Policistke in policisti, bodite

VARNI NA INTERNETU

tako doma kot v službi

si·cert

Varni na internetu, doma in v službi

Spletno okolje je že dolgo prostor povezovanja. Vanj je danes vpeta sleherna organizacija, prav tako posameznik. Omogoča nam lažje poslovanje, komuniciranje in hiter dostop do različnih vsebin, zato se mnoge storitve organizacij in podjetij pa tudi zasebno življenje posameznika selijo v virtualni prostor.

Tako kot si prizadevamo za zaščito svojega doma z nakupom protivlomnih vrat in alarmnih naprav ter doslednim zaklepanjem ključavnic, moramo podobno poskrbeti za varnost svojega »imetja« v virtualnem okolju. Ustrezno varovana infrastruktura, predvsem pa ozaveščena, odgovorna in varna raba spleta vsakega posameznika sta temelja za dobro informacijsko varnost. Kibernetski kriminal je v porastu, napadalci po vsem svetu pa nenehno iščejo nove načine za vdor v informacijske sisteme.

Zato si želimo, da bi knjižica, ki je nastala v sodelovanju z nacionalnim odzivnim centrom SI-CERT, dosegla svoj namen, koristni nasveti v njej pa zaživeli v praksi. Naj varujejo vaše informacije tako dobro, kot tudi vi varujete ljudi!

Policija

si·cert
Nacionalni center za posredovanje pri omrežnih incidentih

KO SMO DOMA

Naprava je pametna toliko kot njen uporabnik

Pametna naprava (pametni telefon, tablica, pametna ura in podobno) je postala 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.

KAKO UKREPATE,

ČE IZGUBITE ALI VAM UKRADEJO PAMETNI TELEFON?

1.

Če uporabljate napravo Android, je prvi, nujen korak obisk strani **https://myaccount.google.com/find-your-phone.** Vpišite se **v svoj račun Google in izberite 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 v telefonu (dostop do imenika, aplikacij itd.)

3.

Če 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.

NAMIG:
Če izgubite ali vam ukradejo iPhone, najdete vsa navodila, kako ukrepati, na tej povezavi:
www.vni.si/iphone.

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.

KAKO SE VARNO POVEŽETE 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.

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.

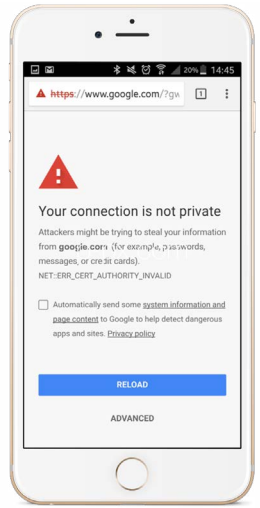
4.

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.



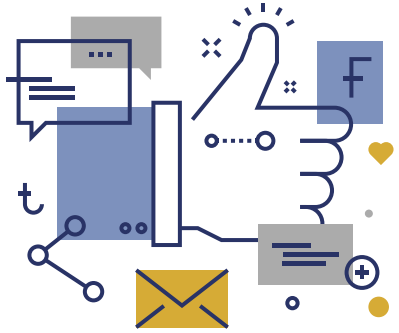
6.

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.

