene mreže: tko god kontrolira pristupnu točku, može steći pristup našem računalu.

Koristite li javnu bežičnu mrežu, kao npr. u kafiću, provjerite kod osoblja kako se zove pristupna točka kako biste se upravo na nju spojili!

KAKO SE ZAŠTITITI?

Do vašeg je računala moguće doći i bez vašeg odobrenja, ali nije sve tako crno. U većini su slučajeva vaše odluke prva i posljednja linija obrane, a vaša svijest o kibernetičkoj sigurnosti najbolji sigurnosni alat i pomagalo. Kako biste održali vašu kibernetičku sigurnost na visokoj razini, važno je da aktivno slijedite preporuke sigurnosnih stručnjaka te se svakodnevno informirate o temama iz svijeta kibernetičke sigurnosti kako biste, kada do toga dođe, mogli odgovoriti na napad te se uspješno obraniti.

Ako ne znamo što nam prijeti i što sve napadači kriju u svom arsenalu, bit ćemo laka meta. Međutim, ako smo svjesni kakvih sve opasnosti i prijetnji ima, moći ćemo se zaštititi te na ispravan djelovati kada se s njima susretnemo.

Kada govorimo o tehničkoj razini, važno je da računalo zaštitimo odgovarajućim sigurnosnim alatima te na ispravan način podesimo svoj operacijski sustav i aplikacije s kojima se služimo. Danas postoji cijeli niz kvalitetnih besplatnih rješenja koje je potrebno samo preuzeti na vaše računalo kako biste podignuli razinu kibernetičke sigurnosti.

U nastavku izdvajamo važne elemente zaštite i pravila kojih se dobro držati, ali valja imati na umu kako se polje kibernetičke sigurnosti iz dana u dan mijenja te kako navedeni savjeti neće učiniti vaše računalo neprobojnim, ali će vam dati dobar temelj te osnovne smjernice za njegovu zaštitu.

1. Antivirus/antispyware/antimalware

Sigurnosna rješenja za prepoznavanje i zaustavljanje aktivnosti zlonamjernog sadržaja koja su obavezan dio programske opreme vašeg računala. Neka rješenja dolaze u paketima s drugim sigurnosnim alatima (npr. vatrozidom), dok su neka samostalna. Danas je na internetu moguće pronaći niz besplatnih antivirusnih alata koji zadovoljavaju različite kategorije korisnika. Svakako potražite one koji vama najviše odgovaraju te njima zaštitite vaše uređaje.

Kako biste bili sigurni da koristite provjerena sigurnosna rješenja, potražite naše preporuke na stranicama Nacionalnog CERT-a:

https://www.cert.hr/alati/

Vatrozid će vas upitati za odobrenje svaki puta kada neka nova aplikacija pokuša poslati podatke putem mreže. Svako upozorenje pažljivo pročitajte kako biste ostali sigurni!

2. Vatrozid

Aplikacija koja ograničava mrežnu komunikaciju između vašeg računala i interneta. Vatrozid selektivnim propuštanjem prometa izbjegava neovlaštenu komunikaciju i smanjuje mogućnost iskorištavanja sigurnosnih propusta u aplikacijama koje ne koristite, a koje imaju mogućnost mrežne komunikacije. Operacijski sustav Windows od inačice XP već sadrži vatrozid s odgovarajućom zaštitom.

3. Automatsko ažuriranje operacijskog sustava i aplikacija

Sigurnosni propusti u programima stalno se otkrivaju. Kako vas ne bi ostavili ranjivima, uključite automatsko ažuriranje u operacijskom sustavu i svim aplikacijama koje dolaze u kontakt sa sadržajima s interneta (npr. preglednici PDF dokumenata). Operacijski sustav Windows promatra je li automatsko ažuriranje operacijskog sustava uključeno te upozorava korisnika ako nije.

Kako se ne bi izgubili u moru lozinki ili morali pamtiti složene lozinke, možemo se služiti upravljačima lozinaka (eng. password managers) koji vaše lozinke kriptiraju i štite jednom glavnom lozinkom (eng. master password). Kako biste se zaštitili, važno je da glavna lozinka bude složena jer u slučaju probijanja te lozinke, napadač ostvaruje pristup do svih vaših lozinki!

