POMEMBNO OBVESTILO!

V času, ko večina zaposlenih dela od doma, vas želimo še enkrat posebej **opozoriti na previdnost pri uporabi elektronske pošte in brskanju po spletu.**

V odzivnem centru za incidente informacijske varnosti v državni upravi (SIGOV-CERT) zaznavamo povečano aktivnost zlonamernih posameznikov in skupin, ki trenutno stanje izkoriščajo v svojo korist, tako da pošiljajo zlonamerno elektronsko pošto, podtikajo zlonamerno programsko kodo na spletne strani, postavljajo nove zlonamerne spletne strani, vse to z namenom okužiti uporabnikov računalnik.

Posebej previdni bodite pri uporabi spletnih strani, ki prikazujejo stanje širjenja okužbe s COVID-19 po svetu, in pri odpiranju spletnih povezav oziroma priponk elektronske pošte. Na spletnih straneh in v elektronski pošti uporabnike prepričujejo, da gre za različne nasvete glede zaščite, preprečevanja širjenja okužbe, zdravila, ki naj bi pri okužbi pomagala in podobno.

Prosimo vas, da redno posodabljate protivirusno zaščito na vaših računalnikih in s tem pripomorete k boljši zaščiti in varovanju vaših podatkov.

Za informacije o trenutnem stanju širjenja COVID-19 in nasvete priporočamo uporabo spletnih mest pristojnih organov (NIJZ, Ministrstvo za zdravje …).

Prosimo za skrajno previdnost pri prejemanju in odpiranju elektronske pošte, še posebej pri klikanju na priponke in spletne povezave, in tudi na splošno pri uporabi interneta. Pri tem se ravnajte po temeljnih načelih informacijske varnosti za uporabnike:

- **Ne odpirajte elektronske pošte s sumljivimi naslovi in vsebino (tudi s strani vam poznanih oseb) ter nanjo ne odgovarjajte, oziroma predhodno preverite avtentičnost pri pošiljatelju. Nevarne so predvsem priponke in spletne povezave (tako v sporočilih kot v brskalnikih); ko jih odprete, se lahko zažene škodljiva koda.**
- **Ne aktivirajte makrojev (»Enable macro?«) v Office (Word, Excel) dokumentih, če niste prepričani o izvoru dokumenta in potrebnosti aktiviranja makrojev.**
- **Ne nasedajte lažnim obvestilom, ki naj bi jih poslale znane korporacije (npr. lažno obvestilo Microsofta o brezplačni (»free«) nadgradnji sistema Windows).**
- **V kolikor je v poštnem sporočilu ali telefonskem klicu (npr. lažni klici računalniške podpore IT korporacij, kot je Microsoft, IBM ipd., kot tudi domnevno vaše lokalne računalniške podpore) zahteva za izvedbo kakršnihkoli aktivnosti na vašem računalniku ali zahteva za vnos osebnih podatkov, uporabniških imen, gesel, PIN kod, številk kartic, tega ne počnite, če pošiljatelja oz. klicatelja ne poznate oz. ga ni možno preveriti.**
- **V kolikor niste prepričani o identiteti pošiljatelja elektronskega sporočila, preverite podrobnosti o pošiljatelju (naslov v polju »od« ali »from« oziroma podatke v ozadju sporočila).**
- **Bodite previdni tudi pri rabi svetovnega spleta, pri klikanju na nepoznane spletne strani ter pri vnašanju osebnih in drugih podatkov na spletne strani, ker so lahko ponarejene.**
- **Ob vsakršnem dvomu se obrnite na vašo podporo za IT.**

Če ste na računalnik dobili virusno okužbo, ga čim prej izklopite iz omrežja (odklopite mrežni kabel) ter pokličite pomoč skrbnika informacijskega sistema.

Prilagamo še nekaj spletnih povezav, kjer najdete koristne informacije in nasvete s področja varnosti na internetu:

https://www.cert.si/si-cert-2020-02

https://www.varninainternetu.si/

https://safe.si/

http://www.policija.si/index.php/preventiva-/preventiva/5788-varni-na-internetu

Glej tudi:

https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html

Ministrstvo za javno upravo

Direktorat za informacijsko družbo in informatiko

Sektor za informacijsko varnost