Karta szkoleniowa IWS

|  |  |
| --- | --- |
| **Tytuł** | **Tożsamość cyfrowa i reputacja w internecie** |
| **Obszar**  **szkoleniowy** | *Wybierz co najmniej jedno z poniższych:*   |  |  | | --- | --- | | Bezpieczeństwo w Internecie |  | | Umiejętność korzystania z kultury i mediów |  | | Transakcje gospodarcze |  | | Ochrona danych osobowych |  | | Tożsamość cyfrowa i reputacja online | *X* | |
| **Słowa**  **kluczowe**  **(metatag)** | **Tożsamość cyfrowa, reputacja online, internet, oszustwa, online, sieci społecznościowe** |
| **Dostarczone przez** | **Internet Web Solutions** |
| **Język** | **Polski** |
| **Cele i wyniki szkolenia** | |
| **Pod koniec tego modułu będziesz mógł:**  **Dowiedzieć się, co powinieneś wiedzieć o swojej tożsamości cyfrowej i reputacji online.**  **Moduł skupia się na:**  **Część 3.1. Doktor Jack i pan Hyde (kim jesteście ty i inni w internecie i jak was chronić)**  **Rozdział 3.1.1 Wstęp**  **Rozdział 3.1.2. Kradzież tożsamości: co się stanie, jeśli ukradną twoją tożsamość?**  **Rozdział 3.2.3. Kradzież konta: co się stanie, jeśli użyją twoich kont? Kilka wskazówek, jak tego uniknąć.**  **Rozdział 3.2.4. Dalsze wskazówki** | |
| **Opis** | |
| **Ta jednostka podaje „zalecenia i zakazy”, takie jak „Nie używaj komputerów publicznych”, „Ustaw silne i złożone hasło”, „Upewnij się, że korzystasz z bezpiecznego połączenia”, uwierzytelnianie dwupoziomowe itp., aby chronić swoją tożsamość cyfrowa. Ta jednostka opowie również o bezpiecznych sposobach korzystania z mediów społecznościowych i o tym, czego nie ujawniać w internecie.** | |
| **Zawartość przedstawiona na 3 poziomach** | |
| **Część 3.1 Doktor Jack i Pan Hyde (kim jesteście wy i inni w internecie i jak was chronić)**  **Rozdział 3.1.1 Wstęp:**  W internecie jesteś wszystkim, co publikujesz i wszystkim, co komentujesz innym użytkownikom.  Wszystko, co publikujesz online, może być widoczne dla innych użytkowników.  Nawet jeśli możesz ustawić ustawienia prywatności, w których publikujesz posty, na "tylko znajomi" lub podobne, osoba, która chce zobaczyć twój post, ma sposoby, aby go uzyskać.  To,ze za ekranem jestes niewidzialny nie daje ci przyzwolenia na nieodpowiednie zachowanie wobec innych.  W przeciwieństwie do prawdziwego życia, wszystko, co publikujesz w internecie, ma ogólnoświatową ekspozycję.  Oznacza to, że ludzie z całego świata mogą dowiedzieć się o tobie, a także ty możesz dowiedzieć się o ludziach z całego świata.  Oszust może obserwować znacznie więcej osób i ostrożniej wybrać swoją ofiarę. Ten  i inne czynniki sprawiają, że oszustwa internetowe są coraz bardziej powszechne.  **Rozdział 3.1.2. Kradzież tożsamości: co się stanie, jeśli ukradną twoją tożsamość?**  Osoba, która nielegalnie korzysta z Twojego konta, może wykonać wiele niebezpiecznych działań.  W najlepszym razie mogą podszywać się pod ciebie, aby publikować kompromitujące lub nielegalne posty.  W najgorszym przypadku mogą podszywać się pod ciebie i rozmawiać ze znajomymi lub rodziną, mówiąc im, że masz problem i potrzebujesz pieniędzy, oszukując ich w ten sposób.  Innym niebezpiecznym przypadkiem jest to, że jeśli ktoś ma dostęp do twoich danych bankowych, może wykonywać zakupy online lub inne transakcje i ukraść twoje pieniądze.  Jeśli tak się stanie, spróbuj skontaktować się z pomocą techniczną platformy, na której skradziono twoje konto, zmień hasła, powiadom osoby, których to dotyczy, a jeśli złodziej był w stanie dokonać zakupu, powiadom również swój bank.  Kradzież tożsamości dotyczy nie tylko ciebie.  **Rozdział 3.2.3 Kradzież konta: co się stanie, jeśli będą korzystać z twoich kont?**  Niebezpiecznym przypadkiem jest to, że jeśli ktoś ma dostęp do twoich danych bankowych, może wykonywać zakupy online lub inne transakcje i ukraść twoje pieniądze.  Jeśli tak się stanie, spróbuj skontaktować sie z pomocą techniczną platformy, na której skradziono twoje konto, zmień hasła, powiadom osoby, których to dotyczy, a jeśli złodziej był w stanie dokonać zakupu, powiadom również swój bank.  Jest kilka rzeczy, które możesz zrobić, aby uniknąć kradzieży konta:  - Nie zapisuj haseł na żadnym urządzeniu, spróbuj je zapamiętać.  - Spróbuj użyć różnych haseł do różnych witryn. Jeśli ktoś znajdzie Twoje hasło do jednej platformy, nie będzie mógł uzyskać dostępu do innych witryn.  - Nie używaj swojego imienia i nazwiska, nazwy użytkownika ani innych danych osobowych na platformie, które ułatwiają znalezienie informacji.  -Używaj haseł dłuższych niż 8 znaków i używaj liczby lub znaku specjalnego, aby uniknąć ataków oszustow.  Nigdy nie udostępniaj swojego hasła online, nawet jeśli ktoś powie ci, że jest moderatorem, administratorem lub personelem pomocy technicznej witryny.  **rozdział 3.2.4. Dalsze wskazówki**  Najbardziej musisz uważać na to, co robisz w mediach społecznościowych.publikować .  Staraj się publikować jak najmniej informacji o sobie, zwłaszcza poufnych, danych identyfikacyjnych lub danych bankowych.  