**JUST Training Fiche: Interacting safely in a digital setting**

|  |  |  |
| --- | --- | --- |
| **Title** | Varna interakcija v digitalnem okolju | |
| **Keywords** | Kibernetska varnost, oblak, zasebnost, spletni bonton | |
| **Provided by** | Internet Web Solutions | |
| **Language** | Slovenščina | |
| **Objectives** | Cilji tega modula so razložiti pomen vzdrževanja dobrih praks kibernetske varnosti, poudariti pomen zaščite osebnih podatkov in zagotoviti splošno predstavo o najbolj priročnih in učinkovitih orodjih za kibernetsko varnost. | |
| **Learning outcomes** | * Spoznavanje kibernetske varnosti: Protokoli so enako pomembni kot aplikacije * Razvijanje odgovornosti: Še posebej pomembna sta spletni bonton in zdrav razum * Razumevanje, kako ohraniti zasebnost: biti zelo pozoren na vsebino, ki se deli na spletu. * Razumevanje uporabnih orodij, kot so VPN, Antimalware in aplikacije v oblaku | |
| **Training Area** | **Poslovni bonton** |  |
| **Digitalne spretnosti** | **X** |
| **Mehke veščine** |  |
| **Pametno delo** |  |
| **Content index** | **Varna interakcija v digitalnem okolju**  **Enota 1: Nasveti in triki za kibernetsko varnost**  Razdelek 1.1: Uvod  Razdelek 1.2: Bodite obveščeni  Razdelek 1.3: Uporabite varnostne kopije!  Razdelek 1.4: Gesla in večfaktorska avtentikacija  **Enota 2: Varne prakse**  Razdelek 2.1: Varujte svojo zasebnost  Razdelek 2.2: Pazite na spletni bonton  **Enota 3: Orodja za izboljšanje varnosti IKT**  Razdelek 3.1: VPN  Razdelek 3.2: Zaščita pred zlonamerno programsko opremo  Razdelek 3.3: Oblak | |
| **Training content** | **Varna interakcija v digitalnem okolju**  **Enota 1: Nasveti in triki za kibernetsko varnost**  **Uvod**  Živimo v vedno bolj povezanem svetu. To vključuje občutek potrebe, da delimo najboljše z našega zadnjega potovanja v naš krog na Instagramu ali preusmerimo temo s prostega časa na delo, vsak klic ali izmenjavo e-pošte, v kateri sodelujemo med našim izobraževalnim in/ali delovnim življenjem.  Te izmenjave informacij nevede vsebujejo veliko podatkov o nas, pogosto občutljivih, ki jih lahko ukradejo in zberejo ljudje, ki jih želijo nezakonito izkoristiti.  Zato je imeti protokole kibernetske varnosti ali samo prakse (kar ne pomeni samo namestitve protivirusnega programa in nato nehati skrbeti) bistvenega pomena za naše spletno življenje.  Bodite obveščeni  Naše naprave nas običajno nadlegujejo z neprijetnimi obvestili o »novi posodobitvi programske opreme«. Čeprav včasih na prvi pogled ne spremenijo ničesar, so te posodobitve zelo uporabne, saj popravljajo nedavno odkrite hrošče in varnostne težave, ki lahko predstavljajo tveganje za naše naprave in informacije, ki jih vsebujejo.  Vendar so lahko te posodobitve programske opreme kratkotrajne, saj hekerji vedno iščejo ranljivosti programske opreme, kar poudarja pomen posodabljanja naših naprav.  Uporabite varnostne kopije!  Hranjenje ločene dodatne kopije vaših datotek je varna stava, ko se kljub našim prizadevanjem zgodi najhujše in se datoteke poškodujejo ali naš sistem doživi kibernetski napad. Da bi se temu izognili, lahko naše datoteke varno shranimo na zunanji disk in/ali spletne aplikacije v oblaku.  V nasprotju s splošnim prepričanjem je treba varnostne kopije ustvariti med postopkom izdelave in ne šele, ko je datoteka končana. Na ta način se lahko preprosto vrnete na prejšnje ponovitve datoteke, če gre kaj narobe s sredinskim osnutkom.  Gesla in večfaktorska avtentikacija  Pogosto spregledana gesla so pomemben del kibernetske varnosti. Kljub težavam s pomnjenjem in predstavljanjem znakovno popolnih, dolgih gesel z as m4nY! vrste znakov so obvezne. Ni treba posebej poudarjati, da uporaba datuma rojstva (in podobno) ni možnost.  