12 NASVETOV ZA KIBERNETSKO VARNOST PRI DELU

V knjižici 12 nasvetov za kibernetsko varnost pri delu najdete nekaj preprostih napotkov, kako lahko sami poskrbite za lastno zaščito in zaščito organizacije, kadar delo opravljate na računalniku ali preko spleta.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

c n v o s
center za informiranje, sodelovanje in razvoj nevladnih organizacij

1

ZAŠČITITE SVOJE PODATKE

V vsakdanjem življenju se izogibamo deljenju osebnih podatkov, kot je številka socialnega zavarovanja ali številka kreditne kartice. Pri delu naj velja enako. S podatki organizacije (društva, zavoda ali ustanove), občutljivimi informacijami in intelektualno lastnino morate ravnati tako previdno kot s svojimi osebnimi podatki.

2

NE ODPIRAJTE POVEZAV IN E-POŠTNIH SPOROČIL NEZNANIH POŠILJATELJEV

Hekerji lovijo osebe v upanju, da bodo odprli pojavna okna ali druge zlonamerne povezave, v katere so vgrajeni virusi ali druga zlonamerna programska oprema. Zato morate biti previdni pri povezavah in prilogah v e-poštnih sporočilih pošiljateljev, ki jih ne poznate. Z enim samim klikom lahko hekerjem omogočite vdor v računalniško omrežje.

Na spletu lahko pogosto zasledite pojavna okna z mamljivimi besedili, kot npr. ˝Čestitamo, zadeli ste nov avto˝ ali ˝En klik vas loči od novega iPhona˝. Teh povezav in pojavnih oken se morate izogibati. Znak za alarm so tudi oglasi, polni slovničnih napak, in oglasi, v katerih zahtevajo vaše osebne podatke.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

cnvos
center za informiranje, sodelovanje in razvoj nevladnih organizacij

3

OBLIKUJTE MOČNA GESLA IN UPORABLJAJTE UPRAVITELJA GESEL

Da bi kibernetskim tatovom preprečili dostop do omrežja in zaupnih podatkov organizacije, morate ustvariti edinstvena in zapletena gesla. Za geslo nikoli ne izberite svojega imena, imena partnerja, otrok ali hišnih ljubljenčkov, datumov obletnic ali podatkov, ki jih lahko hekerji hitro ugotovijo. Če si za geslo izberete ime svojega hišnega ljubljenčka, ki ste ga z imenom objavili na družbenih omrežjih, boste hitro postali žrtev kibernetskega kriminala.

Močno geslo vsebuje najmanj 10 znakov in vključuje številke, simbole ter velike in male črke. Pri ustvarjanju gesla si lahko pomagate s stavkom: izberite prvo črko vsake besede in vsako drugo črko zapišite z veliko začetnico, na začetek in konec pa vstavite naključne številke in simbole. Če je izbrani stavek npr. ˝Čez poletje gremo z letalom na počitnice v Dominikansko Republiko¨, se bo geslo glasilo npr. 6@čPgZlNpVdR3!

Za vsako aplikacijo, ki jo uporabljate, morate ustvariti drugačno geslo. Težava seveda nastopi, ko si je treba vsa ta gesla tudi zapomniti. Pri tem vam lahko pomagajo posebne računalniške aplikacije, t. i. upravitelji gesel, kot npr. Bitwarden, LastPass in KeePass, kjer lahko varno shranite vsa svoj gesla.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

cnvos
center za informiranje, sodelovanje in razvoj nevladnih organizacij

4

POVEŽITE SE Z VARNIM OMREŽJEM WI-FI

Pisarniška brezžična omrežja morajo biti varna, šifrirana in skrita. Če delate na daljavo, ne pozabite zaščititi in zavarovati tudi svojega domačega omrežja. Za zaščito brezžičnega omrežja pa ni dovolj le močno geslo.
Varnost lahko povečate z upoštevanjem spodnjih nasvetov.

