**JUST Training Fiche: Bezpečná interakcia s digitálnym svetom**

|  |  |  |
| --- | --- | --- |
| **Názov** | Bezpečná interakcia s digitálnym svetom | |
| **Kľúčové slová** | Kybernetická bezpečnosť, Cloud, Online bezpečnosť, Netiketa | |
| **Autor** | Internet Web Solutions | |
| **Jazyk** | Slovenčina | |
| **Ciele** | Cieľom tohto modulu je vysvetliť **dôležitosť udržiavania zaužívaných postupov** v oblasti **kybernetickej bezpečnosti**, zdôrazniť dôležitosť **ochrany osobných údajov** a poskytnúť všeobecnú predstavu o najpraktickejších a **účinných nástrojoch kybernetickej bezpečnosti.** | |
| **Ciele vzdelávania** | * Zoznámenie sa s kybernetickou bezpečnosťou: Protokoly sú rovnako dôležité ako aplikácie * Rozvíjanie zodpovednosti: Netiketa a zdravý rozum sú obzvlášť dôležité * Pochopenie toho, ako si zachovať súkromie: Dávajte si veľký pozor na obsah zdieľaný online. * Pochopenie nástrojov, ako sú VPN, antimalvér a cloudové aplikácie | |
| **Okruhy tréningov** | **Obchodná etiketa** |  |
| **Digitálne zručnosti** | **X** |
| **Mäkké zručnosti (Soft Skills)** |  |
| **Inteligentná práca (Smart Working)** |  |
| **Obsah** | **Bezpečná interakcia s digitálnym svetom**  **Časť 1: Kyberbezpečnosť - tipy a triky**  Sekcia 1.1: Úvod  Sekcia 1.2: Ostaňte v dianí!  Sekcia 1.3: Zálohujte!  Sekcia 1.4: Heslá a viac-faktorové overovanie  **Časť 2: Bezpečnostné praktiky**  Sekcia 2.1: Chráňte si súkromie  Sekcia 2.2: Pozor na netiketu  **Časť 3: Nástroje na zlepšenie IKT bezpečnosti**  Sekcia 3.1: VPN  Sekcia 3.2: Antimalvér  Sekcia 3.3: Cloud | |
| **Tréningový obsah** | **Bezpečná interakcia s digitálnym svetom**  **Časť 1: Kyberbezpečnosť - tipy a triky**  **Úvod**  Žijeme v **čoraz viac prepojenom svete**. To sa spája s potrebou zdieľať to najlepšie z našej poslednej cesty na našom instagramovom profile alebo zmeniť súkromnú tému na pracovnú, každý hovor alebo výmenu e-mailov, ktorých sa zúčastňujeme počas nášho voľného času a / alebo pracovného života.  Informácie o nás obsahujú **množstvo citlivých údajov**, ktoré môžu byť ukradnuté a zhromaždené ľuďmi, ktorí ich **chcú nelegálne využiť**.  Preto je pre náš online život nevyhnutné vytvárať **protokoly** **kybernetickej bezpečnosti** a vedieť ich použiť v praxi, čím nemáme na mysli len inštaláciu antivírusových programov.  **Ostaňte v dianí**  Naše zariadenia nás zvyčajne obťažujú nepríjemnými upozorneniami na „novú aktualizáciu softvéru“. Napriek tomu, že sa niekedy na prvý pohľad nič nezmení, tieto **aktualizácie sú veľmi užitočné**, pretože opravujú nedávno objavené chyby a bezpečnostné problémy, ktoré môžu predstavovať riziko pre naše zariadenia a informácie, ktoré obsahujú.  Tieto aktualizácie softvéru však môžu byť krátkodobé, pretože **hackeri neustále hľadajú chyby zabezpečenia**, čo zdôrazňuje dôležitosť aktualizácie našich zariadení.  **Zálohujte!**  Uchovávanie kópie vašich súborov je zväčša hra na istotu, keď napriek nášmu úsiliu dôjde k najhoršiemu a súbory sa poškodia alebo náš systém zasiahne kybernetický útok. Aby sme tomu zabránili, naše súbory by mali byť bezpečne uložené na externom disku a/alebo online cloudových aplikáciách.  Záložné verzie by sa mali vytvárať počas procesu spracovania a nie až po dokončení súboru. Týmto spôsobom sa môžete ľahko vrátiť k predchádzajúcim verziám súboru v prípade, že sa niečo pokazí v polovici návrhu.  **Heslá a viac-faktorové overovanie**  Heslá sú dôležitou súčasťou kybernetickej bezpečnosti. Napriek problémom s ich zapamätaním a zavedením charakterovo dokonalých, **dlhých hesiel so špeciálnym typom znakov** ako “m4nY! t” sú nevyhnutné. Netreba dodávať, že použitie dátumu narodenia (a podobných informácií) neprichádza do úvahy pre kvalitné zabezpečenie súborov.  V dôsledku častého narušenia bezpečnosti je tiež možné heslá ľahko prelomiť, preto majte na každom zariadení alebo účte iné **heslá a nezabudnite ich pravidelne meniť**!  **Viacfaktorové overovanie** je systém, ktorý sťažuje kyberútoky tým, že vyžaduje ďalšie prihlasovacie údaje okrem hesla na zadanie vášho účtu, napríklad SMS kód, hovor alebo použitie špecifickej aplikácie.  **Časť 2: Bezpečnostné praktiky**  **Chráňte si súkromie!**  Máme tendenciu spájať kybernetickú bezpečnosť s hackermi, ktorí pomocou najmodernejších nástrojov prenikajú do našich účtov. Pravdou je, že **väčšina ich úspechu pochádza z googlovania a zhromažďovania „verejných informácií“ zo sociálnych médií, blogov a fór**.  Za predpokladu, že používame pre svoje heslá kombináciu mena nášho domáceho miláčika, priezviska matky, čísla dverí a pod., je iba otázkou času, kedy to sem-tam nejaký hacker dokáže zozbierať, prekombinovať a vlámať sa.  Zvážte, čo pre vás znamenajú „súkromné informácie“. Vráťte sa na svoju časovú os, nájdite akékoľvek obrázky svojho preukazu totožnosti/kreditnej karty/osobných dokumentov a odstráňte ich. **Venujte pozornosť aj profilom, ktoré obsahujú príliš veľa nepotrebných osobných údajov.**  Pamätajte si: Ak si neželáte, aby nejaké informácie videli cudzí ľudia, **jednoducho ich nezverejňujte!**  **Pozor na netiketu**  „**Netiketa“ je súbor pravidiel zdvorilosti navrhnutých na uľahčenie online spolužitia.** Rovnako ako máme spoločenské konvencie pre offline svet, ako je mávanie, pozdrav a čarovné slovo „prosím“.  Tak ako v skutočnom živote, **majte na pamäti, že tento kódex správania nie je nemenný a závisí od kontextu.** Dobrým príkladom je súbor pravidiel, ktoré sa zvyčajne uverejňujú na skupinách alebo fórach na Facebooku.  Pôvodné pravidlá „netikety“ od Virginie Shea (1994) sú stále platné s niektorými aktualizáciami, ako napríklad v nasledujúcom príklade:   * **Vyhnite sa zaťažovaniu užívateľov skupín generickými dopytmi, ktoré vie obslúžiť google Google** – V podstate sa pokúste vyhľadať predchádzajúce príspevky/vlákna, ktoré už na daný problém odpovedali. * **Skúste obmedziť používanie ďalších interpunkčných znamienok, skratiek, emoji, veľkých písmen a alternatívneho pravopisu pri online interakcii** – C0Z N0B0DY wantz T0 R3AD MESSAG3S L1KE th1s, rite???? 😃😃😃 * **Nespamujte vašimi vlastnými produktmi alebo službami** – zvyčajne na to existujú samostatné, špecifické priestory ako online inzercia. * **Neposielajte žiadne osobné ani súkromné informácie** – pozrite si predchádzajúcu časť. * **Uznávajte práva autorov** – nielen z právneho hľadiska, ale aj preto, že hoci ľudia nenávidia plagiáty, radi vidia zdieľanie svojej práce.   **Unit 3: Nástroje na zlepšenie IKT bezpečnosti**  **VPN**  Nie všetko je postavené na opatreniach, pravidlách a zvykoch. Našťastie existuje množstvo nástrojov určených na boj proti kybernetickým hrozbám, ako sú VPN, antimalvér a cloudové aplikácie.  VPN sú filtre, ktoré maskujú vašu online identitu a šifrujú vaše údaje. Fungujú na princípe pripojenia sa k súkromnému serveru, ktorý zakóduje vaše údaje, zablokuje k nim externý prístup a v prípade krádeže ich urobí nečitateľnými.  