Zaradi pogostih vdorov v varnost so lahko gesla tudi zlahka ogrožena, zato imejte različna gesla v vsaki napravi ali računu in jih ne pozabite redno spreminjati!  Večfaktorsko preverjanje pristnosti je sistem, ki kibernetskim kriminalcem otežuje delo, saj poleg gesla zahteva dodatne poverilnice za vstop v vaš račun, na primer kodo SMS, klic ali uporabo določene aplikacije.  Enota 2: Varne prakse  Varujte svojo zasebnost!  Kibernetsko varnost običajno povezujemo s hekerji, ki uporabljajo najsodobnejša orodja za vdiranje v naše račune. Resnica je, da večina njihovega uspeha izvira iz googlanja in zbiranja "javnih informacij" iz družbenih medijev, blogov in forumov.  Na ta način, če radi za svoja gesla uporabljamo kombinacijo imena svojega ljubljenčka, maminega priimka, številke vrat itd., je vprašanje časa, kdaj bo heker lahko vse to pobral od tu in tam, ponovno združil in vlomiti.  Ponovno premislite, kaj za vas pomenijo »zasebni podatki«. Vrnite se na svojo(-e) časovnico(-e), poiščite morebitne slike osebne izkaznice/kreditne kartice/osebnih dokumentov (lahko so poslovilne objave, zahvale ali lažne objave) in jih izbrišite. Bodite pozorni tudi na vse profile, ki vsebujejo preveč nepotrebnih osebnih podatkov.  Ne pozabite: če ne želite, da neznanci vidijo kakršno koli informacijo, je preprosto ne objavljajte!  Pazi na internetni bonton  »Netiquette« je niz pravil vljudnosti, namenjenih olajšanju spletnega sobivanja, tako kot imamo družbene konvencije za svet brez povezave, kot so mahanje, pozdrav in beseda »prosim«.  Poleg tega, kot v resničnem življenju, upoštevajte, da ta kodeks ravnanja ni nespremenljiv in je odvisen od konteksta. Dober primer tega je nabor pravil, ki so običajno lepljivo objavljena v skupinah ali forumih na Facebooku.  Prvotna pravila »netquette« Virginie Shea (1994) so še vedno veljavna z nekaterimi posodobitvami, kot na primer v naslednjem primeru:  • Izogibajte se uporabi spletnih skupnosti kot nadomestkov za Google – v bistvu poskusite poiskati prejšnje objave/teme, ki so že odgovorile na to vprašanje.  • Omejite uporabo dodatnih ločil, okrajšav, emojijev, velikih začetnic in alternativnega črkovanja – C0Z N0B0DY wantz T0 R3AD MESSAG3S L1KE th1s, rite???? 😃😃😃  • Ne pošiljajte neželene pošte svojih izdelkov ali storitev – običajno so za to ločeni, posebni prostori. Če jih ne vidite, niste na pravem mestu.  • Ne pošiljajte osebnih ali zasebnih podatkov – glejte prejšnji razdelek.  • Priznajte avtorjem ustrezno priznanje – ne le s pravnega vidika, ampak tudi zato, ker ljudje sovražijo plagiat, vendar radi vidijo, da se njihovo delo deli z drugimi.  Enota 3: Orodja za izboljšanje varnosti IKT  VPN-ji  Ne bo vse po merah, pravilih in navadah. Na srečo obstaja veliko orodij, zasnovanih za boj proti kibernetskim grožnjam, kot so VPN, aplikacije za zaščito pred zlonamerno programsko opremo in aplikacije v oblaku.  VPN so filtri, ki prikrijejo vašo spletno identiteto in šifrirajo vaše podatke. To stori tako, da se poveže z zasebnim strežnikom. To stori tako, da se poveže z zasebnim strežnikom, ki kodira vaše podatke, blokira zunanji dostop do njih in jih naredi neberljive, če jih ukradejo.  Poleg tega ima večina VPN-jev strežnike v več državah, kar pomeni, da imamo veliko možnosti, da svoj IP prikrijemo kot tujega in dostopamo do geografsko blokiranih vsebin, ki v naši državi niso na voljo:  • NordVPN in Access sta dve razumno plačani možnosti, ki nam omogočata varno brskanje.  • Poleg tega Surfshark in Tunnelbear ponujata tudi privlačne in zanesljive brezplačne načrte.  