Pasti družabnih omrežij



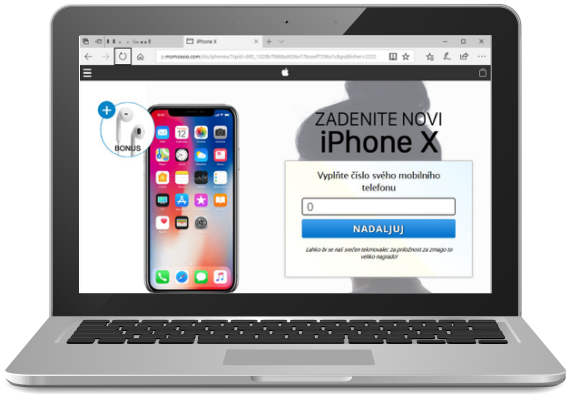
NAJPOGOSTEJŠE PREVARE NA FACEBOOKU

Podjetja na svojih straneh na Facebooku redno objavljajo razne nagradne igre, izzive, natečaje, nekatera se bolj držijo strogih Facebookovih pravil, druga manj. Žal so na Facebooku zelo pogoste tudi povsem lažne nagradne igre, ki zgolj zavajajo uporabnike in se hitro širijo po naših časovnicah. Gre za nagradne igre tipa »všečkaj-deli-komentiraj«, ki nimajo navedenih nobenih informacij o organizatorju ali podjetju, temveč samo obljubljajo drage nagrade znanih blagovnih znamk. Vsi poznamo tiste, ki obljubljajo vinjete, že nekaj let pa se pojavljajo nagradne igre, ki »podarijo« iPhone vsakič, ko se na trgu pojavi nov model. Namen takšnih akcij je le v zelo kratkem času pridobiti veliko novih oboževalcev, obljubljene nagrade pa nikoli ne podelijo.

Recept, kako prepoznate lažne obljube, je zelo preprost. Pomislite, preden kliknete, preden se spustite v lov za nagrado.

Vprašajte se, zakaj bi vam nekdo dal nagrado, vredno skoraj tisoč evrov, v zameno za en sam klik?

Ne gre samo za velike obljube; če niste pozorni, si lahko na glavo nakopljete še **včlanitev v SMS-klub, ki vas lahko stane 20 evrov na mesec.** Velikokrat se v takšnih nagradnih igrah pojavljajo tudi povezave, ki vodijo na strani, kjer se zahteva vpis telefonske številke. Gre za vabe za SMS-klub, kar je razvidno iz drobnega tiska, ki pa ga nepozorni uporabniki pogosto ne preberejo.



3 KLJUČNI NASVETI,
ČE SODELUJETE V NAGRADNIH IGRAH

1. Vedno preverite, kdo je organizator nagradne igre, torej katero podjetje. Pravilo upoštevajte pri vseh nagradnih igrah, ne le tistih na Facebooku.

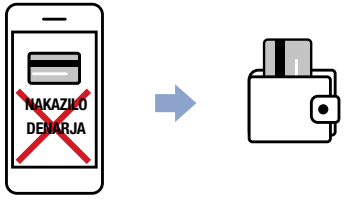
2. Vedno preberite pravila oziroma pogoje nagradne igre: kako poteka žreb, kdo plača davek, če gre za vrednost, višjo od 42 evrov, kam se lahko pritožite itd.

3. Bodite pozorni, kateri osebni podatki bodo zbrani (elektronski naslov, telefonska številka, davčna številka), kdo jih bo shranjeval oziroma obdeloval in za kakšen namen, ali bodo še komu posredovani.

SEXTORTION – IZSILJEVANJE Z INTIMNIMI POSNETKI

Predstavljajte si, da vas na Facebooku kot prijatelja 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. Po izkušnjah SI-CERT so žrtve izsiljevanja plačila nakazovala prek sistema Western Union, denar pa je romal na Slonokoščeno obalo.



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

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.

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

7 SUMLJIVIH ZNAKOV V SPLETNI TRGOVINI

1. Neverjetno nizke cene. Če ponudba po predstavitvi, ceni ali drugih lastnostih močno odstopa od drugih, je to zanesljiv razlog za previdnost. Če ste našli torbico Gucci za 20 evrov ali uro Suunto za 70 evrov, boste gotovo dobili ponaredek ali pa ostali praznih rok.

2. Velike obljube. Čisto vsi artikli so na zalogi, dobavljivi takoj, trgovec pa obljublja še brezplačno dostavo po celem svetu. Če nakupujete pri uveljavljenem spletnem trgovcu, to niti ne bi bilo sumljivo. Če pa ste prišli v popolnoma neznano spletno trgovino, kjer je vse kar za 80 odstotkov znižano, podatki o domeni pa kažejo, da gre za stran, ki je nastala pred tednom dni, potem se raje ne odločite za nakup.

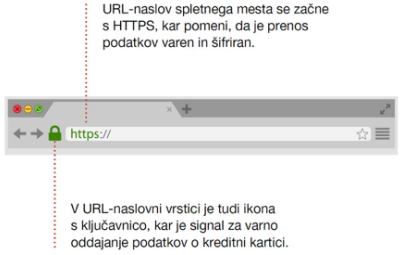
3. Ni podatkov o trgovcu. Kdo sploh stoji za spletno trgovino? Katero podjetje je to, kje je njihov sedež? Morebitne spore je veliko lažje reševati, če gre za podjetje v EU. Če ni nobenih podatkov o podjetju, je to znak za previdnost.

