Slovenski vojaki in
vojakinje ponosni in

VARNI TUDI NA SPLETU

si·cert

Slovenski vojaki in vojakinje ponosni in varni tudi na spletu

Slovenska vojska razvija zmogljivosti kibernetske obrambe. Zavedamo se, da je v procesu kibernetske varnosti ključni in najšibkejši člen ravno človek kot uporabnik informacijsko-komunikacijskega sistema. Še tako napredna tehnologija ali stroga varnostna politika nas ne bo popolnoma zaščitila pred lastno neprevidnostjo ali nepremišljenostjo. V sodelovanju z nacionalnim odzivnim centrom za obravnavo omrežnih incidentov SI-CERT smo izdali priročnik s kratkimi nasveti, kako pripadniki Slovenske vojske postanete in ostanete varni na spletu.

Želimo si, da bi vsak pripadnik Slovenske vojske priročnik prebral in uporabne nasvete delil s svojo družino in prijatelji. Čim več znanja bomo imeli, tem varnejši bomo! Z izdajo knjižice, ki je pred vami, nadaljujemo uspešno sodelovanje odzivnega centra SI-CERT in Slovenske vojske.

Ostanite varni, v kateremkoli omrežju že ste.

Odsek za kibernetsko varnost

si·cert
Nacionalni center za posredovanje pri omrežnih incidentih

Po pameti s pametnimi napravami

Pametna naprava (pametni telefon, tablica, pametna ura in podobno) je po vsebini in namenu v tem času več kot samo orodje za komunikacijo. Postala je naše okno v svet, hkrati pa omogoča pogled v naše življenje. Če je naprava neustrezno zaščitena, ima »najditelj« oziroma novi lastnik vpogled v številne intimne informacije, ki jih naprava hrani, ter s tem dostop do naših fotografij, videoposnetkov, blogov, forumov, spletnega bančništva, računa PayPal, elektronske pošte, SMS-sporočil, profilov na družabnih omrežjih, koledarja, podatkov o tem, kje smo, ter drugih spletnih storitev in aplikacij.

PRVA POMOČ PRI UKRADENI ALI IZGUBLJENI NAPRAVI ANDROID

1.

Prvi, nujen korak je obisk strani https://myaccount.google.com/find-your-phone, kjer poskušate poiskati oziroma zakleniti telefon. Najprej se vpišete v svoj Google račun in izberete napravo, ki jo iščete. Najprej lahko poskusite sprožiti zvonjenje, če je telefon morda v bližini, ali možnost Poišči lokacijo naprave. Pozor, to je mogoče, samo če ste v telefonu prej že vklopili lokacijo.

2.

Najprej poskusite zakleniti telefon in kontaktirati najditelja. Tako najditelju omogočite, da vas pokliče in vam telefon vrne, hkrati pa preprečite dostop do podatkov na telefonu (dostop do imenika, aplikacij itd.)

3.

Če glede na nastalo situacijo ocenite, da je telefon ukraden oziroma za vedno izgubljen, je NUJEN KORAK odjava iz obstoječega računa Google. To je najbolje narediti čim prej, sicer lahko neznanec dostopa do vašega računa za Gmail in vseh povezanih storitev (Google Drive, Facebook, Twitter, PayPal). Pametno je tudi, da na daljavo izbrišete podatke v napravi. To seveda ne pomeni, da boste izbrisali svoj račun Google, ampak le podatke, ki so shranjeni v napravi.

4.

Pokličite svojega operaterja in prekličite kartico SIM. Nekdo bi lahko uporabljal vašo številko in vam povzročil stroške.

5.

Če krajo prijavite policiji, jim sporočite tudi številko IMEI naprave. Zapisana je na embalaži, na garancijskem listu in na nalepki pod baterijo telefona. IMEI se izpiše tudi na zaslonu telefona po vnosu ukaza *#06# in Kliči. Zapišite si jo in shranite na varno mesto! S poznavanjem številke IMEI lahko operater prepreči, da bi kdo uporabljal vašo napravo v njegovem omrežju ne glede na vstavljeno kartico SIM.

PREVENTIVNI UKREPI

1. Zaklepajte zaslon naprave vsaj z vzorcem, še bolje pa s številko PIN, geslom ali prstnim odtisom. Bodite previdni pri izbiri številke PIN – naj ne bo rojstni datum ali številka, ki jo lahko drugi uganejo. Ob morebitni razstavitvi naprave in strojnega dostopa do vsebine v napravi vas zaklepanje zaslona ne varuje. V tem primeru je potrebno tudi šifriranje vsebine naprave.

