Spoštovani,

zavedamo se, da je pred nami daljše obdobje, v katerem bomo primorani prilagoditi poslovanje situaciji, ki nam jo je vsilila pandemija COVID-19. V Detektivsko varnostni agenciji, d. o. o. smo za vas pripravili nekaj nasvetov za varno delo od doma.

Delo od doma, poleg zakonskih izzivov prinaša tudi izzive s področja informacijske varnosti. Zato je pomembno, da se zavedamo, da smo v tem času še dodatno izpostavljeni spletnim napadom in gospodarskemu vohunjenju.

Pri tem opozarjamo predvsem na naslednje nevarnosti:

- Phishing napadi (pojav lažnih oziroma oderuških "hitrih kreditov", davčnih olajšav ipd.),
- Lažne URL povezave (lažne spletne strani za prodajo zaščitne opreme ipd.),
- Fizični napadi (z uporabo socialnega inženiringa neposredno pri žrtvi, kjer npr. storilci nudijo brezplačne maske, pri tem pa izkoristijo dostop do infrastrukture),
- Druge oblike socialnega inženiringa (različni klasični napadi, ki izkoriščajo človeško dobroto in željo po pomoči) in
- Okužena spletna mesta (najpogosteje v obliki zemljevidov za spremljanje izbruha COVID-19, kjer morate prenesti "poseben" vtičnik, ki napadalcu omogoča popolni oddaljeni dostop do vaše naprave).

V prihodnje je mogoče pričakovati tudi stopnjevanje in povečanje obsega tovrstnih napadov, tudi z emaili, ki vas vabijo, da donirate za različne dobrodelne namene ipd.

V nadaljevanju smo vam pripravili nekaj preprostih nasvetov, ki bodo povečali vašo informacijsko varnost.

NASVETI (ker za obvladovanje COVID-19 ni dovolj, da si umivamo le roke, potrebna je tudi spletna higiena):

1. Za delo od doma uporabljajte službeni računalnik in za privatne zadeve uporabljajte privatni računalnik,
2. Redno posodabljajte programsko opremo,
3. Uporabljajte VPN (po možnosti lasten VPN do službenih strežnikov),
4. Če je le možno doma ne uporabljajte WiFi, če pa že uporabljate WiFi uporabljajte le svoj WiFi, kjer veste, kdo je povezan v omrežje. WiFi naj bo ustrezno zavarovan s kompleksnim geslom in WPA3 ali vsaj WPA2 standardom,
5. Izgubljeno ali odtujeno opremo takoj prijavite,
6. Zaupne informacije so še vedno zaupne (pazite, kaj tiskate doma in kaj odvržete v smeti - ustrezno uničite natisnjene dokumente, preden jih zavržete). Še naprej ohranjajte politiko čiste mize, tudi doma,
7. Za komunikacijo uporabljajte le aplikacije, ki zagotavljajo šifrirano komunikacijo po principu end-to-end,
8. Bodite pozorni na odpiranje neznanih URL povezav, še posebej bodite pozorni na skrajšane URL povezave,
9. Bodite pozorni na prejeta email sporočila. Tudi, če je email prišel iz vaše domene @vašadomena.com, ne pomeni, da ne gre za zlorabo. V primeru, da gre za nenavadne zahteve, pokličite pošiljatelja in preverite zahtevo in
10. Uporabljajte posodobljeno proti virusno zaščito.

NEKAJ UPORABNIH POVEZAV:

1. Preverjanje zaglavja prejetih email sporočil: https://mxtoolbox.com/EmailHeaders.aspx
2. Preverite skrajšane URL povezave: https://www.expandurl.net/
3. Preverite ali je URL povezava varna: https://safeweb.norton.com/, https://www.virustotal.com/gui/home/url
4. Preverite ali je prejeta datoteka okužena: https://www.virustotal.com/gui/home/upload
5. Seznam spletnih groženj povezanih s COVID-19: https://www.webarxsecurity.com/covid-19-cyber-attacks/
6. Prava URL povezava do COVID-19 zemljevida: https://coronavirus.jhu.edu/map.html

V Detektivsko varnostni agenciji, d. o. o. vam stojimo ob strani in skrbimo za vašo varnost tudi v tem kriznem času.

Detektivsko varnostna agencija, d. o. o.
+386 (0)1 292 77 95
Brnčičeva ulica 13,1231 Ljubljana - Črnuče
http://www.detektiv-dva.si