VARNOSTNI KONTROLNI SEZNAM ZA DELO NA DALJAVO

Delo na daljavo prinaša veliko koristi, vključno s prihrankom časa, ki bi ga običajno porabili za prevoz na delo, manj motnjami pri delu, manjša je tudi verjetnost okužbe. Če torej delate na daljavo, pa naj bo to od doma ali s katere koli druge lokacije, ste edina oseba, odgovorna za zagotavljanje lastne varnosti ter varnosti vaših naprav in vseh informacij, s katerimi razpolagate.

Oglejte si spodnji kontrolni seznam in preverite, ali ste pripravljeni na delo na daljavo.

	Vprašanje	Stanje
1	Je vaš lokalni požarni zid omogočen?	☐
2	Je vaš protivirusni program aktiven in posodobljen?	☐
3	So aktivirana vsa orodja, povezana z varnostjo (npr. Windows Defender)?	☐
4	Ste posodobili svoj operacijski sistem?	☐
5	Ste posodobili vse programe, s katerimi delate (npr. brskalnik Chrome, bralnik Adobe itd.)?	☐
6	Poznate vse politike podjetja (BYOD – »Prinesi svojo napravo«, delo na daljavo, uporaba interneta itd.)?	☐
7	Ste ustvarili ločen uporabniški račun za opravila, povezana z delom?	☐
8	Ste poskrbeli, da vaš račun za delo nima skrbniških pravic?	☐
9	Ali uporabljate programsko opremo za šifriranje, da zaščitite mape z občutljivimi podatki podjetja?	☐
10	Ste preverili, ali se vaš računalnik samodejno zaklene po petih minutah?	☐
11	Ste spremenili geslo in nastavili novo, močno geslo?	☐
12	Ali gesla shranjujete na varno mesto (npr. uporabljate sistem upravljanja z gesli)?	☐
13	Ste zavarovali svojo mobilno napravo (omogočili možnosti »oddaljeno-brisanje« in »najdi-mojo-napravo«, izbrisali aplikacije, ki jih ne uporabljate itd.)?	☐
14	Ste poskrbeli, da vaš usmerjevalnik Wi-Fi uporablja močno šifriranje in je dostop omogočen samo ljudem, ki jim zaupate?	☐
15	Ali vaš usmerjevalnik Wi-Fi za skrbniški vmesnik uporablja varno geslo po meri?	☐
16	Ali imate napravo za varnostno kopiranje ali storitev v oblaku, kamor lahko varno shranjujete podatke?	☐

	Vprašanje	Stanje
17	Ste poskrbeli, da je e-poštna komunikacija šifrirana (z uporabo certifikata S/mime ali varne komunikacije SMTP itd.)?	☐
18	Ste zagotovili, da vašega računalnika ne uporablja nihče drug (vključno z družinskimi člani)?	☐
19	Ali lahko na usmerjevalniku ustvarite ločeno omrežje WLAN, ki ločuje službeni in zasebni promet?	☐
20	Če ne morete delati prek varne (šifrirane) povezave – ali imate nameščeno programsko opremo VPN?	☐

30 SMART COM

Že več kot 30 let delujemo na področju IKT in smo eden izmed vodilnih sistemskih integratorjev v Jugovzhodni Evropi.
Z ekipo več kot 70 strokovnjakov in specialistov vzpostavljamo sodobna in zanesljiva komunikacijska omrežja in varnostne rešitve za zaščito pred naprednimi kibernetskimi grožnjami. Z vpeljavo tehnoloških rešitev, ki temeljijo na strojnem učenju in umetni inteligenci ter avtomatizacijo in orkestracijo skrbimo za zaščito IK infrastrukture.

Smart Com d.o.o., Brnčičeva 45, 1231 Črnuče - Ljubljana

www.smart-com.si