2. Nastavite šifriranje vsebine naprave in kartice SD. S tem preprečite dostop do vsebine pri fizičnem vdoru v napravo.

NALAGANJE APLIKACIJ

Za svoje potrebe ali zabavo v naprave nalagamo različne aplikacije.

1. Aplikacije vedno nameščajte samo iz uradnih trgovin (npr. Google Play ali Apple Store). V nastavitvah izberite možnost, ki onemogoči nalaganje aplikacij iz neznanih virov.

2. Marsikatera aplikacija, še posebej to velja za brezplačne, med namestitvijo od nas zahteva, da ji omogočimo dostop do številnih podatkov. Na primer, preprosta aplikacija za bujenje lahko zahteva dostop do naših stikov in slik ali želi dovoljenje za snemanje zvoka. V takem primeru je najbolje prekiniti proces namestitve in izbrati drugo aplikacijo, ki zahteva manj podatkov. Običajno je cena za brezplačne aplikacije skrita drugje: v vrednosti, ki jo imajo naši podatki za oglaševalce. Zato vedno preverite, katera dovoljenja zahteva aplikacija.

3. Vprašajte se, ali aplikacijo res potrebujete. Ko aplikacijo prenehate uporabljati, jo odstranite.

NAKUP PAMETNIH ELEKTRONSKIH NAPRAV

Številne tuje spletne trgovine, predvsem kitajske, ponujajo mobilne naprave in elektroniko po občutno nižjih cenah. Tehnične lastnosti izdelkov se zdijo povsem primerljivi, vendar se morate zavedati, da smo kupci pri nakupih zunaj Evropske unije veliko manj zaščiteni. Na prvi pogled poceni izdelek nas lahko na koncu še kako drago stane!

Spletni kupci so manj zaščiteni, če nakupujejo pri ponudnikih, ki so zunaj Evropske unije (Kitajska, ZDA, Indija), saj ti niso zavezani k spoštovanju skupne evropske zakonodaje. To pomeni, da kot kupec ne morete odstopiti od pogodbe, zahtevati vračila kupnine ali zamenjati blaga. Če z izdelkom niste zadovoljni, žal velja pravilo »Kar dobiš, to imaš«, saj naše potrošniške pravice sežejo le do evropskih meja.

Nezadovoljnemu kupcu preostane samo dopisovanje s trgovcem in le od trgovčeve dobre volje je odvisno, ali bo pritožbo upošteval. Največkrat se na SI-CERT obrnejo kupci, ki so v spletni trgovini kupili ponaredek znane blagovne znamke in so nezadovoljni s kakovostjo prejetega blaga.

VARNO POVEZOVANJE V INTERNET

1.

Za povezovanje v internet raje izberite mobilni prenos podatkov kot pa brezplačno omrežje Wi-Fi, če paket pri vašem ponudniku mobilne telefonije to omogoča in so stroški gostovanja v tujini za vas sprejemljivi. Uporaba javnega omrežja Wi-Fi pa je še vedno varnejša kakor uporaba javnih računalnikov, saj v splet vstopate prek svoje ustrezno zaščitene naprave. Uporaba javnih računalnikov je primerna za pregled vremenske napovedi, novic, nikoli pa za storitve, v katere se prijavite z geslom (Facebook, e-pošta, PayPal, e-bančništvo ipd.).

2.

Vedno preverite, katero je uradno brezžično omrežje (SSID), ko ste na letališču, v restavraciji, kampu ali kateremkoli drugem mestu, kjer vam v sklopu storitev ponujajo brezplačen Wi-Fi.

3.

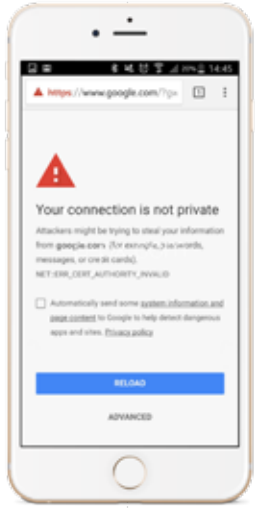
Če imate na voljo šifrirano in nešifrirano omrežje, se odločite za šifrirano in si priskrbite geslo za Wi-Fi.

4.

