# ZAKAJ MORAMO POSKRBETI ZA VARNOST, KO DELAMO OD DOMA

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.

Ne moremo se zanašati na visoko raven varnosti, ki jo imamo, ko delamo v pisarni, zato se je na delo na daljavo potrebno dobro pripraviti. Če tega ne storimo, tvegamo, da postanemo lahka tarča napadalcev, ki bodo zlahka ukradli osebne podatke ali podatke podjetja, ki so slabo ali pa sploh niso zaščiteni. Z dobro pripravo pa lahko bistveno zmanjšamo varnostna tveganja, zaradi česar bo naša izkušnja dela na daljavo bolj prijetna in produktivna.

## *S katerimi varnostnimi tveganji se soočamo pri delu na daljavo*

Številni dejavniki lahko ogrozijo našo varnost, ko delamo od doma, in varnost poslovnih podatkov, ki jih vsakodnevno uporabljamo. Tveganja smo razvrstili v **štiri glavne kategorije** – fizična kraja ali izguba, pomanjkanje osebne ozaveščenosti, nezavarovana javna povezava in neomejen dostop do podjetja.

### *FIZIČNA KRAJA ALI IZGUBA*

Delo v pisarniškem okolju ima številne prednosti, vključno z dobro dodelanimi varnostnimi sistemi in za to usposobljenim osebjem, mehanizmi za varovanje digitalnih podatkov, uveljavljenimi varnostnimi praksami in zaposlenimi varnostniki.

Ko se naše delovno mesto preseli na drugo lokacijo, npr. v domačo pisarno, kavarno ali kateri koli drug javni prostor, varnostnih ukrepov, na katere bi se lahko oprli, ni več. Tako naše delovne naprave postanejo lahka tarča za številne osebe, od 'klasičnega' tatu, ki bo ob prvi priložnosti prodal naš računalnik, do hekerja, ki bo z veseljem zaobšel oslabljeni požarni zid in ukradel poslovne podatke.

### *POMANJKANJE OSEBNE OZAVEŠČENOSTI*

V veliko primerih delo na daljavo zmanjša število motenj, zaposleni pa lahko opravimo zahtevnejše delo, ko smo izven pisarniškega okolja. Toda, če ni v naši navadi, da mislimo tudi na varnostni vidik, morda niti ne opazimo, da nas opazujejo/spremljajo, nam sledijo, nas napadajo z lažnim predstavljanjem ali kako drugače.

Poleg tega se pri delu na daljavo mnogi zaposleni navadijo dostopati do podatkov podjetja prek nezavarovanih osebnih ali javnih naprav ali, kar je še huje, tako, da tretjim osebam omogočajo brskanje po spletu z naprave podjetja. Na žalost lahko takšne prakse zlahka ogrozijo varnost in podatke katere koli organizacije.

## NEOMEJEN DOSTOP DO PODJETJA

Mnoga podjetja svojim zaposlenim, ki delajo na daljavo, podelijo enake pravice in dostop, kot bi jih imeli v varnem pisarniškem okolju. To vključuje popoln dostop do omrežij podjetja, dostop do oblaka, notranjih sistemov itd. Če pri tem zaposleni ni skrben in nima potrebnega znanja ali zavezanosti k varnosti, lahko podeljene pravice napadalcu omogočijo popoln dostop do podatkov podjetja.

## NEZAVAROVANE JAVNE POVEZAVE

Kolikokrat ste med potovanjem uporabljali javno omrežje Wi-Fi, na primer na letališču ali v hotelski sobi? Večina teh omrežij nima vzpostavljenega nikakršnega varnostnega sistema, kar pomeni, da uporaba takšnega omrežja za poslovne namene našo napravo in podatke izpostavi morebitnemu vdoru.

