PL

INTELIGENTNE TECHNOLOGIE 04

Bezpieczeństwo i urządzenia mobilne

Moduł opisuje wybrane zagadnienia, na które należy zwrócić uwagę podczas korzystania z technologii mobilnych.

Rozpocznij kurs>

Co-funded by the Erasmus+ Programme of the European Union

INTELIGENTNE TECHNOLOGIE MODUŁ 4

Bezpieczeństwo i urządzenia mobilne

W ciągu ostatnich kilkudziesięciu lat urządzenia mobilne zmieniły się z prostych do bardzo zaawansowanych technologicznie urządzań. Dziś na smartfonie możemy mieć dostęp do bankowości, różnych aplikacji, Internetu. Wraz z nowymi funkcjami pojawiła się obawa o bezpieczeństwo danych. W tym module wyjaśnimy jak chronić dane, jak tworzyć i zmieniać hasła, jak bezpiecznie korzystać z sieci Wi-Fi oraz jak chronić się przed cyberprzemocą i trollami internetowymi.

Dla kogo jest ten moduł?

Ten moduł jest przeznaczony dla wszystkich, którzy chcą dowiedzieć się o tym jak bezpiecznie poruszać się w sieci, o ochronie danych, ciasteczkach (cookies) i o tym jak prawo chroni nasze dane osobowe (RODO).

Jeśli będziesz czuł, że ten moduł stanowi dla Ciebie wyzwanie poproś przyjaciela aby przerobił go razem z Tobą.

Dla facylitatorów moduł ten może stanowić źródło informacji, które mogą wykorzystać później by udzielać porad na temat bezpieczeństwa w technologiach cyfrowych.

Czego nauczysz się w tym module

1. O ochronie danych osobowych RODO i zgodach na pliki cookie.
2. Jak tworzyć i zmieniać hasła.
3. Czym jest włamanie do systemu i jak można się przed nim zabezpieczyć?
4. Jak chronić się przed cyberprzemocą?

Rozdziały w tym module

INTELIGENTNE TECHNOLOGIE | MODUŁ 4 | ROZDZIAŁ 1

Bezpieczeństwo: urządzenia mobilne i własność danych

„Informacja to władza”! Dane osobowe są jednym z naszych najcenniejszych dóbr. We współczesnej erze ten ważny zasób jest zupełnie niedoceniany przez konsumentów, ale nie przez firmy! Niektóre z największych firm na świecie odniosły sukces dzięki umiejętnemu wykorzystaniu Twoich danych. W tym rozdziale wyjaśnimy kwestię własności danych w dobie urządzeń mobilnych i tzw. "chmury".

Czego nauczysz się w tym rozdziale

1. Czym jest Rozporządzenie o Ochronie Danych Osobowych (RODO).
2. Ochrona danych osobowych zgodnie z RODO.
3. Jak zarządzać plikami cookie.
4. Rodzaje danych osobowych.
5. Gdzie są przechowywane Twoje dane.
6. Jak wykonać kopię zapasową urządzenia mobilnego.

Analityka danych - jedna z najszybciej rozwijających się nowych branż

Gromadzenie i analizowanie danych jest ważne dla przedsiębiorstw, aby zrozumieć potrzeby swoich klientów i ulepszyć kierowane do nich usługi.

Analityka danych sprawia, że strony internetowe i aplikacje są bardziej użyteczne. Pozwala na przykład użytkownikowi smartwatcha (inteligentnego zegarka) zobaczyć liczbę kroków wykonanych w ciągu dnia. Analityka danych często wykorzystuje (Twoje) **dane osobowe.**

Dane osobowe, a urządzenia mobilne i urządzenia ubieralne

Dane osobowe to informacje, które pozwalają na zidentyfikowanie osoby fizycznej.

Firmy muszą chronić dane osobowe obywateli zgodnie **Rozporządzeniem o Ochronie Danych Osobowych (RODO)** poprzez kodowanie wrażliwych **informacji,** które są przechowywane lub przesyłane za pośrednictwem sieci publicznych.

RODO zostanie omówione w dalszej części tego rozdziału.

Dlaczego ważne jest zabezpieczanie danych gromadzonych przez urządzenia mobilne

W przypadku, gdy ktoś uzyskuje dostęp do danych osobowych - adresu, wieku, płci, kwestii zdrowotnych, statusu finansowego, zainteresowań danej osoby bez jej zgody może to spowodować problemy dla tej osoby.

Dane osobowe to dane, które odnoszą się do możliwej do zidentyfikowania osoby. Takie informacje pomagają spersonalizować usługę dla użytkownika. Firmy muszą chronić Twoje dane osobowe zgodnie z prawem **RODO,** szyfrując wrażliwe **informacje,** tj. dane osobowe, wysyłane do stron trzecich za pośrednictwem sieci publicznych.

Więcej informacji na ten temat można znaleźć na stronie https://uodo.gov.pl/pl/404/224.

Czym jest RODO?

Aby zapobiec pozyskiwaniu przez firmy danych osobowych obywateli bez ich zgody, Komisja Europejska wprowadziła **Rozporządzenie o Ochronie Danych Osobowych (RODO)**.

RODO chroni dane osobowe obywateli, którzy mieszkają i pracują na terenie Unii Europejskiej. Organizacje działające w UE muszą mieć zgodę na przetwarzanie danych osobowych.

RODO - jakie prawa daje na terenie UE?

RODO oferuje następujące prawa dla osób fizycznych:

- prawo do informacji,
- prawo dostępu,
- prawo do sprostowania i usunięcia danych,
- prawo do ograniczenia przetwarzania danych,
- prawo do przenoszenia danych,
- prawo do sprzeciwu,
- prawa dotyczące zautomatyzowanego profilowania.