Antimalware  Kljub temu, da se običajno imenuje "protivirusna programska oprema", je programska oprema za zaščito pred zlonamerno programsko opremo zasnovana za odkrivanje, karanteno in odpravljanje vseh kibernetskih groženj, ne le virusov.  Medtem ko so virusi zasnovani tako, da se razmnožujejo in povzročajo okvare naprav, je zlonamerna programska oprema krovni izraz za kakršno koli zlonamerno programsko opremo, ki širi neželeno pošto in oglase ter krade podatke in gesla (in morda celo zahteva odkupnino!).  Dandanes je res, da ima večina programske opreme proti zlonamerni programski opremi protivirusno aplikacijo in obratno, z velikim naborom funkcij in načinov:  • Po plačljivih možnostih izstopajo ESET, Norton in Avast.  • Poleg tega brezplačni različici Malwarebytes in Bitdefender ponujata tudi prvovrstno storitev.  Oblak  »Oblak« je spletna storitev gostovanja, ki uporabnikom omogoča nalaganje, spreminjanje, shranjevanje in skupno rabo svojih datotek.  Shranjevanje vaših datotek na spletu v zasebne strežnike ščiti omenjene datoteke pred morebitnimi lokalnimi napadi ali poškodbami in preprečuje težave s fizičnimi trdimi diski, kot je pomanjkanje prostora, izgube ali poslabšanje. »Oblak« kljub imenu ni edinstvena entiteta, ampak ima vsak ponudnik svojega, zato je na voljo več možnosti:  • Dropbox je priljubljena možnost kljub temu, da se je preusmeril na plačljive načrte, in ponuja 2 GB brezplačnega paketa.  • S 5 GB oziroma 15 GB ponujata tudi Microsoftov OneDrive in Google Drive popolno integracijo v svojih okoljih.  • Končno, čeprav se večinoma uporablja za skupno rabo datotek, MEGA brezplačnim uporabnikom omogoča shranjevanje do 20 GB. | |
| **Glossary** | Varnostna kopija: digitalna kopija datoteke, shranjena ločeno in uporabljena v primeru izgube ali poškodbe izvirnika.  Večfaktorska avtentikacija: način dostopa, ki zahteva predložitev dveh ali več dokazov za dodatno varnost.  VPN: filtri, ki prikrijejo vašo spletno identiteto in šifrirajo vaše podatke. To stori tako, da se poveže z zasebnim strežnikom, ki kodira vaše podatke, blokira zunanji dostop do njih in jih naredi neberljive, če jih ukradejo.    Antimalware: programska oprema, zasnovana za odkrivanje, karanteno in odpravljanje kakršnih koli kibernetskih groženj, ne samo virusov.    Oblak: storitev spletnega gostovanja, ki uporabnikom omogoča nalaganje, spreminjanje, shranjevanje in skupno rabo svojih datotek stran od lokalnih napadov ali poškodb. | |
| **Self-evaluation (multiple choice queries and answers)** | 1. Spletni bonton ne zagovarja:  a) Iščete prejšnje odgovore, ki bi vam lahko pomagali.  b) Uporaba velikega števila okrajšav.  c) Zasluge avtorjem.  2. Objava osebnih podatkov je najvarnejša, če:  a) Objavljeno zasebno.  b) Ni objavljeno.  c) Naloženo v oblak.  3. Hekerji zberejo večino svojih informacij o povprečnih uporabnikih tako, da:  a) Googlanje njihovih imen.  b) Uporaba sofisticirane programske opreme.  c) Izsiljevanje.  4. Ali so virusi in zlonamerna programska oprema enaki?  a) Da, so sinonimi.  b) Sploh ne.  c) Virusi so le vrsta zlonamerne programske opreme.  5. Kateri ima največ prostora?  a) Google Drive  b) Dropbox   1. c) Mega | |
| **Bibliography** | * <https://www.ionos.es/digitalguide/online-marketing/redes-sociales/netiquette/#:~:text=Este%20t%C3%A9rmino%20hace%20referencia%20a,t%C3%A9rmino%20netiqueta%2C%20su%20traducci%C3%B3n%20directa> * <https://www.avast.com/es-es/c-malware-vs-virus#:~:text=%C2%BFCu%C3%A1l%20es%20la%20diferencia%20entre,que%20un%20tipo%20de%20malware> * <https://www.trellix.com/en-au/security-awareness/ransomware/malware-vs-viruses.html#:~:text=Malware%20is%20a%20catch%2Dall,its%20code%20into%20other%20programs> | |
| **Resources (videos, reference link)** |  | |