Za dostop do storitev, ki zahtevajo vpis uporabniškega imena in gesla, namesto spletnega brskalnika raje uporabite aplikacijo, saj praviloma že sama aplikacija poskrbi za šifrirano povezavo in s tem neko stopnjo zaščite. V brskalniku pa pri vpisu podatkov vedno preverite, ali gre za varen prenos (HTTPS in znak ključavnice).

5.

Vedno predpostavljajte, da dostopna točka nima ustrezne zaščite in da v omrežju vaš promet lahko prestrezajo nepovabljene osebe. Če pri povezovanju v izbrano brezžično omrežje v brskalniku naletite na opozorilo o neveljavnem digitalnem certifikatu, je to morda znak, da nekdo skuša prestrezati vaš promet. V takem primeru prekinite povezavo in izberite drugo omrežje.



Prav posebno previdnost pa zahteva t. i. ad-hoc brezžično omrežje, ki ga kdo ustvari kar na svojem računalniku. V tem

primeru se povežete neposredno na prenosnik neznanca! Taka omrežja so po navadi prikazana z malce drugačno ikono. Zato se vedno pozanimajte, katero je pravo omrežje hotela ali cybercafeja.

6.

Da se izognete nenadzorovanemu povezovanju naprave v brezžična omrežja, v nastavitvah onemogočite samodejno povezovanje v omrežja Wi-Fi.

7.

Za dostop do spletnih storitev, pri katerih bi morebitna kraja vaših prijavnih podatkov imela hujše posledice (npr. služba, spletno bančništvo), vedno uporabite zaščiteno povezavo VPN.

PRILAGODITEV NAPRAV ZA MISIJE ALI PODOBNE DOGODKE

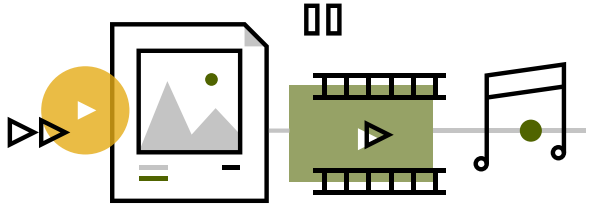
Vedno, ko se odpravljate na dogodke v tujini oziroma v okolja, ki so sporna ali niso domača, prilagodite pametne naprave, s katerimi se boste povezovali v omrežja.

Pred odhodom na MOM, mednarodno vajo ali seminar v tujini očistite pametne naprave vseh podatkov, katerih odtujitev bi imela neugodne posledice za vas ali Slovensko vojsko. Poleg tega po vrnitvi napravo »sterilizirajte« oziroma ponastavite na tovarniške nastavitve ali preprosto obnovite arhivsko kopijo, ki je bila ustvarjena pred odhodom. Kajti nikoli ne morete biti prepričani, da se vaša naprava v spornem okolju ni okužila s škodljivo kodo, ki bo neznani osebi omogočila nadzor nad vašo napravo ali odtekanje podatkov iz nje.

Hkrati morate biti pri vsakršni aktivnosti v tujini pazljivi pri uporabi mobilnih naprav, saj vas lahko prek njih spremljajo. Pazljivi morate biti tudi pri objavljanju vsebin na družabnih omrežjih, uporabi fotoaparata in snemanju videoposnetkov, da ne izdate občutljivih službenih informacij.

Pasti družabnih omrežij

Vedno imejte v mislih, da so družabna omrežja javen prostor, zato dobro pretehtajte, katere informacije boste delili z drugimi. Podatke, slike in videoposnetke, ki jih boste objavili, izbirajte preudarno.



Fotografije in videoposnetki, ki jih objavite, lahko povsem nehote razkrijejo stvari, ki jih ni pametno deliti z drugimi, na primer tehnično opremo v stanovanju (TV, osebni računalnik), lokacijo in razmestitev objektov na vaji ali MOM, osebe, ki so sodelovale na vojaških urjenjih, oborožitev ali celo nastavitev radijskih postaj in podobno. Iz fotografij, ki jih objavljajo naši pripadniki na MOM, je mogoče določiti število objektov, šotorov v namestitvenih rajonih, rutine pripadnikov, opremo, točne lokacije in druge pomembne podrobnosti. Poleg tega lahko pripadniki zaradi razširjenega zmotnega mnenja, da za misije prejmejo velika finančna sredstva, postanejo tarče manjših izsiljevanj ali goljufivih investicijskih ponudb.