Jakie rodzaje danych mogą kwalifikować się jako dane osobowe?

Aby zrozumieć znaczenie praw do prywatności danych w Unii Europejskiej, musimy znać rodzaje danych osobowych, na które może wpłynąć RODO.

Przyjrzyjmy się kilku typowym przykładom danych, które mogą być uznane za dane osobowe, a więc powinny być chronione.

Przykłady danych osobowych

1

2

3

Informacje demograficzne

Kiedy osoba wypełnia formularz, aby na przykład ubiegać się o dotację, obdarza zaufaniem organizację, która go sporządza, że będzie traktować informacje wrażliwe w sposób poufny. Jest to rodzaj danych osobowych.

Przykłady danych osobowych

1

2

3

Dokumentacja medyczna

Wizyta u lekarza jest uważana za prywatne i poufne doświadczenie. Dane, które są rejestrowane na temat indywidualnego pacjenta, są również wysoce poufne i stanowią dane osobowe.

Przykłady danych osobowych

1

2

3

Zapis codziennych czynności

Zapis dokonanych zakupów, odwiedzonych miejsc i podróży odbytych przez konkretną osobę to również dane osobowe.

Codzienne czynności

Urządzenia mobilne i ubieralne rejestrują niezwykłą ilość informacji na temat codziennej aktywności danej osoby. Wiele z tych danych osobowych trafia do baz danych w chmurze aplikacji mobilnych. Posiadając te dane, firmy technologiczne mogą dostarczać użytkownikowi szczegółowe informacje na temat jego aktywności.

Przykłady danych osobowych

4

5

Osobiste informacje finansowe

Wyciągi finansowe, informacja o zdolności kredytowej i salda bankowe to kolejna kategoria danych osobowych. Mogą one posłużyć do zakwalifikowania Cię jako osoby wydającej dużo lub kupującej z rozwagą.

Przykłady danych osobowych

4

5

Zdjęcia lub nagrania osób

Właściciele kamer monitoringu muszą uważać na przechowywanie nagrań wideo, ponieważ mogą one zawierać dane osobowe. To samo dotyczy nagrań dźwiękowych. Oba powinny być przechowywane tylko za zgodą osób, które są nagrywane.

Cookies: umowy o przekazywaniu danych osobowych firmie

Cookies (ciasteczka) to małe pliki, które strony internetowe wysyłają do Twojego urządzenia, aby zapamiętać pewne informacje o Tobie, np. Twoje preferencje sportowe lub szczegóły dotyczące logowania.

Zgodnie z przepisami RODO, strona internetowa musi uzyskać zgodę użytkownika na zainstalowanie plików cookies na jego urządzeniu.

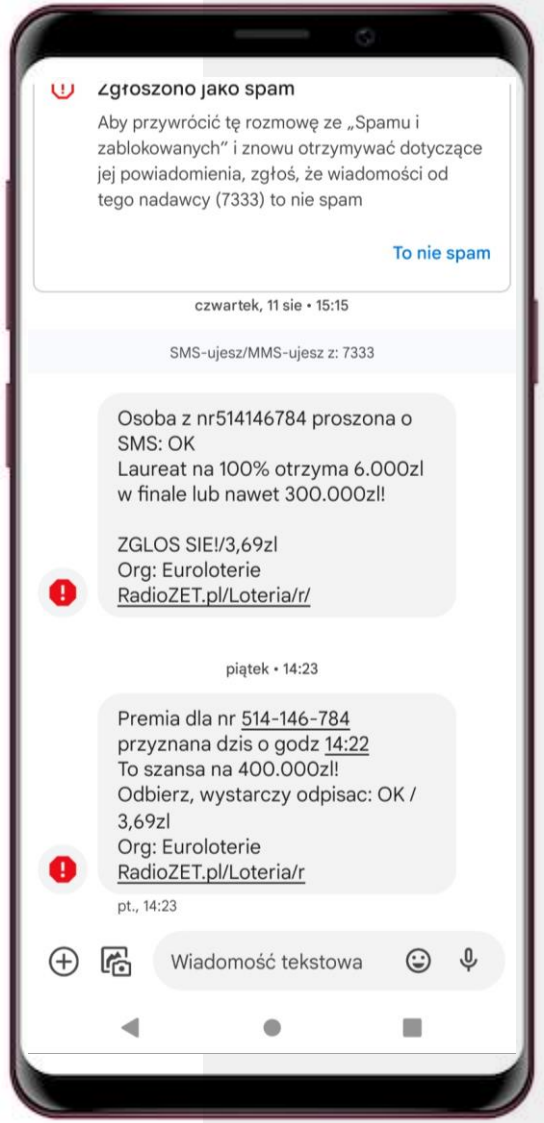
Jeśli obawiasz się, że Twoje dane będą analizowane, możesz wybrać opcję "Odrzuć wszystko" lub „Niezbedne pliki cookie”. Wyłączenie plików cookie oznacza, że strona nie jest spersonalizowana i nie może zapamiętywać szczegółów takich jak hasło lub zakupy.