4. Ni kontaktnih podatkov. Preverite, kako lahko kontaktirate trgovca, ali je navedena telefonska številka za pomoč uporabnikom, elektronski naslov. Je na voljo samo obrazec za sporočilo? Če ni naveden niti en sam podatek za stik, je to še en znak za previdnost.

5. Elektronski naslov pripada brezplačnemu ponudniku. Spletni goljufi za komunikacijo uporabijo brezplačni poštni predal (gmail.com, hotmail.com itd.), kar je morda še en znak, da gre za prevaro.

6. Pred kratkim ustvarjena domena. Na strani **http://whois.domaintools.com/** preverite, kje in kdaj je bila domena registrirana in kateri kontaktni podatki so navedeni. Včasih lahko že na podlagi teh podatkov sklepamo, da nekaj ni v redu – spletna trgovina se na primer hvali z dolgo tradicijo, domena pa je bila registrirana pred kakšnim mesecem ali pa je bil pri registraciji domene uporabljen brezplačen elektronski naslov.

7. Vpis kreditne kartice ni varen. Če boste plačali s kreditno kartico, vedno preverite, ali v naslovni vrstici piše HTTPS, kar dokazuje, da gre za varno povezavo. To pomeni, da je prenos podatkov o kreditni kartici šifriran ter tako skrit pred očmi morebitnih vsiljivcev v omrežju.



Ko vpisujete podatke o kreditni kartici, vedno preverite, ali se povezava začne s HTTPS.

Elektronska pošta in odpiranje priponk

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.

Redno izdelujte varnostne kopije

Varnostne kopije vam bodo prišle prav, če izgubite pametni telefon, pomotoma izbrišete nujno datoteko ali pa se pokvari trdi disk računalnika. Nezadržno širjenje izsiljevalskih kriptovirusov je še en argument, zakaj je pametno poskrbeti za kopije pomembnih dokumentov (angl. backup).

Izsiljevalski virusi, ki zaklenejo vse dokumente v računalniku in nato zahtevajo plačilo odkupnine, so v zadnjih letih postali zelo resna težava na področju računalniške varnosti, lahko bi rekli, da gre za epidemijo. **Žrtev izsiljevalskih virusov lahko postane vsak spletni uporabnik in vsako podjetje.** 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.

> Pravi pomen varnostnih kopij spoznamo šele takrat, ko izgubimo vse dokumente!

Ne ustrašite se zapletenih izrazov; gre za zelo preprosto kopiranje (copy/paste) dokumentov. Vse, kar potrebujete, je dovolj velik USB-ključ, ki se zelo verjetno valja nekje v predalu, ali pa kupite cenovno že zelo ugoden zunanji disk. Sproti, ko ustvarite pomembne dokumente (to so verjetno fotografije, videoposnetki, Wordove in Excelove datoteke, certifikati ipd.), jih preprosto prekopirate še na drug pomnilnik.

UPOŠTEVAJTE DVE PRAVILI
PRI IZDELAVI VARNOSTNIH KOPIJ

1. Kopijo podatkov shranite na dve ločeni lokaciji: eno na disk in drugo v oblak. Zunanji disk ali USB-ključ, kamor shranite podatke, po kopiranju varno spravite nekje zunaj računalnika.

2. Ni dovolj, da za kopije poskrbite le enkrat na leto. Poskušajte jih izdelovati sproti, ko ustvarjate nove vsebine (dokumenti, fotografije).

Načela varne rabe bančnih kartic

1. Preden uporabite bankomat, preverite režo za vstavljanje bančne kartice – ali je razrahljana, ali manjkajo vijaki ipd. Kriminalci lahko namestijo lažne čitalce kartic (t. i. skimming) in tako pridobijo zapis vaše kartice. Te podatke lahko pozneje uporabljajo kot klonirane kartice za odpiranje vrat, plačevanje na bankomatu ali plačevanje v trgovinah na POS-terminalih.

2. Pred vnosom kode PIN z roko zakrijte tipkovnico.

3. Pri izdaji denarja bodite pozorni na t. i. money trapping, ko nepridipravi blokirajo režo za izdajo denarja, vi opravite transakcijo, denar pa poberejo, ko zapustite bankomat. Vsako nepravilnost ali zlorabo, ki jo opazite, nemudoma sporočite banki ali hranilnici na telefonsko številko, ki je zapisana na kartici in policiji na številko 113.