Na Facebooku za prijatelje potrdite le osebe, ki jih dejansko poznate, in objave delite le v krogu potrjenih prijateljev! Močno priporočamo, da omejite vidnost samo na prijatelje, saj bodo drugače vsi, tudi tisti, ki sploh nimajo profila na Facebooku, videli vse vaše objave. Prav tako je koristno, da ne delite seznama prijateljev, saj tako razkrijete, s kom se družite in v katerem okolju nastopate.

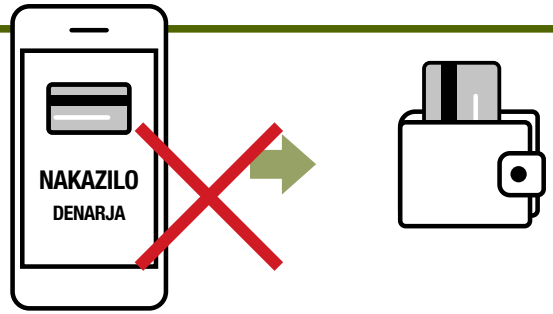
NE NASEDAJTE LAŽNIM NAGRADNIM IGRAM, ki vam v zameno za en sam všeček obljubljajo vredne nagrade ali kupone za nakupovanje. V večini primerov gre le za poceni pridobivanje všečkov, tovrstne nagradne igre pa lahko vodijo v plačljive SMS-klube, ki vas utegnejo stati 20 evrov na mesec.

SEXTORTION – IZSILJEVANJE Z INTIMNIMI POSNETKI

Predstavljajte si, da vas na Facebook doda privlačna neznanka. Po začetnem klepetu vas povabi na Skype, in ko prižgete kamero, je na drugi strani brez oblačil. Povabi vas, da še vi odvržete svoja. In vam seveda obljubi, da bo to vajina mala skrivnost. Kmalu za tem, ko prejme vaš posnetek ali fotografije (ali vas posname s spletno kamero), grozi z njihovo objavo, če ji ne boste nakazali denarja. Finančne zahteve so v vseh obravnavanih primerih precejšnje, znašajo lahko tudi več tisoč evrov. Izsiljevalci ustvarjajo izjemno velik psihični pritisk na žrtev, grozijo z organi pregona, FBI-jem, tožbami zaradi posredovanja pornografije, predvsem pa, da bodo posnetek razposlali vsem prijateljem, družini, nadrejenim. Svoje grožnje morda tudi uresničijo ter posnetke in fotografije objavijo na YouTubu in Facebooku, žrtev pa o tem obvestijo, da bi stopnjevali pritisk in jo še naprej izsiljevali.

Za izzivalnimi profilnimi fotografijami se skrivajo organizirane kriminalne združbe, njihov edini cilj pa je prepričati sogovornike, da se slečejo pred spletno kamero ali sami pošljejo svoje gole fotografije. Žrtve izsiljevanja so plačila nakazovala prek sistema Western Union, denar pa je romal na Slonokoščeno obalo. Upanja na uspešen pregon tovrstnega kriminala skoraj ni, saj naši organi pregona v afriških državah nimajo nobene pristojnosti.

Zato žrtvam svetujemo, naj nemudoma in v celoti prekinejo vso komunikacijo z izsiljevalci. Nikakor ne nakazujte denarja in ne nasedajte obljubam, da bodo po plačilu sporne posnetke izbrisali. Nasprotno, izsiljevalci bodo zahtevali čedalje večje zneske. Če bodo posnetke javno objavili po internetu, se lahko obrnete na cert@cert.si za pomoč pri odstranjevanju teh vsebin.



Na koncu se vedno izkaže, da za spletno varnost lahko največ storimo uporabniki sami.
ZATO NE SPREJEMAJTE PROŠENJ ZA PRIJATELJSTVO OD NEZNANCEV, NE ZAPLETAJTE SE V KOMUNIKACIJO Z NJIMI IN NIKOLI NE SODELUJTE V IZMENJAVI INTIMNIH FOTOGRAFIJ Z NEZNANCI.

Goljufije pri spletnem nakupovanju – ko dobra kupčija pusti luknjo v denarnici

Prednosti, ki jih svetovni splet prinaša v naša življenja, nedvomno odtehtajo tveganja, na katera lahko naletimo. Povsem enako velja za spletne trgovine, saj ponujajo množico izdelkov in storitev po ugodnih cenah. Nakup po spletu je hiter, udoben, preprost, spletni trgovci pa ponujajo vse boljšo uporabniško izkušnjo. Na spletu pa svojo »poslovno« priložnost iščejo tudi spletni goljufi, ki s preprostimi ukanami zavedejo nepozorne kupce.