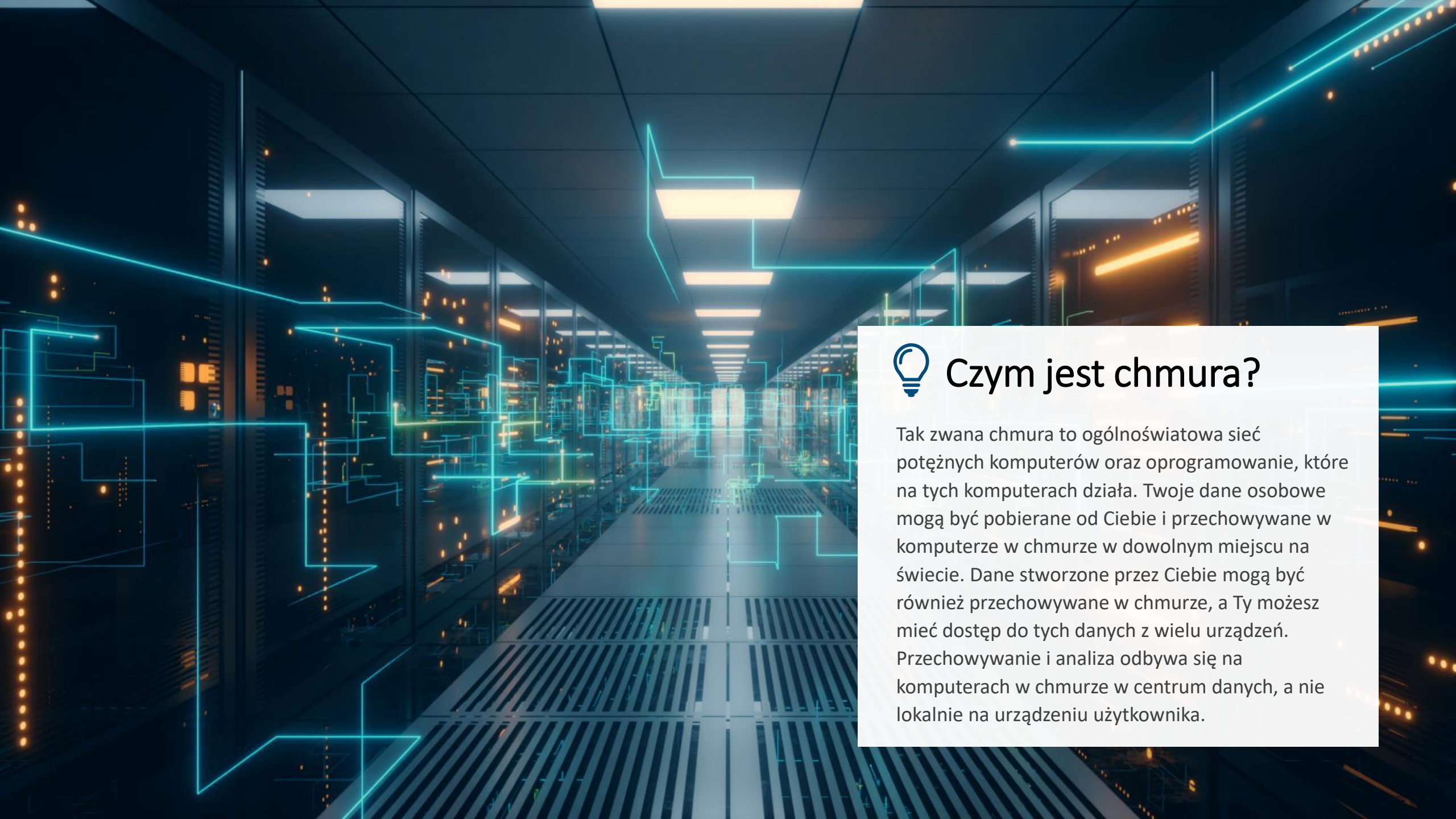
Fałszywe wiadomości - ostrzeżenie!

Czasami na Twoim urządzeniu mobilnym pojawiają się dziwne wiadomości. Kiedy widzisz wiadomość o nagrodzie lub innym zdarzeniu, które wydaje się zbyt dobre, aby było prawdziwe, to zazwyczaj podstęp w celu kradzieży Twoich pieniędzy.

W przypadku otrzymania takiej wiadomości ważne jest, aby **nie** wypełniać formularza, **nie** klikać linku i **nie** udostępniać danych osobowych, takich jak numery telefonów, adresy e-mail lub adres zamieszkania.

Wiadomości otrzymywane przez telefon mogą być fałszywe lub sfabrykowane, to tzw. "fake news„ (fejk njuz).





Czym jest chmura?

Tak zwana chmura to ogólnoświatowa sieć potężnych komputerów oraz oprogramowanie, które na tych komputerach działa. Twoje dane osobowe mogą być pobierane od Ciebie i przechowywane w komputerze w chmurze w dowolnym miejscu na świecie. Dane stworzone przez Ciebie mogą być również przechowywane w chmurze, a Ty możesz mieć dostęp do tych danych z wielu urządzeń. Przechowywanie i analiza odbywa się na komputerach w chmurze w centrum danych, a nie lokalnie na urządzeniu użytkownika.

Chmura jest bardzo przydatna dla urządzeń mobilnych

Problem: pamięć urządzenia jest ograniczona

Większość urządzeń mobilnych ma ograniczoną pamięć i moc obliczeniową. W pewnym momencie przestrzeń dyskowa się kończy, a przetwarzanie danych staje się powolne.

Rozwiązanie: przechowywanie i analiza danych w chmurze

Pliki, zdjęcia, filmy można kopiować do chmury, której dyski są bardzo wydajne. Należy jednak pamiętać, że bezpieczeństwo chmury może być problematyczne.

Bezpieczeństwo w chmurze

Jak bezpieczne są więc dane, gdy opuściły urządzenie mobilne i są przechowywane na komputerze w chmurze?
Dane osobowe w chmurze mogą zostać zhakowane i wykorzystane do celów przestępczych. Bezpieczeństwo chmury jest ważne dla danych osobowych i urządzeń mobilnych. Upewnij się, że Twój dostawca usług przechowywania i przetwarzania danych ma siedzibę w Unii Europejskiej.

