Predlogi in nasveti

Tu je nekaj predlogov in nasvetov, ki vam lahko pomagajo pridobiti dobre navade za varnost na spletu. Ta razdelek je bil pripravljen v sodelovanju z organizacijo Get Safe Online iz Združenega kraljestva in ministrstvom Združenih držav za domovinsko varnost

- Varovanje osebnega računalnika in prenosnih naprav
- Varovanje osebnih podatkov in identitete
- Varovanje poslovnih informacij zunaj vaše organizacije
- Premišljeno povezovanje
- Spletna ozaveščenost

Varovanje osebnega računalnika in prenosnih naprav

Osebni računalniki:

- uporabite požarni zid: požarni zid varuje vaše omrežje pred nekaterimi virusi in hekerji;
- namestite protivirusno programsko opremo: protivirusni programi preprečujejo, da bi se virus razširil na vaš računalnik;
- namestite najnovejše varnostne posodobitve: vaša programska oprema in operacijski sistem naj ostaneta delujoča, zdrava in posodobljena;
- zaustavite vohunsko programsko opremo: ne dovolite, da bi neznanci prišli do vašega računalnika, tako da se izogibate sumljivi e-pošti in prilogam;
- redno ustvarjajte varnostne kopije: zaščitite svoje podatke pred najhujšim.

Prenosni računalniki:

- izključite brezžično povezavo, kadar je ne uporabljate ali ni potrebna;
- prenosni računalnik redno povezujte z zaupanja vrednim omrežjem, da posodobite varnostne mehanizme;
- ustvarite varnostno kopijo podatkov, shranjenih v vašem prenosniku;
- ne puščajte svojega prenosnika brez nadzora.

USB-ključi:

- uporabljajte samo šifrirane USB-ključe;
- USB-ključ z vgrajenim stikalom preklopite v način, ki omogoča samo branje, da bi se izognili prenašanju virusov: nekateri USB-ključi imajo stikalo, s katerim jih lahko preklopite v način, ki omogoča samo branje, tako da računalnik, na katerem ga uporabljate, ne more pisati podatkov nanj ali jih spreminjati;

- po kopiranju datotek z računalnika, ki ni vreden zaupanja ali ki ni pooblaščen, preglejte USB-ključ s protivirusnim programom, da bi se izognili prenašanju virusov;
- pred vstavljanjem vašega USB-ključa v računalnik druge osebe zbrišite vse datoteke, ki niso potrebne pri načrtovanem opravilu;
- redno ustvarjajte varnostne kopije podatkov z vašega USB-ključa, da jih zaščitite pred najhujšim;
- USB-ključe pripnite na obeske za ključe ali ovratni trak, da jih ne izgubite: ker so USB-ključi vedno manjši, se lahko hitro izgubijo ali vam jih lažje ukradejo. Poleg tega imajo čedalje več prostora za shranjevanje, kar poveča morebitno količino podatkov, do katerih lahko kdo nepooblaščeno dostopa. USB-ključi se pogosto prenašajo v torbicah, nahrbtnikih, torbah za prenosne računalnike, jaknah in žepih ali pa se puščajo brez nadzora v računalniku. Število neljubih dogodkov se je v zadnjem času povečalo, ker se USB-ključi izgubijo, založijo, sposojajo brez dovoljenja ali so ukradeni.

Mobilni telefoni in dlančniki

Dlančniki, kot so na primer Windows Mobile, Palm, iPhone, ter naprave Android in Blackberry imajo internetno povezavo in zmogljivosti, da shranjujejo ogromne količine podatkov. Že zaradi njihove prenosljivosti je treba z njimi ravnati zelo previdno:

- izključite brezžično povezavo (npr. Bluetooth in brezžično lokalno omrežje), kadar je ne uporabljate. Tehnologija Bluetooth elektronskim napravam omogoča medsebojno komunikacijo z radijsko povezavo s kratkim dosegom;
- ne puščajte mobilnega telefona in dlančnika brez nadzora. V nasprotnem primeru lahko pride do izgube podatkov;
- uporabite funkcijo za gesla, da preprečite oddaljene vdore v vaš pametni telefon.

Varovanje osebnih podatkov in identitete

- **uporabite zapleteno geslo**: vaše geslo je ključavnica in ključ vhodnih vrat vaše „hiše“ na spletu. Gesla so pomembna obramba in dobre navade pri njihovi uporabi vam bodo pomagale osebne podatke in identiteto ohraniti bolj varne. Geslo za prijavo v vaš računalnik je ključ za dostop do vseh informacij, poslovnih in osebnih, ki jih imate shranjene v svojem računalniku in na spletnih računih. Za varovanje podatkov uporabite zapleteno geslo – tj. zapleten nabor znakov ter združite velike in male črke, številke in simbole. Bolj raznoliki kot so znaki, ki jih uporabite v geslu, težje ga je uganiti. Ne uporabljajte osebnih podatkov, kot so ime, ime vašega otroka, rojstni datumi ipd., ki jih lahko nekdo že pozna ali enostavno poišče, prav tako se izogibajte običajnim besedam: nekateri hekerji uporabljajo programe, ki preskusijo vsako besedo iz slovarja;
- **geslo spreminjajte redno**: če menite, da je bil vaš sistem ogrožen , takoj spremenite geslo;
- **vaše geslo naj ostane skrivno**: vaše geslo je edinstveno in ga ne smete povedati nikomur. Kadar koli je to mogoče, si ga poskusite zapomniti. Imejte strategijo, s katero si ga boste

lažje zapomnili. Če si gesla zapisujete, pazite, kje jih hranite. Zapisov ne puščajte nikjer, kjer ne bi bili pripravljeni pustiti podatkov, ki jih ta gesla varujejo;