Na prvi pogled odlična kupčija se na koncu lahko izkaže za zgrešen nakup. Najpogostejše prevare pri spletnem nakupovanju so:

1. Izdelek kupimo v lažni spletni trgovini, plačamo kupnino, vendar izdelka ne prejmemo. Lahko tudi pride do zlorabe kreditne kartice, zato svetujemo preklic, kar pa ustvari še dodatne stroške.

2. Kupimo ponarejen izdelek, misleč, da kupujemo pristno blago. Pri uvoznih postopkih carina ugotovi, da gre za ponaredek, in poleg izgubljene kupnine moramo kriti še stroške uničenja izdelka.

3. Izdelek, ki smo ga kupili, ne izvira iz EU, kot je dajala vtis spletna stran. Ker gre za nakup zunaj EU, moramo plačati še uvozne dajatve.

PRAVILA VARNEGA SPLETNEGA NAKUPOVANJA

Ključna načela varnega spletnega nakupa lahko strnemo: preverimo ceno, možnosti plačila, podjetje, domeno in izkušnje drugih kupcev.

1. Prvi znak, ki kaže na tvegan spletni nakup, je naravnost neverjetna cena. Če ponudba po predstavitvi, ceni ali drugih lastnostih močno odstopa od konkurence, je to upravičen razlog za previdnost.

2. Če spletni trgovec zahteva nakazilo prek sistema **Western Union** ali **MoneyGram**, je to velik znak stop! Ta plačilna mehanizma sta namenjena hitremu prenosu denarja fizičnim osebam, sledenje nakazilu pa ni mogoče. Ko nakupujete po spletu, če le imate možnost, izberite plačilo prek zaupanja vrednih posrednikov (na primer PayPala). Če opravljate rezervacijo ali plačilo s kreditno kartico, vedno poiščite znamenja varne povezave:

   URL-naslov spletnega mesta se začne s **HTTPS,** kar pomeni, da je prenos podatkov varen in šifriran.

   
   V URL-naslovni vrstici je tudi ikona s **ključavnico**, kar je znak za varno oddajanje podatkov o kreditni kartici.

3. Natančno preverite, katero podjetje stoji za spletno trgovino. Preverite kontaktne podatke (naslov podjetja, telefonska številka za pomoč uporabnikom, elektronski naslov). Navežite stik s prodajalcem in izmenjajte nekaj sporočil. Ali se njegov elektronski naslov ujema z naslovom spletne trgovine? Če prodajalec uporablja brezplačni poštni predal (gmail.com, hotmail.com itd.), je to še en znak, da gre morda za prevaro.

4. Na strani http://whois.domaintools.com/ poiščite več informacij o domeni, kje in kdaj je bila registrirana in kateri kontaktni podatki so navedeni.

5. Poiščite ocene drugih kupcev, preverite njihove izkušnje, kritike in mnenja. V iskalnik vnesite spletni naslov trgovine in preverite, ali se po forumih oglašajo kupci, ki so imeli s trgovino slabe izkušnje. Tu velja pravilo: dobre novice se hitro širijo, slabe še hitreje.

Programska oprema

Vaša skrb je, da imate vedno posodobljeno vso programsko opremo v računalniku, zato nikoli ne zanemarite obvestil o posodobitvah, ki se vam pojavijo na zaslonu. Priporočamo, da za vsakdanjo uporabo računalnika ne uporabljate dostopa z administratorskimi pravicami, temveč si ustvarite uporabniški račun z omejenimi pravicami. Tako morebitni okužbi preprečite, da bi se naselila pregloboko v sistem.

Osnovno zaščito vašega računalnika sestavljajo tri komponente, ki preprosto morajo biti nameščene, še preden se povežete v internet:

1. Aktiviran požarni zid. Požarni zid (angl. firewall) prepreči dostop do storitev vašega računalnika, ki niso namenjene javni uporabi. Operacijski sistemi Windows takšno pregrado že vsebujejo, zato je ne izklapljajte, tudi če vam zaradi njega kakšen program ne dela, kot bi si želeli.

2. Nameščen in posodobljen protivirusni program. Zavedati se morate, da noben protivirusni program ne zagotavlja stoodstotne zaščite. Pisci virusov uporabljajo razne trike, da preslepijo protivirusne programe. Če imate nameščen protivirusni program, to še ne pomeni, da lahko klikate vsepovsod in odpirate nepreverjene programe. Bodite pozorni na redno in uspešno posodabljanje protivirusnih definicij.