Dane w chmurze: gdzie trzymać pliki? Lokalnie czy w chmurze?

Zalety

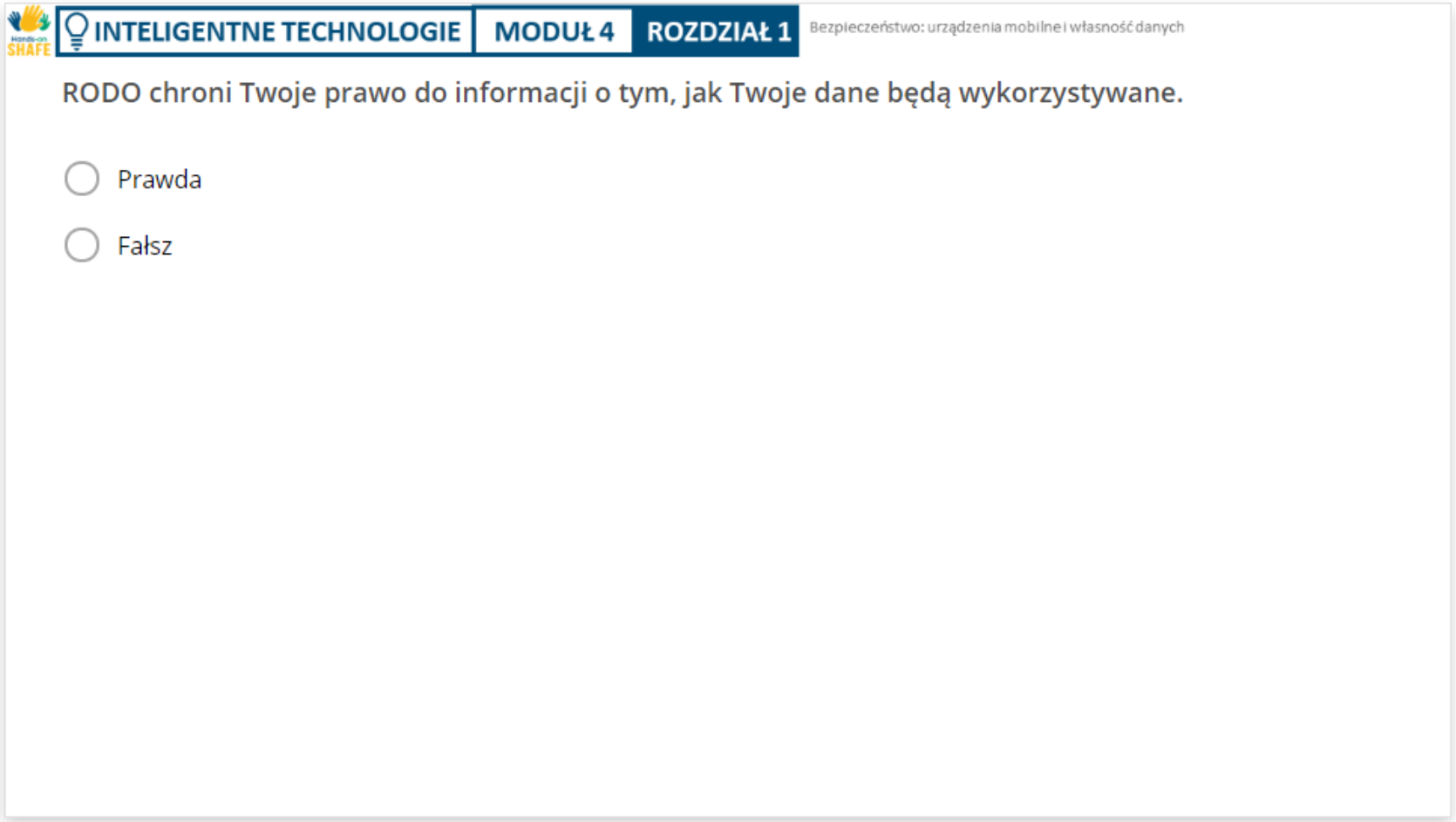
- Personalizacja i lepsza obsługa
- Więcej miejsca na przechowywanie danych, ponieważ urządzenie mobilne ma ograniczoną pamięć
- Więcej danych oznacza lepsze decyzje
- Wszystkie dane wydają się być "w jednym miejscu"

Wady

- Użytkownik godzi się na utratę prywatności danych na rzecz dostawcy chmury
- Możliwość kradzieży i oszustwa
- Gdy dane znajdą się w chmurze, niezwykle trudno jest je usunąć