- **en račun, eno geslo**: uporabljajte različna gesla za vsak spletni račun, do katerega dostopate (ali pa uporabljajte vsaj nekaj različnih gesel). Če uporabljate isto geslo za več računov, bo napadalec, ki dobi dostop do enega računa, lahko dostopal do vseh vaših računov;
- **zavarujte svoje račune**: številni ponudniki računov ponujajo dodatne načine za preverjanje istovetnosti pred opravljanjem poslovanja na zadevnem spletnem mestu;
- **nadzirajte svojo prisotnost na spletu**: če je mogoče, prilagodite nastavitve zasebnosti in varnosti na spletnih mestih na raven skupne rabe informacij, ki se vam zdi primerna. Zaželeno je, da nastavite omejitve glede na to, s kom si izmenjujete informacije;
- **družabna spletna omrežja uporabljajte previdno**: zavedajte se, da lahko družabna omrežja na spletu združujejo številna tveganja, povezana s prisotnostjo na spletu: ustrahovanje, razkritje zasebnih podatkov, spletno zalezovanje, dostop do vsebin, ki niso primerne za mladoletne ter, kar je najhuje, zapeljevanje prek spleta in zloraba otrok.

Varovanje poslovnih informacij zunaj vaše organizacije

- **pazite, da občutljivi podatki ostanejo varni**: kadar ste zunaj vaše organizacije, je treba zagotoviti, da so občutljive informacije in oprema vedno varne pred krajo ali izgubo. Z informacijami ravnajte previdno zlasti na javnih mestih;
- **poslovne informacije naj ostanejo zaupne**: zavedajte se, da lahko nekdo prisluškuje vašim pogovorom. Naj zaupne informacije vaše organizacije ne bodo na voljo vsem;
- **pazite, kdo vam gleda čez ramo**: kadar potujete ali delate z oddaljenega mesta, se zavarujte pred ljudmi, ki bi vam lahko gledali čez ramo;
- **spletno pošto uporabljajte pametno:** pri uporabi spletnega brskalnika za branje pošte morate biti enako previdni kot pri branju pošte na namiznem računalniku, poleg tega pa tak način prebiranja pošte pomeni nekaj dodatnih tveganj.

Premišljeno povezovanje

- **izključite brezžično povezavo, kadar je ne uporabljate ali ni potrebna;**
- **pamet v roke pri uporabi dostopnih točk Wi-Fi**: ko uporabljate dostopne točke Wi-Fi, omejite vrsto poslovanja in prilagodite varnostne nastavitve na vaši napravi, da omejite dostop do nje;
- **zavarujte svoj denar**: pri spletnem bančništvu ali nakupovanju preverite, ali je spletno mesto varno. Iščite naslove, ki vsebujejo „https://“ ali „shttp://“, kar pomeni, da spletno mesto uporablja dodatne ukrepe, ki pomagajo zavarovati vaše podatke; Spletna mesta http:// niso varna;
- **zaustavite neželeno pošto**: neželena pošta pomeni tveganje za varnost. Ne odpirajte neznanih e-poštnih sporočil in prilog;

- **ko ste v dvomih, izbrišite**: če se vam povezave v e-sporočilih, objavah v storitvi Twitter, drugih objavah in spletnih oglasih zdijo sumljive, tudi če poznate vir, jih je najbolje izbrisati ali, če je to ustrezno, označiti kot neželeno pošto;
- **posredujte e-sporočilo, če je to primerno**: razmislite o brisanju zgodovine sporočil, preden to storite;
- **po spletu brskajte previdno;**
- **ne nalagajte dokumentov in gradiva iz virov, ki niso vredni zaupanja;**
- **javne računalnike uporabljajte previdno:** na javnem računalniku se povežite samo, kadar imate šifrirano povezavo (kar označuje simbol ključavnice na spodnji desni strani okna vašega brskalnika in črke „https://“ na začetku naslova spletnega mesta);
- **uporabljajte samo storitve spletne pošte dobro poznanih in zaupanja vrednih podjetij.**

Spletna ozaveščenost

- **ostanite na tekočem:** sledite novim načinom za varnost na spletu – na zaupanja vrednih spletnih mestih poiščite najnovejše informacije ter jih delite z družino, prijatelji in sodelavci, te pa spodbujajte k spletni ozaveščenosti. Zagotovite varnost vašega brskalnika;
- **premislite preden ukrepate**: bodite previdni pri sporočilih, ki vas pozivajo k takojšnjemu ukrepanju, ponujajo nekaj, kar se sliši predobro, ali zahtevajo osebne podatke;
- **ustvarite varnostne kopije**: zaščitite svoje delo, glasbo, fotografije in druge digitalne podatke tako, da ustvarite elektronsko kopijo in jo varno shranite.