3. Nenehno morate skrbeti za posodabljanje operacijskega sistema, brskalnika in vseh nameščenih programov, saj s popravki odpravljate tudi varnostne luknje in tako zmanjšujete možnost zlorabe svojega računalnika.

Zaklepanje delovne postaje in gesla

Vedno, ko zapustite delovno mesto (vstanete od mize), morate delovno postajo zakleniti tako, da zaklenete namizje.

To storite s kombinacijo tipk Ctrl + Alt + Delete in možnostjo »Lock this computer« ali s kombinacijo tipk Win + L.

Ctrl + Alt + Del ALI Win + L

Ko delovno mesto zapustite za več ur ali odhajate domov, delovno postajo izključite. Z rednim izklapljanjem delovne postaje omogočite, da se vam ob ponovnem zagonu namestijo popravki.

Pri izbiri gesla tako za delovno postajo kot vse druge storitve morate upoštevati navodila o zapletenosti, dolžini in pogostosti menjave:

1.

Nikoli ne uporabljajte istega gesla za različne storitve. Če vam napadalec ukrade geslo za eno storitev, tako ne bo mogel zlorabiti tudi drugih.

2.

Vaše geslo naj bo dolgo vsaj 8 znakov in naj vsebuje male in velike črke, številke in ločila.

Če geslo po dolžini ni omejeno, si namesto ene besede izberite daljšo frazo; uporabite lahko tudi daljši stavek, ki si ga boste zlahka zapomnili. Nikoli ne uporabljajte zaporednih črk ali številk, prav tako ne sosednjih tipk na tipkovnici (npr. 12345678 ali asdfghj).

3.

Ne uporabljajte gesel, ki jih je lahko uganiti (npr. ime in priimek, imena otrok, datum rojstva, znamka avtomobila, ki ga vozite, in kombinacije teh podatkov).

4.

Gesel ne zapisujte na vidna ali splošno dostopna mesta. Zapisanega gesla ne shranjujte v bližini svojega računalnika (listek z geslom, nalepljen na računalniški zaslon ali pisalno mizo).

5.

Če si gesla za delovno postajo ne boste zapomnili, potem ga zapišite, vstavite v kuverto, zapečatite in shranite v ognjevarno omaro, po možnosti pri nadrejenem ali v tajništvu organizacijske enote.

6.

Svojega gesla ne zaupajte nikomur, prav tako nihče ne bo od vas zahteval, da mu izdate svoje geslo! Geslo je le vaše in ga je prepovedano komurkoli razkriti. Vašega gesla od vas ne bo zahteval niti sistemski administrator.

Vedno, ko tiskate dokumente, stopite do tiskalnika takoj po tem, ko kliknete gumb za tiskanje. Tako preprečite, da dokumente po pomoti vzame kdo drug ali da nanje pozabite in obležijo na tiskalniku. Samo tako lahko zagotovite, da ne pridejo v roke komu, ki ni pristojen za vpogled v nekatere dokumente.

Elektronska pošta in odpiranje priponk

Elektronska pošta je eden najbolj množičnih načinov za širjenje škodljive kode. Zato nikoli ne odpirajte sumljivih priponk ali pošte neznanih pošiljateljev. Vklopite si prikazovanje končnice v imenu priponk, saj napadalci pogosto uporabljajo dvojno končnico, da bi tako zavedli žrtev, npr. fotografija.jpg.exe.

Če ste bili tarča izsiljevalskega kriptovirusa in ne želite oziroma ne zmorete plačati izsiljevalcem, pospravite okuženi disk in na spletni strani **https://www.nomoreransom.org/** občasno preverite, ali obstaja kakšna rešitev. Po nasvet pa se je priporočljivo obrniti na nacionalni center SI-CERT ali ga vsaj obvestiti.

ELEKTRONSKI PREDAL ODPIRA VRATA ŠTEVILNIM ZLORABAM

Geslo za elektronski predal odpira vrata v vse storitve, ki jih imate vezane na ta predal – družabna omrežja, spletne trgovine, PayPal ipd. Napadalci do gesel po navadi pridejo s tako imenovanim ribarjenjem (angl. phishing), kjer vam pošljejo elektronsko sporočilo, ki se na prvi pogled zdi, kot da vam ga je poslal vaš ponudnik. Pod kako pretvezo, na primer da ste prekoračili podatkovno kvoto, od vas zahtevajo, da kliknete povezavo v sporočilu. Ta vodi na spletno stran, ki je videti kot vstopna stran vašega ponudnika za elektronsko pošto, v resnici pa gre za lažno stran pod nadzorom napadalca. Če na tej strani vpišete svoje geslo, ga pravzaprav sporočite napadalcem.