4. Pri svoji banki se pozanimajte, ali ponuja dodatne varovalne mehanizme, na primer obveščanje o transakcijah s SMS-sporočili.

KO SMO V SLUŽBI

Zaklepanje delovne postaje

Svojega gesla za delovno postajo ne zaupajte nikomur, prav tako ne bi smel nihče zahtevati, da mu izdate svoje geslo! Geslo je le vaše in ga je prepovedano komurkoli razkriti. Vašega gesla ne sme od vas zahtevati niti sistemski administrator.

1.

Vedno ko zapustite delovno mesto (vstanete od mize), morate delovno postajo zapustiti z zaklenjenim namizjem.

Ctrl + Alt + Del

2.

Gesla naj imajo najmanj 9 znakov, uporabite pa kombinacijo črk, številk in drugih znakov, na primer 3tNpelai@7.

3.

Izberite geslo, ki ga je težko uganiti. Ne uporabljajte svojega imena, priimka, naslova, datuma rojstva, zaporedja črk ali številk.

4.

Gesla ne zapišite na papir, ki ga hranite na mizi, steni ali monitorju svojega računalnika.

5.

Ne uporabljajte istega gesla za službene uporabniške račune in zasebne, na primer Gmail, Facebook.

Uporaba službenega GSM-aparata ali prenosnega računalnika

Prenosne naprave (prenosni računalnik, tablični računalnik, GSM-aparat) uporabljamo zunaj varnega službenega omrežja, zato moramo biti še posebej previdni.

1.

Zaklepajte zaslon naprave vsaj z vzorcem, še bolje pa s številko PIN ali geslom.

2.

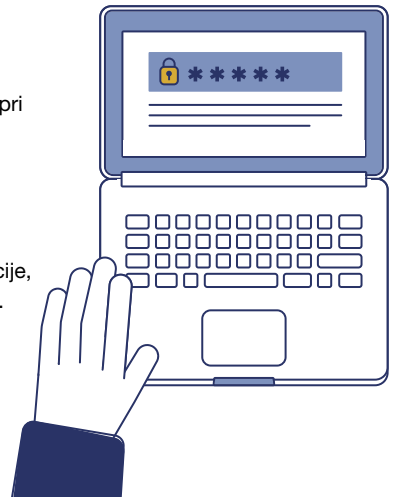
Nastavite šifriranje vsebine naprave in kartice SD. S tem preprečite dostop do vsebine pri fizičnem vdoru v napravo.

3.

Nameščajte samo tiste aplikacije, ki vam jih dovoli administrator.

4.

Vsak sum zlorabe vaše mobilne naprave, izgubo ali krajo morate prijaviti odgovorni osebi kot varnostni incident.



Uporaba USB-ključev na službenih računalnikih

Lastnih USB-ključev ne uporabljajte na službenih računalnikih, saj lahko nevede okužite delovno postajo ali pa celotno lokalno računalniško mrežo in s tem vse računalnike, ki so priklopljeni na omrežje. Še večje tveganje predstavljajo najdeni USB-ključi, za katere ne veste, kdo in za kakšne namene jih je uporabljal.

Če službene podatke prenašate po zunanjih medijih (npr. USB-ključi, prenosni diski), je treba podatke v teh napravah nujno šifrirati, recimo z orodji Bitlocker, Veracrypt ipd. S šifriranjem podatkov zagotovimo njihovo zaupnost, saj jih ob izgubi ali odtujitvi medija nihče ne bo mogel prebrati.

Podatkovnih nosilcev ne uničujte sami, temveč jih predajte strokovnim službam, ki bodo poskrbele za trajen in nepovraten izbris podatkov.

POLICISTKE IN POLICISTI, BODITE VARNI NA INTERNETU TAKO DOMA KOT V SLUŽBI

Avtor publikacije:
Nacionalni center za odzivanje na omrežne incidente SI-CERT in Policija
Leto izida: 2017
Natis: 5.000 izvodov
Založnik: Javni zavod Arnes
Oblikovanje in prelom: PM, poslovni mediji, d. o. o.

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

Policija

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