Quiz

Click the **Quiz** button to edit this object

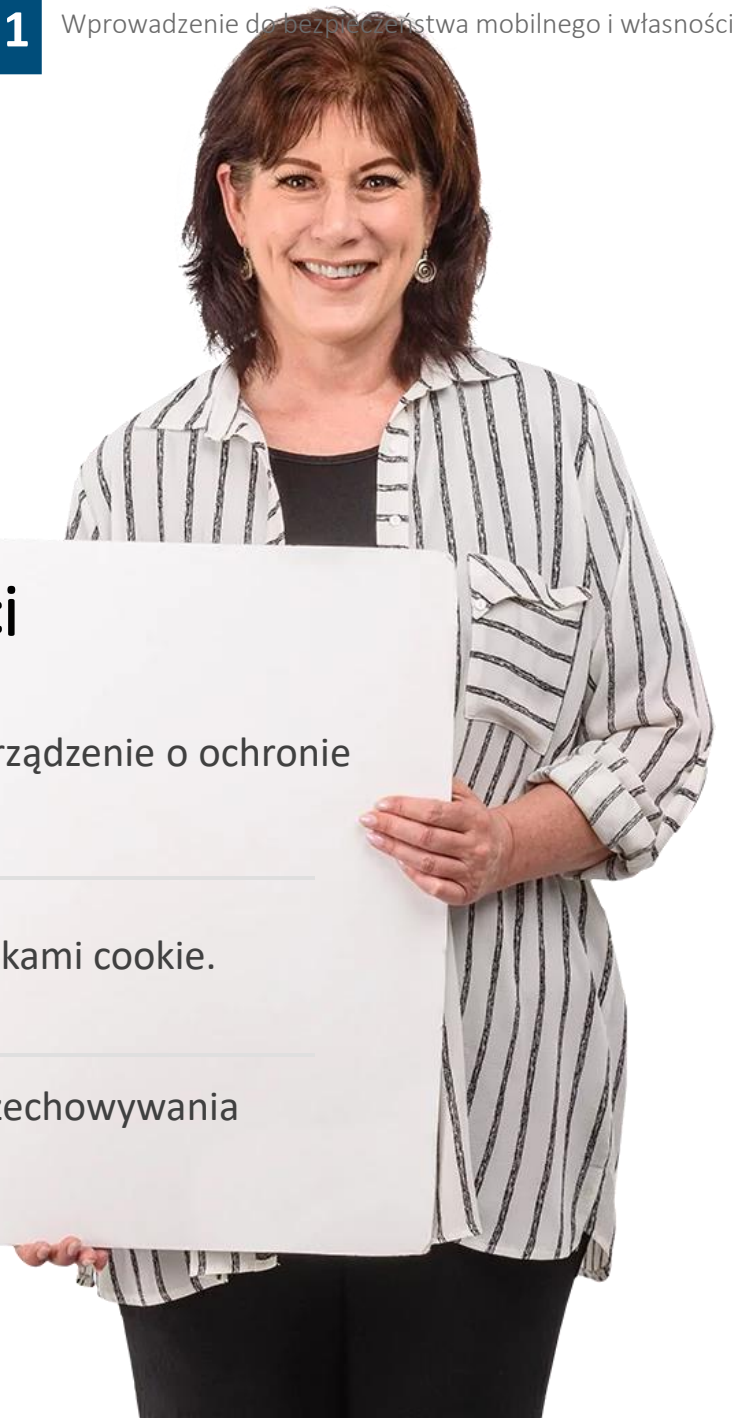


Podsumowanie rozdziału

1. Dowiedziałaś/eś się o prywatność danych.
2. Dowiedziałaś/eś się jak RODO chroni Twoje dane.
3. Dowiedziałaś/eś się o zarządzaniu plikami cookie.
4. Poznałaś/eś zasady działania chmury.
5. Poznałaś/eś, jak Twoje dane są przechowywane w chmurze.
6. Dowiedziałaś/eś się o ochronie prywatności danych mobilnych.

Rozdział zakończony!

Gratulacje! Udało Ci się ukończyć ten rozdział!



Nabyte umiejętności

1. Wiesz czym jest rozporządzenie o ochronie danych osobowych.
2. Wiesz jak zarządzać plikami cookie.
3. Znasz wady i zalety przechowywania danych w chmurze.

Co dalej?

Teraz możesz powtórzyć ten rozdział lub przejść do następnego klikając na jeden z przycisków:

Powtórz

Dalej

INTELIGENTNE TECHNOLOGIE | MODUŁ 4 | ROZDZIAŁ 2

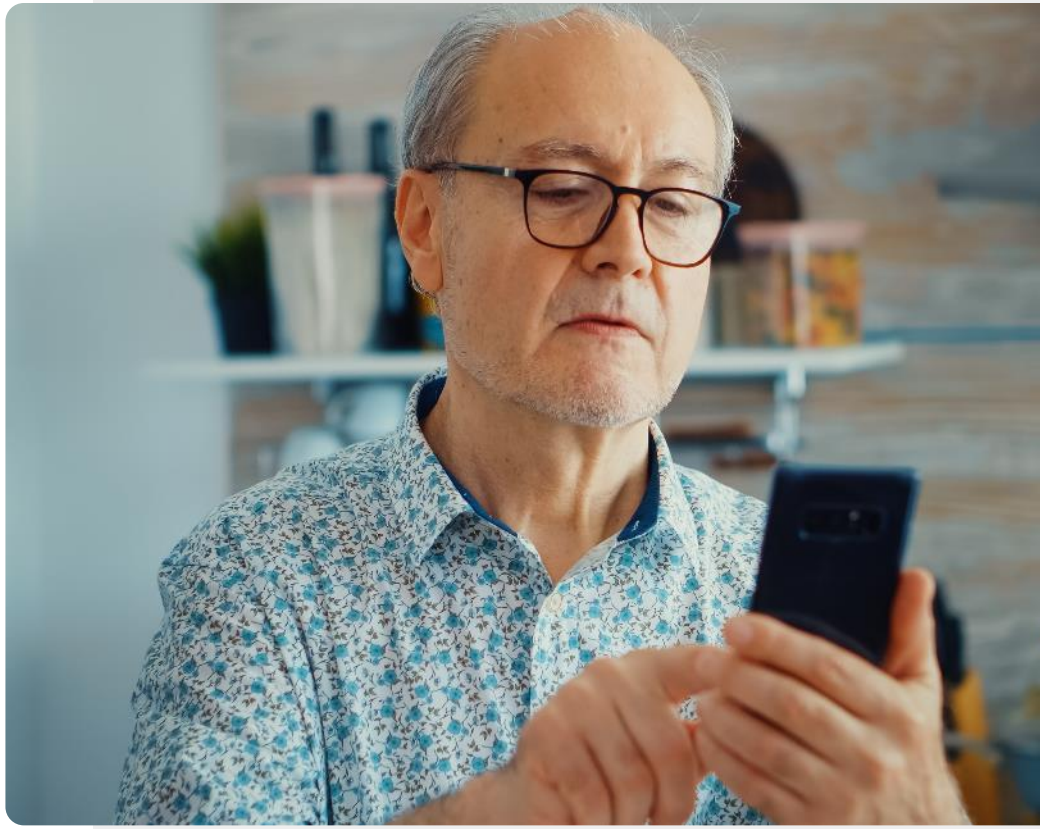
Uwierzytelnianie

W tym rozdziale zapoznasz się procesem uwierzytelniania, czyli rozpoznawania tożsamości użytkownika w celu przyznania mu dostępu do usług. Technologia uwierzytelniania wspiera bezpieczeństwo i ochronę danych osobowych. Poznasz rodzaje uwierzytelniania, w tym biometryczne, a także dowiesz się, jak tworzyć silne hasła.

Uwierzytelnianie - jak urządzenia wiedzą, kim jest aktualny użytkownik

Uwierzytelnianie to procedura rozpoznawania tożsamości użytkownika. Często dzieje się to po otwarciu aplikacji.

Różne systemy wymagają różnych informacji, zwanych **poświadczeniami,** aby potwierdzić tożsamość. Tym poświadczeniem jest często hasło, ale może ono obejmować również inne formy uwierzytelniania.



Czego nauczysz się w tym rozdziale

1. Czym jest uwierzytelnianie i dlaczego jest potrzebne
2. Jakie są rodzaje uwierzytelniania
3. Jak stworzyć silne hasło
4. Jakie są różne rodzaje uwierzytelniania biometrycznego

Rodzaje uwierzytelniania

W ostatnich dekadach gwałtownie wzrosła liczba sposobów uwierzytelniania użytkownika urządzeń mobilnych.

Zapoznajmy się teraz z kilkoma głównymi typami uwierzytelniania, które mogą być dostępne na urządzeniu mobilnym.

Rodzaje uwierzytelniania

1

2

3

Uwierzytelnianie na podstawie hasła

Hasła są prawdopodobnie najbardziej rozpowszechnioną formą uwierzytelniania. Bezpieczne hasła zazwyczaj zawierają litery, cyfry i inne znaki. Temat ten zostanie omówiony w dalszej części tego rozdziału.

Rodzaje uwierzytelniania

1

2

3

Uwierzytelnianie oparte na certyfikatach

Certyfikat cyfrowy to dokument elektroniczny oparty na zasadzie prawa jazdy lub paszportu. Przykładem jest certyfikat cyfrowy, który przedstawia pełne dane dotyczące szczepienia szczepionką COVID-19.

Rodzaje uwierzytelniania

1

2

3

Uwierzytelnianie biometryczne

Uwierzytelnianie biometryczne to procedura bezpieczeństwa, która opiera się na niepowtarzalnych cechach właściciela urządzenia, takich jak twarz, głos lub odciski palców. Za chwilę zobaczymy, że urządzenia mobilne obsługują różne rodzaje sposobów uwierzytelniania biometrycznego.

Rodzaje uwierzytelniania

4

5

Uwierzytelnianie na podstawie tokena

Takie rozwiązanie pozwala użytkownikom wprowadzić dane uwierzytelniające tylko raz i tworzy tajny klucz cyfrowy - token. Użytkownik może użyć tokena, podobnie jak biletu kolejowego, aby uzyskać dostęp do systemów, zamiast ponownie wprowadzać dane uwierzytelniające.

Rodzaje uwierzytelniania

4

5

Uwierzytelnianie wieloczynnikowe (MFA)

Po zidentyfikowaniu użytkownika w jeden sposób, do urządzenia mobilnego wysyłany jest kod, który użytkownik musi wprowadzić w aplikacji lub na stronie internetowej. Jest to **uwierzytelnianie dwuczynnikowe**.

Uwierzytelnianie za pomocą hasła

Wybierzmy kilka z podanych typów uwierzytelniania i przyjrzyjmy się im bliżej.

Prawdopodobnie najpopularniejszym rodzajem uwierzytelniania i tym, który od wielu lat jest stosowany na urządzeniach mobilnych, jest hasło.