Pri uporabi elektronske pošte je pomembno vedeti:

1.

Nikoli ne odpirajte priponk neznanih pošiljateljev.

2.

Če vam je pošiljatelj sporočila znan, preverite ime pripete datoteke. Če je ime priponke sumljivo, na primer 226KL2100.docx, po telefonu ali e-pošti pošiljatelja vprašajte, ali vam je priponko res poslal on.

3.

Če prejmete elektronsko pošto, v kateri vas »nujno« pozivajo k vpisu svojega uporabniškega imena in gesla (za elektronsko pošto ali kako drugo storitev), tega nikoli ne storite.

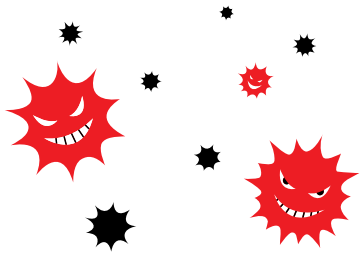
4.

Če prejmete datoteko s končnico **.doc** ali **.xls** in ob odprtju datoteke program od vas zahteva vklop makra, tega ne storite. Izjema so interne datoteke med sodelavci, vendar tudi takrat preverite, ali vam jo je res poslal sodelavec, preden vklopite makre.

5.

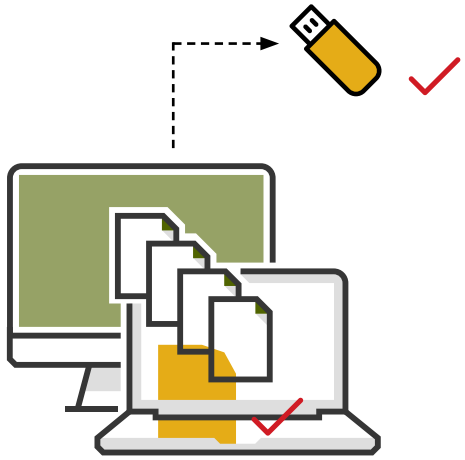
Če vaš ponudnik elektronske pošte to omogoča, si nastavite dvofaktorsko avtentikacijo, pri kateri morate, ko se prijavljate z novo napravo, prijavo potrditi na svojem pametnem telefonu ali vpisati dodatno geslo. Dodatno geslo lahko prejmete s SMS-sporočilom ali pa ga generirate s posebno aplikacijo na pametnem telefonu. Taka zaščita napadalcu prepreči vdor, tudi če mu uspe ukrasti vaše geslo.

Po vrnitvi s potovanja v tujino smo še posebno dovzetni za elektronska sporočila s priponkami, ki so videti kot račun, na primer Invoice. pdf ali podobno. V strahu, da katerega računa, storitve ali kazni nismo plačali, hitro in nepremišljeno kliknemo priponko, v kateri se lahko skriva škodljiva koda, ki zašifrira vse dokumente v računalniku.



REŠI VAS LAHKO LE VARNOSTNA KOPIJA!

Dosedanje izkušnje kažejo, da so imele v primeru okužbe z izsiljevalskim kriptovirusom žrtve le malo možnosti za ukrepanje. Če niso imele ustreznih varnostnih kopij pomembnih dokumentov, je bilo plačilo kriminalcem žal edina možnost. Virus pride v računalnik v obliki močno zamaskirane kode, kar lahko prelisiči marsikateri protivirusni program. Hkrati pa virusu uporabniki sami dovolimo zagon, ko v e-pošti odpremo zlonamerno priponko.



Najučinkovitejša zaščita so še vedno pravilno izdelane varnostne kopije dokumentov (angl. backup). Pri ustvarjanju varnostnih kopij veljata dve pravili: kopije vedno shranjujte na dve ločeni mesti in ustvarjajte jih redno. Kopijo podatkov najprej shranite v zunanji pomnilnik, na primer na zunanji disk ali USB-ključ, ki ju po končanem kopiranju varno spravite stran od računalnika. Če recimo disk ostane priklopljen, virus zašifrira tudi podatke na njem, in s takšno varnostno kopijo si ne boste mogli pomagati. Drugo kopijo podatkov shranite v oblak: datoteke v oblaku virus sicer ravno tako zašifrira, toda večina ponudnikov oblačnih storitev ponuja možnost obnovitve prvotnih datotek. Na voljo je tudi več specializiranih programov za izdelavo varnostnih kopij.