4. Složene i različite lozinke

Današnja su računala dovoljna snažna da mogu iznimno brzo isprobavati različite kombinacije imena i lozinki pa su zato lozinke koje sadrže riječi iz govornog jezika, datume, imena i slično iznimno jednostavne za pogađanje. Dobra lozinka sastoji se od najmanje 12 znakova, te je kombinacija velikih i malih slova, brojki te specijalnih znakova.

5. Sigurnosne kopije i njihova pohrana

Danas je korištenje računala u poslovne svrhe potpuno uobičajena stvar te velika većina korisnika na računalu pohranjuje važne i povjerljive podatke čiji bi gubitak predstavljao značajan udarac na poslovanje ili privatnost. Na sreću, ovom je problemu veoma lako doskočiti izradom sigurnosnih kopija i pohranom tih kopija ili na specijalizirane internetske servise ili na vanjske medije koji nisu povezani mrežom.

6. Informiranje o kibernetičkoj sigurnosti

facebook.com/CERT.hr/
twitter.com/HRCERT
cert.hr/

Kako bi se znali zaštititi, moramo znati što nam i kako prijeti. S ovim nam pomaže niz specijaliziranih internetskih portala koji svakodnevno pišu o zanimljivostima iz svijeta kibernetičke sigurnosti. Nacionalni CERT svakodnevno objavljuje informacije o novim trendovima u svijetu kibernetičke sigurnosti u obliku koji je prilagođen svim korisnicima bez obzira na razinu tehničkog znanja.

Što je HTTPS i što čini ispravan certifikat? Svaka web stranica kojoj pristupamo na početku svoje adrese u adresnoj traci sadrži oznaku protokola.

7. Upisivanje podataka na internetu

Internet nam omogućuje da iz udobnosti svojeg doma kupujemo robu i usluge korištenjem naše kreditne kartice ili nekog drugog servisa za internetsko plaćanje. Takve su stranice posebno atraktivna meta za napadače i moramo biti na posebno oprezni kada upisujemo svoje povjerljive podatke na internetskim stranicama jer ih vješt napadač može presresti i iskoristiti ih kako bi stekao novčanu ili neku drugu dobit.

Uz HTTP, postoji i HTTPS, sigurniji protokol koji podrazumijeva i da je stranica ispravno certificirana. Prije upisivanja podataka uvjerite se da stranica koristi HTTPS protokol i da je označena kao sigurna.

DRUŠTVENE MREŽE I APLIKACIJE ZA RAZMJENU PORUKA

Društvene mreže su fenomen karakterističan za 21. stoljeće i često iz šale znamo reći „ako nije bilo na fejsu, nije se ni dogodilo!". Nažalost, iako su donijele prethodno neviđenu razinu komunikacije, društvene su nas mreže učinile ranjivima na napade zlonamjernih korisnika. Posebno su ranjivi korisnici koji bez zadrške prihvaćaju svaku inovaciju te bez straha koriste tehnologiju ne razmišljajući pritom o rizicima i prijetnjama. Kako bismo učinili društvene mreže sigurnijim mjestom, sve korisnike valja educirati o opasnostima, ali nikako u njima ne smijemo probuditi strah ili ih otjerati s interneta. Kada se služimo internetom i društvenim mrežama, trebali bismo biti hrabri, oprezni i znatiželjni, ali odgovorni. Čini se kao težak posao koji je teško ostvariv, ali tom cilju treba težiti. Sljedeće poglavlje donosi pregled najpopularnijih društvenih mreža te kratak opis za one koji se s njima prvi put susreću.

1. **Instagram**
Minimalna dob za registraciju: 13 godina

Korisnici mogu snimati, uređivati i dijeliti fotografije i kratak video sadržaj. Postavke privatnosti mogu biti podešene tako da sadržaj učine javno dostupnim ili privatnim. Sama platforma dopušta dijeljenje i komentiranje sadržaja. Sve dok je korisnički račun privatan, nitko ne može pogledati ili komentirati objavu. Rizici uključuju dijeljenje neprimjerenog sadržaja među prijateljima te javno dijeljenje lokacije na temelju oznaka lokacije.