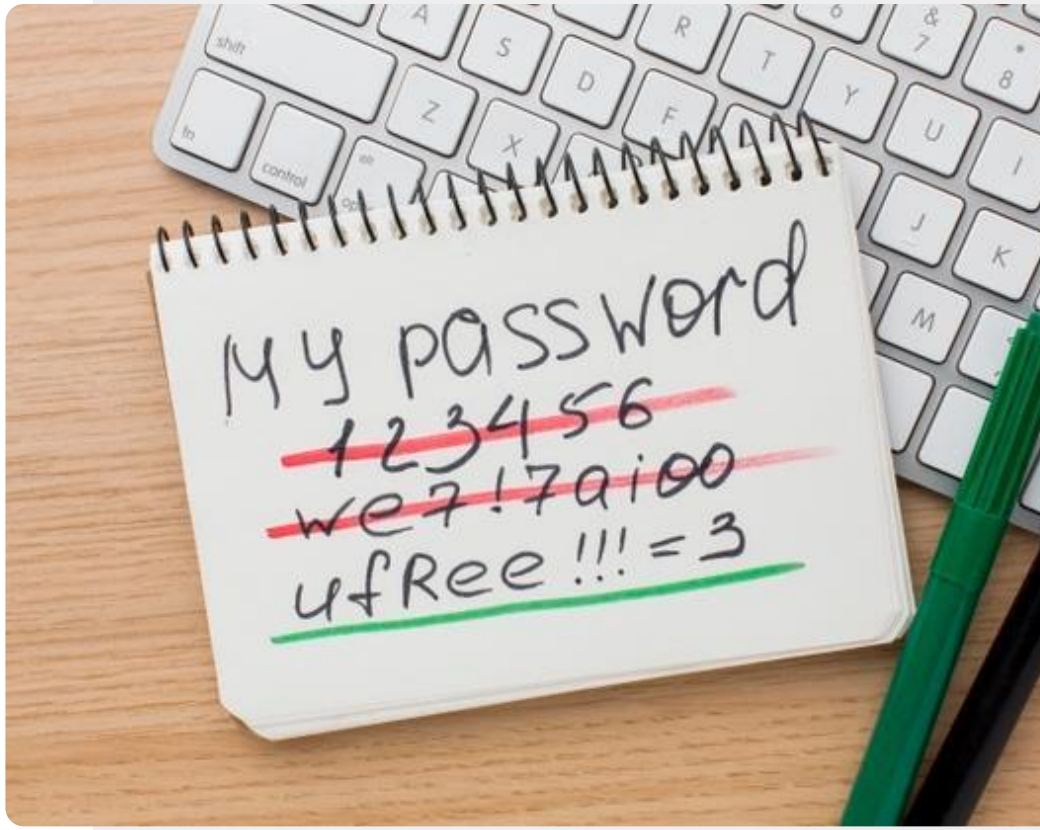
Hasło na zdjęciu jest łatwe do odgadnięcia, więc nie jest zbyt bezpieczne. Czy można zrobić je bezpieczniejsze?

Silne hasła

Wiele stron internetowych wymaga, aby wybrać hasło, które ma kilka z następujących właściwości

- Ma co najmniej 8 znaków
- Zawiera duże i małe litery
- Zawiera liczbę
- Zawiera znak interpunkcyjny

Przyjrzyjmy się teraz, jak przy użyciu tych elementów można stworzyć łatwe do zapamiętania, a przy tym silne hasło.



Tworzenie silnego hasła

1

2

3

Wybierz słowo, które znasz

Wyjmij długopis i kartkę papieru. Zapisz długie słowo lub słowa, które mają dla ciebie duże znaczenie, ale nie byłyby oczywiste dla nikogo innego. Może to być "cierpliwość" lub "Bizancjum" czy "antylopa".

Tworzenie silnego hasła

1

2

3

Zastąp niektóre znaki w słowie lub wyrażeniu

Użyj zamienników znaków, na przykład:

1 = ! e = 3 a = @ 8 = % E =£ I =| S = $ S = 5

K =(T = + G = 6 O = 0 I = 1 Z = 2 B = 8

Na przykład **Karolina** mogłaby zostać **(@ro|1n@**

Tworzenie silnego hasła

1

2

3

Używanie hasła do urządzenia lub strony internetowej

Teraz dokładnie zniszcz hasło zapisane na papierze lub umieść je w bardzo bezpiecznym miejscu, np. w sejfie.

Teraz możesz wprowadzić nowe silne hasło do urządzenia lub strony internetowej.

Chroń swoje hasło

Po utworzeniu hasła należy je zabezpieczyć.

Najlepiej jest spróbować po prostu je zapamiętać. Jeśli zdecydujesz się je zapisać, powinno być przechowywane w bardzo bezpiecznym miejscu.

NIGDY nie należy przechowywać hasła w telefonie lub w jego pobliżu.

Wykonaj zadanie!

Antonio chce stworzyć bezpieczne hasło. Jak powinien to zrobić?

✓Poznaj António. Informacje o António można znaleźć tutaj.

✓ António wybiera frazę **brakbarier** jako podstawowe słowo dla swojego hasła.

✓Zastąp niektóre znaki we frazie według wcześniejszego opisu.

Hasła do telefonów i kody SIM

Urządzenia mobilne można skonfigurować za pomocą **haseł w** celu ochrony plików. **Karty SIM** w urządzeniu łączą je z siecią telefoniczną i są wyposażone w **kod PIN,** który wprowadza się, aby uzyskać dostęp do sieci. Umożliwiają one dostęp do kontaktów znajdujących się na karcie SIM, a w przypadku kradzieży urządzenia, kartę SIM można przenieść na inne urządzenie.

Jeśli kod PIN zostanie wprowadzony niepoprawnie 3 razy, potrzebny jest drugi kod zwany kodem **PUK.** Z tego powodu ważne jest, aby przechowywać kod PIN i kod PUK w bezpiecznym miejscu po otrzymaniu ich z urządzeniem lub kartą SIM.

Uwierzytelnianie biometryczne

Dowiedziałeś się, że system uwierzytelniania biometrycznego rozpoznaje niepowtarzalne cechy użytkownika urządzenia, aby umożliwić mu dostęp do urządzenia lub systemu.

Dokonajmy teraz przeglądu różnych rodzajów uwierzytelniania biometrycznego.

Uwierzytelnianie biometryczne

1

2

3

Skanery linii papilarnych

Odciski palców są niepowtarzalne, więc mogą być wykorzystywane do identyfikacji użytkownika. Wiele nowoczesnych urządzeń mobilnych ma wbudowane skanery linii papilarnych, a telefon może być odblokowany poprzez umieszczenie palca nad skanerem linii papilarnych.