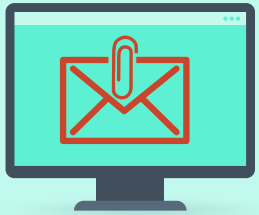
SLOVENSKI VOJAKI IN VOJAKINJE PONOSNI IN VARNI TUDI NA SPLETU
Avtor publikacije: Nacionalni center za odzivanje na omrežne incidente SI-CERT in Slovenska vojska Odsek za kibernetsko varnost
Leto izida: 2017
Natis: 5.000 izvodov
Založnik: Javni zavod Arnes
Oblikovanje in prelom: PM, d.o.o.

KAKO

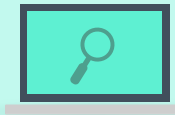
SE LAHKO OKUŽITE Z IZSILJEVALSKIM VIRUSOM?

Izsiljevalski virusi so trenutno najbolj razširjena grožnja za spletne uporabnike, po drugi strani pa največji vir zaslužka za spletne kriminalce. Preverite, kako lahko postanete žrtev izsiljevalskih virusov in kako učinkovito zaščitite svoje dokumente.

1. Škodljiva koda se širi v glavnemna dva načina:



1. **V priponkah elektronske pošte.**



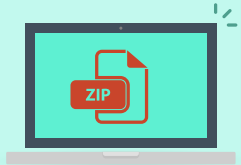
2. **Prek okužb v mimohodu** (»okužili« se boste, če po spletu brskate z zastarelo različico brskalnika, nevarne so čisto običajne spletne strani. Npr. spletna trgovina, kjer nakupuje vaša sodelavka, ali spletna stran vrtca, ki ga obiskujejo vaši otroci).

NAMIG

- Upoštevajte enostaven recept: ne klikajte priponk v elektronski pošti, za katere vam ni čisto jasno, zakaj ste jih dobili. Poskrbite, da imate vedno posodobljene različice vseh programov, brskalnika in operacijskega sistema.

2. Kako nas prepričajo, da prenesemo priponko z virusom?

Spletni kriminalci navadno (uspešno) računajo na našo radovednost, zato razpošiljajo elektronsko pošto s priponkami, ki vzbudijo našo pozornost. Tako se virusi lahko skrivajo v opozorilih o neplačanih računih, obvestilih logistične službe o prispeli pošiljki, tudi v novoletnih e-voščilnicah.



1. Spletni kriminalci ponaredijo naslovnika, da je videti, kot da vam je sporočilo poslal **znanec** ali da ste si sporočilo poslali **sami**.

3. Virus pošljejo v obliki zamaskirane izvršilne datoteke s končnico **.exe, .vbs ali .js.**
4. Po novem se boste lahko okužili tudi z navadno **datoteko zbirke MS Office (Excel, Word ipd.)**

NAMIG

- Ne odpirajte priponk ZIP in ne vklopite Officeovih makrov. Trik je prav v makrih: če jih boste ob odprtju datoteke omogočili ali pa imate že predhodno nastavljene tako, da se ob odprtju zaženejo, bodo v vaš računalnik naložili virus.

3. Prihranite tisoč evrov

- Okoli **1000 evrov** (v zadnjem času pa tudi več) boste morali plačati izsiljevalcem, da bi prejeli šifrirni ključ, s katerim boste lahko datoteko odklenili.
- **BITCOIN** je virtualna valuta, v kateri izsiljevalci zahtevajo odkupnino.

NAMIG

- Vedno in povsod imejte v mislih dve preprosti, a zlati pravili:
  1. Če ne veste, zakaj ste dobili pošto, nikoli ne odpirajte priponk niti ne klikajte na povezave.
  2. Ne čakajte in ustvarite varnostno kopijo dokumentov še danes.

www.varninainternetu.si

Več nasvetov o varni rabi interneta in prepoznavanju spletnih prevar poiščite na portalu **www.varninainternetu.si**

si·cert
Nacionalni center za posredovanje pri omrežnih incidentih

Odsek za kibernetsko varnost

VARNI NA INTERNETU
Od mene je odvisno vse.
www.varninainternetu.si