2. **WhatsApp**
Minimalna dob za registraciju: 16 godina

Veoma popularna aplikacija za razmjenu poruka, WhatsApp korisnicima omogućava da šalju tekstualne poruke, zvučne zapise, video sadržaj i fotografije jednoj ili više osoba bez naknade. WhatsApp korisniku ograničava pristup na samo one korisnike koje ima u imeniku. Međutim, korisnici koji se nalaze u istim grupama kao vi, mogu komunicirati s vama čak i ako ih nemate u imeniku.

3. **Snapchat**
Minimalna dob za registraciju: 13 godina

Popularna aplikacija za dijeljenje fotografija, Snapchat korisnicima dopušta dijeljenje fotografija i video sadržaja unutar određenog vremenskog perioda. Sam sadržaj se automatski briše nakon što vremenski period prođe. Međutim, valja imati na umu kako zlonamjerni korisnici mogu preslikom ekrana sačuvati sadržaj te ga na taj način pohraniti. Snapchat kod korisnika budi lažnu sigurnost jer smatraju da će se sadržaj uvijek obrisati, ali postoje načini kako se ovo može zaobići. Također, opcija *Discover* (hrv. Otkrij) može omogućiti djeci pristup do zlonamjernog ili neprimjerenog sadržaja.

4. **Twitter**
Minimalna dob za registraciju: 13 godina

Mikrobloging servis koji sadrži opciju koja korisniku omogućava da svoje objave učini javno dostupnima ili privatnima. Najčešće ju koriste korisnici koji žele pratiti svoje prijatelje, bližnje i kolege te poznate osobe. Iako Twitter ima opciju za brisanje vaših objava, objavljeni sadržaj mogao je biti kopiran ili pohranjen.

5. **Facebook**
Minimalna dob za registraciju: 13 godina

Globalno popularna društvena mreža koja korisnicima dopušta da dijele fotografije, video i ostali sadržaj te ga komentiraju. Također, Facebook posjeduje svoju aplikaciju za razmjenu poruka zvanu Messenger. Putem Facebooka korisnici održavaju kontakt s bližnjima, prijateljima, kolegama, ali i prate događaje, razne stranice te mogu biti članovi raznih grupa.

6. **YouTube**
Minimalna dob za registraciju: 13 godina

Popularna usluga za razmjenu video sadržaja na kojoj korisnici mogu postavljati, pregledavati i ocjenjivati video sadržaj. Za pregledavanje sadržaja nije potrebna registracija, ali je potrebna za komentiranje i postavljanje vlastitog sadržaja. YouTube korisnicima brani postavljanje pornografskog sadržaja, nasilja, sadržaja koji podržava kriminalne radnje, sadržaja s ciljem sramoćenja, klevete i reklama.

SIGURNOST NA DRUŠTVENIM MREŽAMA

Kako bismo se zaštitili na društvenim mrežama, dobro je postaviti si sljedeća pitanja:

1. **Znam li sve svoje prijatelje na društvenim mrežama?**
Mnogi od nas na društvenim mrežama dodaju korisnike koje ili ne poznaju ili nisu sigurni u njihov stvarni identitet. Trebamo biti sigurni s kim komuniciramo i nikako ne ulaziti u interakciju s korisnicima koji su nam nepoznati.

2. **Je li internet mjesto bez zakona, digitalni pješčanik?**
Ne. Sve što se događa na internetu izravno je povezano sa stvarnim životom. Štoviše, sa svakim će danom biti sve teže razgraničiti stvarni život od virtualnog tako da što prije treba osvijestiti kako postupci na društvenim mrežama mogu rezonirati i u stvarnom životu.

3. **Trebam li na društvenim mrežama objavljivati osobne i povjerljive informacije?**
Takvo što, u svakom slučaju, nije dobra ideja i može imate dalekosežne posljedice kojih nismo svjesni u trenutku objavljivanja sadržaja. Stoga je važno uvijek imati na umu kako sve što objavimo postaje dio našeg digitalnog otiska.