Grožnja je realna, saj večina javnih omrežij ni šifriranih in za vzpostavitev povezave ne zahtevajo avtentikacije. Takšno omrežje, tudi če je vzpostavljeno doma, lahko hekerjem zlahka omogoči dostop do vseh informacij, ki jih pošiljamo prek interneta – vse od zaupnih e-poštnih sporočil do varnostnih poverilnic vašega podjetja in celo do podatkov o kreditnih karticah.

## Kaj lahko naredimo, da zaščitimo sebe in svoje podjetje, ko delamo od doma

Na srečo lahko vsakdo zaščiti svojo 'oddaljeno pisarno'. Potrebna je le pazljivost, vzpostavljanje nekaterih novih navad in poznavanje potrebnih varnostnih postopkov.

### 1 Dobra priprava

Ko moramo delati zunaj pisarne, ne glede na to, ali potujemo ali preprosto delamo od doma, se najprej prepričajmo, da smo dobro pripravljeni za učinkovito izvrševanje svojih nalog. IT podporo mora zagotoviti ustrezen in varen dostop do datotek in sistemov podjetja, ki jih bomo potrebovali za učinkovito delo.

Preden odidemo, pospravimo računalnik, napajalnik in vse dokumente, ki jih bomo potrebovali pri svojem delu – vendar ne pretiravajmo. Zaupne podatke o strankah, občutljive poslovne načrte, zaščitene informacije in lastniške podatke je najbolje pustiti v pisarni, če niso nujno potrebni. S tem previdnostnim ukrepom bomo zmanjšali število stvari, ki jih moramo zaščititi, in tveganja za svoje podjetje v primeru morebitne kraje ali izgube svoje naprave.

### 2 Posodabljajmo in varujmo naprave

Če želimo zaščititi svoje naprave, moramo poskrbeti, da je posodobljena vsa nameščena programska oprema, vključno z operacijskim sistemom. Upoštevajmo, da noben operacijski sistem ni povsem varen. Varnostne ranljivosti se razkrivajo nenehno in lahko vplivajo na katero koli različico nameščene programske opreme. Vendar je tveganje veliko večje, če je operacijski sistem starejši in nima nameščenih najnovejših popravkov. Zato je torej pametno, da se prepričamo, da osebne in poslovne naprave, ki jih uporabljamo, vedno delujejo v podprti in po možnosti najnovejši različici operacijskega sistema.

Za odpravo večine varnostnih ranljivosti sta potrebna več kot dva meseca. Predstavljamo si lahko, kaj se zgodi s sistemom, če je v tem obdobju izpostavljen grožnjam. Če želimo odpraviti nadaljnje zamude pri posodabljanju naprav z najnovejšimi varnostnimi popravki, je najbolje, da vklopimo možnost samodejnih posodobitev in tako sistemu omogočimo prenos in namestitev posodobitev takoj, ko so na voljo.

Ko je sistem z izvajanjem rednih posodobitev zaščiten, je čas, da pozornost usmerimo na vse ostale programe znotraj sistema. To vključuje vsa pisarniška ali kreativna orodja, brskalnik in vso drugo programsko opremo, ki lahko predstavlja potencialno ranljivost. Na srečo sodobna programska oprema samodejno preverja posodobitve, zato je potrebno poskrbeti, da se prenesene posodobitve pravočasno namestijo.

## 3 Zaščitimo računalnik

Ko delamo izven pisarne, moramo zagotoviti, da je računalnik podjetja varen, saj lahko tako računalnik kot tudi na njem shranjene informacije tatu ali konkurentu predstavljajo dragoceno korist. V nadaljevanju podajamo seznam previdnostnih ukrepov, ki jih lahko izvedemo za zaščito svoje naprave in vseh podatkov, shranjenih na njej:

### 3.1. Omogočimo samodejno zaklepanje

Kadar koli se moramo ločiti od svoje naprave, bodisi v domači pisarni ali v skupnem delovnem prostoru, je ne pozabimo zakleniti. Tudi če to pozabimo storiti ročno, nastavimo samodejno zaklepanje svoje naprave: po 30-ih sekundah nedejavnosti za telefon ali tablični računalnik ter po 5-ih minutah za prenosnik.