- Vklopite šifriranje brezžičnega omrežja. Šifriranje je eden najučinkovitejših načinov varovanja vaših podatkov. Deluje tako, da vaše podatke in vsebino premeša, tako da ga hekerji ne morejo razvozlati. Najvarnejša vrsta šifriranja za domače omrežje Wi-Fi je WPA2. Če želite preveriti, ali vaš usmerjevalnik uporablja ustrezno šifriranje, preverite nastavitve omrežja in lastnosti brezžične povezave.
- Uporabite VPN, ki šifrira vaše podatke, tako da heker ne more ugotoviti, kaj počnete na spletu in kje se nahajate.
- Skrijte svoje omrežje. Na ta način se ime vašega omrežja ne bo pojavilo na seznamu ljudi v okolici.
- Spremenite ime omrežja. Večina naprav je konfiguriranih s privzetim omrežnim imenom, ki ga dodeli proizvajalec. S spremembo imena hekerjem boste pred hekerji skrili informacijo o usmerjevalniku in tako zmanjšali možnost napada.
- Posodabljajte programsko opremo usmerjevalnika. Vdelana programska oprema usmerjevalnika, tako kot katera koli druga programska oprema, lahko vsebuje ranljivosti, zaradi katerih lahko lažje pride do napadov. Večina usmerjevalnikov nima možnosti samodejne posodobitve, zato jo morate posodobiti ročno.
- Onemogočite oddaljeno upravljanje. Oddaljeno upravljanje omogoča vsakomur, ki je dovolj blizu omrežja, da si ogleda ali spremeni nastavitve Wi-Fi. Če nimate potrebe po oddaljenem povezovanju z usmerjevalnikom Wi-Fi, je najbolje, da to funkcijo izklopite.

Pomembno je tudi, kako izberete ime omrežja. Ime omrežja naj ne razkriva vaše lokacije in dejavnosti vaše organizacije.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

cnvos
center za informiranje, sodelovanje in razvoj nevladnih organizacij

ZAGOTOVITE SI POŽARNI ZID

Požarni zid za omrežje organizacije in domače omrežje je prva obrambna linija pri zaščiti podatkov pred kibernetskimi napadi. Požarni zidovi nepooblaščenim uporabnikom preprečujejo dostop do vaših podatkov in informacij in blokirajo nezaželen promet. Ne zanašajte se samo na požarni zid svoje organizacije, temveč namestite požarni zid tudi v domačem omrežju, če delate od doma.

Preden se odločite požarni zid, se pozanimajte, kakšno zaščito potrebujete. Izbira požarnega zidu je odvisna od velikosti in obsega vaše organizacije.
V Sloveniji obstajajo tri splošne kategorije požarnih zidov:

- Filtriranje paketov. Požarni zidovi za filtriranje paketov preverjajo vhodne in odhodne pakete podatkov po vnaprej programiranih merilih, da ugotovijo, ali so varni ali ne.
- Požarni zidovi s statusom in strežnikom proxy. Opravljajo tako funkcije filtriranja paketov kot funkcije požarnega zidu na ravni vezja. Požarni zidovi na ravni vezja ugotavljajo, ali so naprave, ki želijo med seboj komunicirati, zaupanja vredne. Vendar so takšni požarni zidovi v Sloveniji prepovedani. Čeprav so požarni zidovi s statusom in strežnikom proxy najbolj celovita zaščita za organizacije, ti požarni zidovi zmanjšujejo zmogljivost omrežja, kar lahko povzroči neprijetne časovne zamike za vašo ekipo.
- Požarni zidovi naslednje generacije. Vzdržujejo najširšo paleto pregledov prometa in zmanjšanja groženj. Ponujajo dodatne funkcije, kot je skeniranje protivirusnih programov, zlonamerne programske opreme in e-pošte, ter napredne zmogljivosti spremljanja, na primer pregled paketov, ki vam omogoča neprestano spreminjanje vseh sej brskanja po internetu, ki se pojavljajo v vašem omrežju.

Kadar se odločate o nakupu požarnega zidu, preverite, ali ponudnik omogoča vrhunske obrambne funkcije, kot so filtriranje paketov, funkcionalnost usmerjevalnika, lokalni overitelj (on-premises authenticator), skeniranje zlonamerne programske opreme, portal za oddaljeni dostop in filtriranje spletnih mest.