Väčšina sietí VPN má navyše servery v niekoľkých krajinách, čo znamená, že máme veľa možností, ako zamaskovať našu IP ako zahraničnú a získať prístup k geograficky blokovanému obsahu, ktorý nie je v našej krajine dostupný. Vyskúšajte napríklad:   * NordVPN a Access sú dve primerane platené možnosti, ktoré nám umožňujú bezpečne prehliadať. * Surfshark a Tunnelbear navyše ponúkajú atraktívne a spoľahlivé bezplatné plány a vernostné programy.   **Antimalvér**  Napriek tomu, že sa bežne nazýva „antivírus“, antimalvérový softvér je navrhnutý na detekciu, karanténu a elimináciu akýchkoľvek kybernetických hrozieb, nielen vírusov.  Zatiaľ čo vírusy sú navrhnuté tak, aby sa **replikovali** a spôsobili poruchu zariadení, **malvér je zastrešujúci termín pre akýkoľvek druh škodlivého softvéru, ktorý šíri spam a reklamy a kradne informácie a heslá** (a môže dokonca žiadať o výkupné!).  V súčasnosti je pravdou, že väčšina antimalvérových softvérov má antivírusovú aplikáciu, s veľkým rozsahom funkcií a modalít:   * Pokiaľ ide o platené možnosti, ESET, Norton a Avast vynikajú. * Okrem toho bezplatné verzie Malwarebytes a Bitdefender ponúkajú   tiež prvotriednu službu.  **Cloud**  „Cloud“ je online hostingová služba, ktorá používateľom umožňuje nahrávať, upravovať, ukladať a zdieľať svoje súbory.  Ukladanie súborov online na súkromných serveroch chráni uvedené súbory pred akýmkoľvek lokálnym útokom alebo poškodením a predchádza problémom s fyzickými pevnými diskami, ako je nedostatok miesta, strata alebo poškodenie. Napriek svojmu názvu „Cloud“ , nejedná sa o jedinečnú službu, ale každý poskytovateľ má svoj vlastný, a preto existuje niekoľko možností:  Dropbox, populárna možnosť, napriek prechodu na platené programy, ponúka bezplatné využitie do 2 GB. Plnú integráciu ponúkajú OneDrive a Disk Google od spoločnosti Microsoft s 5 GB a 15 GB kapacity. | |
| **Slovník** | **Záloha**: digitálna kópia súboru uložená oddelene a použitá v prípade straty alebo poškodenia originálu.  **Viacfaktorová autentifikácia**: Spôsob prístupu, ktorý vyžaduje predloženie dvoch alebo viacerých dôkazov na zvýšenie bezpečnosti.  **VPN**: filtre, ktoré maskujú vašu online identitu a šifrujú vaše údaje. Robí to pripojením k súkromnému serveru, ktorý zakóduje vaše údaje, zablokuje k nim externý prístup a v prípade krádeže ich urobí nečitateľnými.    **Antimalvér**: softvér určený na detekciu, karanténu a elimináciu akýchkoľvek kybernetických hrozieb, nielen vírusov.    **Cloud**: Online hostingová služba, ktorá používateľom umožňuje nahrávať, upravovať, ukladať a zdieľať svoje súbory bez lokálnych útokov alebo korupcie. | |
| **Sebahodnotenie** | 1. Netiketa neobhajuje:   1. Hľadajte predchádzajúce odpovede, ktoré by vám mohli pomôcť. 2. **Používanie veľkého množstva skratiek.** 3. Dávať autorom náležité uznanie.   2. Zverejnenie osobných údajov je najbezpečnejšie, ak:   1. Sú zverejnené súkromne. 2. **Nie sú zverejnené.** 3. Sú nahrané do cloudu.   3. Hackeri zhromažďujú väčšinu svojich informácií o priemerných používateľoch:   1. **Googlením ich mien.** 2. Pomocou sofistikovaného softvéru. 3. Ich vydieraním.   4. Sú pojmy ako vírus a malvér rovnaké?   1. Áno, sú to synonymá. 2. Vôbec nie. 3. **Vírus je len typom malvéru.**   5. Ktorý cloud ponúka najviac miesta?   1. disk Google 2. Dropbox 3. **Mega** | |
| **Bibliografia** | * <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> | |
| **Iné zdroje** |  | |