### 3.2. Izklopimo samodejno prijavljanje

Dostopa do naše naprave ne sme imeti nihče razen nas. Prepričajmo se, da je za prijavo potrebna avtentikacija v obliki gesla, kode PIN ali biometrične alternativne možnosti. Samodejne prijave predstavljajo resnično grožnjo varnosti podjetja, zato se prepričajmo, da je ta možnost **vedno onemogočena**.

### 3.3. Uporabimo močna gesla

Ne moremo dovolj poudariti, kako pomembna je uporaba močnih gesel/kod PIN pri vseh napravah. Šibka gesla vključujejo enake ali zaporedne črke/številke, zlahka ugotovljene najpogostejše besede in osebne podatke, ki so na voljo na družbenih omrežjih (na primer rojstni kraj, datum rojstva, registrska tablica itd.).

**Močno geslo** se mora drugim zdeti naključno in mora vsebovati vsaj 8 znakov, med katerimi so tako male kot velike tiskane črke, številke in simboli.

### 3.4. Investirajmo v sistem upravljanja z gesli (mnogi so brezplačni)

Ko pričnemo uporabljati močna, edinstvena gesla za vse svoje naprave in uporabniške račune, jih je težko ročno upravljati. Včasih lahko gesla pozabimo, zagotovo pa jih ne želimo hraniti zapisane na listu papirja. V takšnih primerih so sistemi upravljanja z gesli resnično priročni, saj lahko shranijo neomejeno število informacij, jih šifrirajo in shranijo v eno samo geslo, ki ga lahko enostavno spremljamo. Odločite se lahko za **1Password, LastPass** in številne druge.

### 3.5. Uporabimo dvofaktorsko avtentikacijo (2FA)

V mnogih primerih je zgolj uporaba gesla za zaščito naših računov postala nezadostna, zlasti ko gre za sisteme podjetij, spletno bančništvo, e-poštna sporočila ali sistem za upravljanje z gesli. Vsa ta mesta hranijo pomembne podatke visoke vrednosti, ki jih je treba varovati ves čas.

Zato je bila pred nekaj leti uvedena dvofaktorska avtentikacija (2FA). Preprosto povedano, to pomeni, da za preverjanje identitete ne potrebujemo le gesla, ampak tudi dodatno metodo preverjanja pristnosti. Lahko gre za **enkratno kodo**, ki je poslana prek SMS-sporočila ali **prek aplikacije**. Omogočena 2FA na vseh napravah in računih zagotovo pomeni, da lažje dihamo.

### 3.6. Omogočimo možnosti "najdi mojo napravo" in "oddaljeno brisanje"

V primeru izgube ali kraje je možnost, da na daljavo najdemo in izbrišemo podatke s svoje naprave, ne le koristen, ampak tudi **izjemno pomemben varnostni ukrep**. Takšen ukrep, zlasti glede brisanja, lahko zavaruje naše osebne in poslovne podatke ter prepreči, da bi prišli v roke napadalcev.

### 3.7. Tovarniška nastavitev

Brisanje je treba izvesti tudi takrat, ko napravo prenehamo uporabljati. Napravo ponastavimo na tovarniške nastavitve, preden jo prodamo, podarimo ali kako drugače predamo naprej. Ne pozabimo, da z brisanjem izbrišemo vse podatke, shranjene na napravi. Če te podatke potrebujemo za nadaljnjo uporabo, najprej naredimo varnostno kopijo!

## 4 Upoštevajmo svoje fizično okolje

Naše fizično okolje je zelo pomembno, neupoštevanje tega vidika lahko ogrozi našo varnost, kot tudi varnost naprave in poslovnih podatkov. To še posebej velja, če delamo na daljavo, tudi če delamo od doma. Da zagotovimo varno delovno okolje, vrata vedno zapiramo in zaklepamo.