6

NA JAVNIH OMREŽJIH UPORABLJAJTE VPN

VPN je navidezno zasebno omrežje oziroma preprosta programska oprema, namenjena za zaščito vaše zasebnosti na spletu. VPN je bistvenega pomena pri opravljanju dela izven pisarne ali na službenem potovanju. Če ima vaša organizacija VPN, ki mu zaupa, se povežite z njim in ga tudi uporabljate. VPN pomaga ohraniti zasebnost vaših podatkov na javnih omrežjih Wi-Fi ali drugih neznanih omrežjih. Kadar ste povezani s strežnikom VPN, je vaš internetni promet šifriran, kar pomeni, da nihče ne more spremljati, kar počete na spletu, ali vam slediti. V letu 2021 sta med najboljšimi ponudniki npr. CyberGhost in NordVPN.

7

NAMESTITE POSODOBITVE VARNOSTNE OPREME

Upoštevanje najboljših praks varnosti pomeni, da sta vaša varnostna programska oprema in operacijski sistem posodobljena z najnovejšo zaščito. Če vaša organizacija pošlje navodila za varnostne posodobitve, jih takoj namestite. To velja tudi za osebne naprave, ki jih uporabljate pri delu. Takojšna namestitev posodobitev pomaga pri obrambi pred najnovejšimi kibernetskimi grožnjami.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

cnvos
center za informiranje, sodelovanje in razvoj nevladnih organizacij

8

NIKOLI NE PUŠČAJTE NAPRAV BREZ NADZORA

Ne pozabite zakleniti svojih naprav, kadar jih pustite brez nadzora. Prav tako se prepričajte, da se naprave samodejno zaklenejo v stanju mirovanja. Pazite tudi, da ne izgubite USB ključkov in drugih diskov, na katerih shranjujete podatke in občutljive informacije.

9

NAMESTITE ZAŠČITO PRED VIRUSI

Zaščita pred virusi je bistvena za vsako organizacijo, ki želi zaščititi svoje podatke in računalniške sisteme. Protivirusna programska oprema je kot varnostnik, ki preprečuje vstop nezaželenim osebam. Ne glede na delo, ki ga opravljate, se prepričajte, da ste zaščiteni pred virusi. Pred virusi se zaščitite tako, da imate na računalniku nameščen posodobljen in aktiven protivirusni program. Pred virusi boste zaščiteni tudi z upoštevanjem zgoraj naštetih nasvetov.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

cnvos
center za informiranje, sodelovanje in razvoj nevladnih organizacij

10

VARNOSTNO KOPIRAJTE DATOTEKE

Ustvarjanje varnostnih kopij je kritičen korak pri vzdrževanju računalnika za zaščito vaših podatkov in podatkov organizacije v primeru okvare sistema ali okvare datotek. Datoteke morate varnostno kopirati, kadarkoli spremenite ali dodate nove datoteke. Varnostno kopiranje datotek naj postane vsakodnevna navada.

11

IZKLJUČITE GLASOVNO VODENE PAMETNE NAPRAVE NA DOMAČI DELOVNI POSTAJI IN POKRIJTE SPLETNO KAMERO, KO JE NE UPORABLJATE

Če na računalnik ponesreči namestite zlonamerno programsko opremo, lahko kibernetski kriminalci pridobijo nadzor nad vašo opremo, tudi nad spletno kamero in mikrofonom. Zato je pomembno, da nikoli ne odpirate sumljivih povezav od ljudi, ki jih ne poznate.

12

NE NASEDAJTE DIREKTORSKIM PREVARAM

Direktorska prevara je prevara, pri kateri se kriminalci lažno predstavljajo za vodjo organizacije, da bi delavca zavedli k nepooblaščenemu prenosu sredstev ali posredovanju zaupnih podatkov. Pred direktorskimi prevarami se lahko zaščitite tako, da strogo sledite veljavnim varnostnim postopkom za plačila in javna naročila, da pri obravnavi občutljivih informacij vedno skrbno preverite e-poštne naslove in se v primeru dvoma posvetujete s pristojnim sodelavcem, da omejite informacije, ki jih delite z drugimi, in ste previdni pri deljenju informacij na družbenih omrežjih. Če prejmete sumljivo e-pošto ali klic, o tem obvestite ustrezno osebo.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

cnvos
center za informiranje, sodelovanje in razvoj nevladnih organizacij