4. **Trebam li paziti da ne objavljujem svoju lokaciju na društvenim mrežama?**
Svakako, jer vješt napadač ili bilo koji zlonamjerni korisnik može taj podatak iskoristiti i uzrokovati štetu. Lokacija je osobni podatak iako se mnogima od nas ne čini tako te s njom treba postupati kao i s ostalim osobnim podacima – pažljivo i odgovorno. Također, ponekad se lokacija može ustanoviti na temelju objavljene fotografije te je i ovdje veoma važno paziti koje informacije kome otkrivamo.

5. Trebam li ispunjavati svaki upitnik na kojeg naiđem na društvenim mrežama?

Ispunjavanje upitnika na društvenim mrežama rijetko je kada dobra ideja i može biti potencijalna prijetnja. Pogotovo treba biti oprezan prilikom ispunjavanja upitnika koji od vas traže neke povjerljive ili osobne podatke uz obećanje kako ćete, ako ispravno ispunite upitnik, dobiti neku nagradu. U ovakvim je situacijama važno osvijestiti kako su u tom odnosu vaši podaci kapital i nagrada, a korisnici koji ulaze u sumnjive odnose se moraju upitati za koliko su spremni svoje podatke ustupiti na slobodno korištenje potencijalno zlonamjernom korisniku.

6. Treba li dopustiti vanjskim aplikacijama pristup do mog korisničkog računa?

Ponekad nam se na društvenim mrežama može dogoditi da pokrenemo aplikaciju koja od nas traži pristup do korisničkih podataka našeg profila. Iako mogu djelovati bezazleno na prvu, ovakve aplikacije mogu dijeliti osobne ili povjerljive podatke bez našeg saznanja. Poznate aplikacije prilikom povezivanja s vašim korisničkim računom navode što im je potrebno te na koji će se način s vašim podacima služiti. Svakako obratite pozornost da aplikacije kojima se služite jasno navedu za što će i kako vaše podatke koristiti kako bi se zaštitili.

ZLATNA PRAVILA SIGURNOSTI

Detalje svake opasnosti koja nam prijeti na Internetu nije lako upamtiti. Zato smo vam pripremili ovaj brzi podsjetnik o osnovnim koracima koji vas mogu učiniti sigurnijima u svakodnevnom korištenju računala. Želite li bolje razumjeti neko od ovih pravila, uvijek se možete vratiti na prethodna poglavlja na koja se ovdje upućuje.

1. Redovito ažurirajte operacijski sustav i sve aplikacije koje dolaze u kontakt sa sadržajima na internetu

2. Koristite dobru enkripciju na kućnoj bežičnoj mreži i javne bežične mreže kojima vjerujete

3. Koristite kompleksne lozinke za pristup javnim servisima (društvenim mrežama, elektroničkoj pošti i sl.)

4. Poslujete li s karticama ili koristite servise koji u vaše ime mogu obavljati transakcije, provjeravajte ispravnost certifikata servisnih stranica

5. Sve novčane transakcije, a posebno rad s elektroničkim bankarstvom, obavljajte s računala koje je najmanje izloženo riziku zaraze

6. Uvijek sami u internetskom pregledniku upisujte adresu stranice na kojoj poslujete novcem, ne koristite poveznice iz primljenih poruka

7. Kada primite poruku u kojoj vam se nudi ili se od vas traži nešto neočekivano, provjerite je li riječ o prijevari

8. Čuvajte sigurnosne kopije najvažnijih podataka i pri povratu sigurnosne kopije provjerite sadržaj antivirusnim alatom

9. Ne ugrađujte u računalo aplikacije iz nepoznatih i neprovjerenih izvora, posebno ako se radi o sigurnosnim alatima

10. Ne isključujte vatrozid i antivirusni alat i ne ignorirajte njihova upozorenja

CERT.hr

Hrvatska akademska
i istraživačka mreža

CARNET

Projekt je sufinanciran sredstvima CEF - Connecting Europe Facility programa Europske komisije, broj ugovora: INEA/CEF/ICT/A2016/1334308 (Action No: 2016-HR-IA-0085)

Sufinancirano instrumentom Europske unije za povezivanje Europe