Pozorni moramo biti na dejavnosti, ki se dogajajo okoli nas; **naprav/USB ključev na javnih mestih nikoli ne puščamo brez nadzora**. V času, ko gremo na stranišče, lahko napravo ukradejo ali nanjo namestijo zlonamerno programsko opremo. Izguba naprave in na njej shranjenih informacij ne povzroči samo stresa in motenje v našem delovnem procesu, temveč povzroči tudi globe, ki prizadenejo nas in naše podjetje.

## 5 Bodimo pozorni na svojo okolico

Ko delamo na javnem mesta, bodimo pozorni na dogajanje v svoji okolici v našem vidnem polju. Če je mogoče, smo s hrbtom obrnjeni proti steni tako, da nihče ne more gledati v naš zaslon izza našega hrbta **(znana hekerska tehnika – gledanje čez ramo ali angl. shoulder surfing)**. Druga možnost je namestitev Privacy Filter aplikacije, ki drugim preprečuje, da bi pod kotom kukali v naš zaslon in tako prišli do informacij, ki jim niso namenjene.

## 6 Zaščitimo zaupne informacije

Ko delamo izven pisarne, je še posebej pomembno, da zaščitimo vse zaupne ali osebne podatke, ki jih uporabljamo, prenašamo in hranimo. Na javnem kraju bi lahko številni ljudje imeli slabe namene, kar vključuje tudi tatove in konkurente – v primeru izgube ali kraje naprave oz. podatkov pa lahko podjetje odgovarja za razkritje zaupnih podatkov.

Upoštevajmo, da javni računalniki niso varni in jih nikoli ne bi smeli uporabljati, če razpolagamo z osebnimi ali zaupnimi podatki. Nikoli ne vemo, ali je bila zlonamerna programska oprema morda predhodno nameščena na javni napravi, zato se izogibajmo vnosu poverilnic, podatkov o bančnih računih, številk socialnega zavarovanja ali drugih zaupnih podatkov. Če moramo uporabljati javni računalnik, se najprej prepričajmo, da uporabljamo 'zasebno brskanje'. Ne označimo nobenega polja z navedkom 'shrani' ali 'zapomni si'. Preden zapremo brskalnik, počistimo zgodovino brskanja in izbrišemo vse prenose.

Ne glede na to, ali potujete s službenim računalnikom ali prek njega delo opravljate od doma, še vedno obstaja nevarnost, da drugi pridobijo dostop do njega. Naprave podjetja uporabljajte samo v službene namene in ne dovolite, da bi jih uporabljal kdo drug, npr. prijatelji ali družinski člani. Tudi pri nenamernem ogrožanju podatkov podjetja še vedno odgovarjate za njegovo varnost.

## 7 Službeni podatki naj ostanejo na službenih računalnikih

Velika verjetno je, da naše osebne naprave niso posodobljene in pregledane ter da ne izvajajo natančno nastavljenih protivirusnih pregledov programov, požarnega zidu, šifriranja, omrežja in drugih storitev, ki delujejo v ozadju vaše delovne naprave. Če sami nismo IT-strokovnjak (in tudi to ni 100-odstotno zagotovilo), verjetno nismo seznanjeni z vsemi previdnostnimi varnostnimi ukrepi, ki jih na ravni podjetja izvajajo učinkovite IT-ekipe.

Morda nas bo zamikalo služben računalnik uporabljati za osebne zadeve, kot je spletno nakupovanje, bančništvo ali celo preverjanje e-pošte. Ali obratno, osebne naprave za službene namene. Vendar pa lahko že povezava ene same nezadostno varne naprave, kot je računalnik, v omrežje podjetja, ogrozi varnost celotnega omrežja, zaradi česar smo odgovorni za nastalo škodo v povezavi z zaupnimi podatki, shranjenimi na strežnikih podjetja.

Obstaja pa način za odpravo tveganja, če moramo delati na svojem osebnem računalniku – in to je, da **uporabljamo okolja v oblaku, kot je Office 365**. Na ta način praktično delamo preko spleta, ne da bi prenašali ali sinhronizirali datoteke in/ali e-poštna sporočila na svojo osebno napravo.