Ważnymi informacjami, których **NIE** należy udostępniać publicznie, mogą być:  - lokalizacja, w której mieszkasz  - adres e-mail  - numer telefonu  - kompromitujące treści multimedialne  - dokumenty osobiste  - informacje o transakcjach bankowych  - informacje o wynagrodzeniu  - hasła wszelkiego rodzaju  Kradzież konta i tożsamości  Unikaj logowania się do kont na komputerach innych osób, zwłaszcza na komputerach publicznych.  Wiele platform obsługuje uwierzytelnianie dwuetapowe, np. za pomocą numeru telefonu, korzystaj z niego, gdy masz taką możliwość.  To, co trafia do Internetu, pozostaje online na zawsze. To, co opublikujesz, co powiesz, jak się zachowasz, będzie dostępne dla wszystkich, w tym: ewentualnych przyszłych pracodawców, twojej rodziny i dzieci oraz twoich przyjaciół. Nie tylko teraz, także w przyszłości. | |
| **Treść w punktach** | |
| **Staraj się publikować jak najmniej informacji o sobie, zwłaszcza poufnych informacji, danych identyfikacyjnych lub danych bankowych.**  **To, co trafia do internetu, pozostaje online na zawsze. To, co opublikujesz, co powiesz, jak się zachowasz, będzie dostępne dla wszystkich, w tym: ewentualnych przyszłych pracodawców, twojej rodziny i dzieci oraz twoich przyjaciół. Nie tylko teraz, także w przyszłości.**  **Używaj haseł dłuższych niż 8 znaków i używaj cyfr lub znaków specjalnych, aby uniknąć ataków ze strony oszustów.** | |
| **5 haseł ze słownika** | |
| **Tożsamość cyfrowa:**  *Tożsamość cyfrowa jest obecnie często wykorzystywana w sposób, który wymaga powiązania danych o osobach przechowywanych w systemach komputerowych z ich tożsamością cywilną lub narodową.*  **Reputacja online:**  *Jest to reputacja firmy, osoby, produktu, usługi lub dowolnego innego elementu w Internecie i na platformach cyfrowych.*  **Uwierzytelnianie dwuetapowe:**  *Jest to metoda uwierzytelniania elektronicznego, w której użytkownik uzyskuje dostęp do strony internetowej lub aplikacji dopiero po pomyślnym przedstawieniu dwóch lub więcej dowodów (lub czynników) w mechanizmie uwierzytelniania..*  **Kradzież tożsamości:**  *Nielegalna praktyka wykorzystywania imienia i nazwiska oraz danych osobowych innej osoby w celu uzyskania kredytu, pożyczek itp.*  **Oszust:**  *Oszust może obserwować znacznie więcej osób i ostrożniej wybrać swoją ofiarę. Ten i inne czynniki sprawiają, że oszustwa internetowe są coraz bardziej powszechne.* | |
| **Referencje i więcej informacji na ten temat** | |
| [**https://www.careercast.com/career-news/10-ways-build-your-online-identity**](https://www.careercast.com/career-news/10-ways-build-your-online-identity)  [**https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/**](https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/)  [**https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php**](https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php)  [**https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html**](https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html)  [**https://whatis.techtarget.com/definition/digital-identity**](https://whatis.techtarget.com/definition/digital-identity)  [**https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html**](https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html)  [**https://www.techopedia.com/definition/23915/digital-identity**](https://www.techopedia.com/definition/23915/digital-identity)  [**https://www.techopedia.com/definition/1327/domain-name**](https://www.techopedia.com/definition/1327/domain-name) | |
| **Pięć pytań do samooceny wielokrotnego wyboru** | 1. W internecie:   A. Tylko osoby, które znasz, mogą cię znaleźć  B. Tylko oszuści mogą cię znaleźć  C. Ludzie na całym świecie mogą cię znaleźć  **Poprawny: C**  2) Do czego służy kradzież tożsamości?  A. Oszust ma dostęp tylko do twoich danych bankowych  B. Oszust przychodzi do twojego domu i kradnie twój laptop  C. Oszust uzyskuje dostęp do twojego konta i wykonuje niebezpieczne/nielegalne działania  **Poprawny: C**  3) Jakie dane osobowe zalecamy nie publikować w internecie?  A. Twój rozmiar buta  B. Twój numer telefonu  C. Twój profil na Facebooku  **Poprawny: B**  **4**) Hasło i bezpieczeństwo. Które z poniższych stwierdzeń jest prawdziwe?  A. Lepiej nie zapisywać hasła na żadnym urządzeniu  B. Użyj hasła krótszego niż 8 znaków  C. Użyj swojego numeru telefonu jako hasła  **Poprawny: A**  5) Dlaczego tak ważne jest, aby unikać logowania się na komputerach innych osób?  A. Ponieważ jest to niebezpieczne  B. Aby chronić hasło  C. Aby chronić Twoją tożsamość cyfrową  **Poprawnie: A** |
|  |  |
| **Powiązane PPT** | [**SOS creativity Module 3 Digital Identity and Online Reputation**](file:///C:\Users\K-Ctech\Downloads\PPTs\SOS%20creativity%20Module%203%20Digital%20Identity%20and%20Online%20Reputation.pptx) |
| **Powiązany link** |  |
| **Film w formacie YouTube (jeśli istnieje)** |  |