## 8 Izogibamo se javni povezavi Wi-Fi

Ko delamo z javnega mesta, nas pogosto zamika, da uporabimo **razpoložljivo brezplačno javno povezavo Wi-Fi**. Toda varnostno tveganje, ki ga lahko povzroči 'enostaven' dostop, bo verjetno povzročilo veliko težav tako nam kot našemu podjetju.

Dve glavni težavi, ki ju predstavlja uporaba javne povezave Wi-Fi, sta:
1) nezaščiteno omrežje, ki si ga hkrati deli več naprav, in
2) nezaščiten podatkovni promet, ki poteka med javno povezavo Wi-Fi, ki jo uporabljamo, in omrežjem na našem delovnem mestu.

Če želimo rešiti prvo težavo, lahko na svojem telefonu ali drugi mobilni napravi nastavimo svoje **lastno brezžično omrežje Wi-Fi**, imenovano **dostopna točka (angl. hotspot)**. Čeprav dostopna točka ne šifrira našega prometa, pa prav tako drugim ne omogoča, da bi na istem omrežju zajemali naše podatke. Seveda mobilni operater zaračuna dodaten strošek za vzpostavitev našega zasebnega omrežja Wi-Fi, vendar bo ta strošek v primerjavi z morebitno škodo, ki jo lahko povzročijo javna brezžična omrežja, zanemarljiv.

Za rešitev druge težave priporočamo vzpostavitev **navideznega zasebnega omrežja (VPN-Virtual Private Network)**, ki zagotavlja varen in šifriran kanal za naš promet, ki potuje po internetu. Omrežja VPN kibernetskim napadalcem izjemno otežijo prestrezanje naših podatkov, skrijejo našo pravo lokacijo in nam omogočijo spletno zasebnost, ki jo potrebujemo.

## 9 Šifrirajmo občutljive podatke v e-pošti in na svoji napravi

Nobeni podatki, poslani prek e-pošte, niso varni, razen če jih predhodno šifriramo. Šifriranje je postopek, ki informacije kodira tako, da jih nepooblaščene osebe težko razvozlajo. Če moramo občutljive podatke poslati prek e-pošte, je nujno, da jih najprej šifriramo.

Kot previdnostni ukrep moramo vedno šifrirati vse svoje shranjene podatke, tako da v primeru izgube ali kraje naše naprave nihče ne more pridobiti dostopa do shranjenih podatkov, ne da bi poznal geslo ali kodo PIN.

## 10 Pazimo na USB ključe

Presenečeni bi bili nad številom ljudi, ki najdejo na videz zapuščen USB ključ in ga vtaknejo v svoj računalnik. Čeprav gre za klasično hekersko tehniko, **imenovano USB dropping oz. podtikanje USB ključev**, ji še vedno nasede veliko ljudi. Ko zlonameren USB ključ pridobi dostop do podatkovnih vrat (port-a) v računalniku, so lahko ogroženi naši podatki in morda tudi celotno omrežje našega podjetja. Tovrstnim situacijam se je potrebno izogniti za vsako ceno.

Druga morebitna nevarna praksa je **polnjenje naprave prek USB kabla na javnih postajah** za polnjenje telefonov. Če je to edina možnost polnjenja, uporabimo zaščito podatkov v obliki USB, ki povezuje električno omrežje z vhodom, ne omogoča pa prenosa podatkov.

## 11 Službenih računalnikov ali naprav nikoli ne puščajmo na nezavarovanih mestih

Da se izognemo kraji službenih naprav in s tem občutljivih osebnih ali poslovnih podatkov, jih moramo imeti vedno pri sebi. Ne puščamo jih v avtomobilu – niti v prtljažniku. Tudi hotelske sobe niso varne, saj lahko osebje kadar koli dostopa do njih.

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