Uwierzytelnianie biometryczne

1

2

3

Skanowanie siatkówki

Podobnie jak odciski palców, wzory w oku są niepowtarzalne u każdego. Kamera w niektórych urządzeniach mobilnych potrafi rozpoznać wzór siatkówki oka właściciela i wykorzystać go do odblokowania urządzenia.

Uwierzytelnianie biometryczne

1

2

3

Rozpoznawanie twarzy

Innym podobnym podejściem do uwierzytelniania użytkownika jest skanowanie twarzy. Również w tym przypadku kamera jest wykorzystywana do rozpoznawania niepowtarzalnych cech twarzy właściciela urządzenia w celu jego odblokowania.

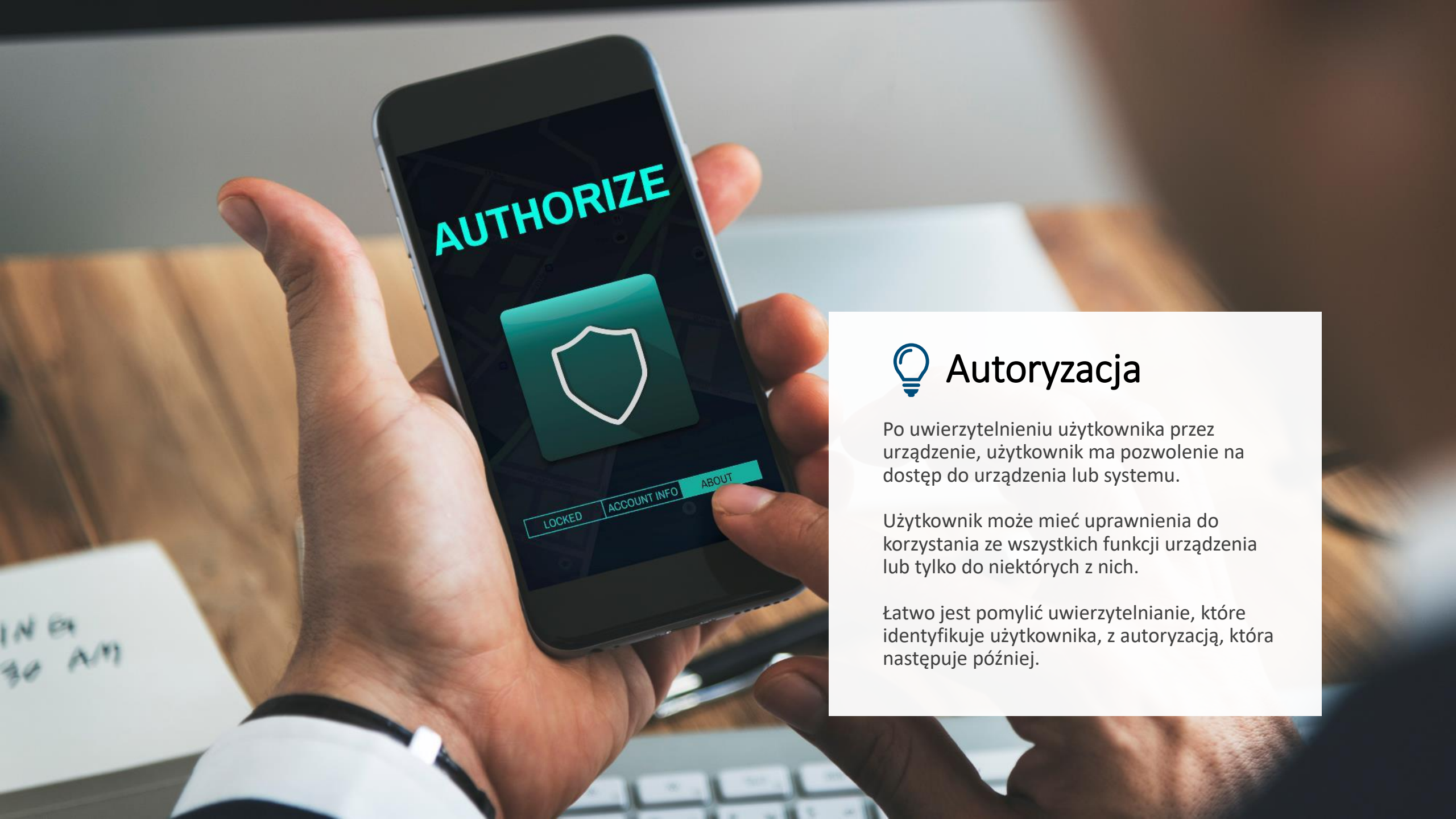
Wykonaj zadanie!

Tom chce używać uwierzytelniania w swoim telefonie. Czy możesz pomóc mu wybrać odpowiedni sposób?

✓Poznaj Toma. Informacje o Tomie możesz znaleźć tutaj.

✓ Tom pracował kiedyś w firmie informatycznej, więc jest doświadczonym użytkownikiem technologii, ale nie jest zaznajomiony z nowoczesnymi metodami uwierzytelniania. Chciałby zabezpieczyć swój smartfon, aby inne osoby nie miały dostępu do jego informacji.

✓Na podstawie informacji zawartych na poprzednich slajdach, udziel Tomowi porady, jakie sposoby uwierzytelniania mógłby zastosować.



Autoryzacja

Po uwierzytelnieniu użytkownika przez urządzenie, użytkownik ma pozwolenie na dostęp do urządzenia lub systemu.

Użytkownik może mieć uprawnienia do korzystania ze wszystkich funkcji urządzenia lub tylko do niektórych z nich.

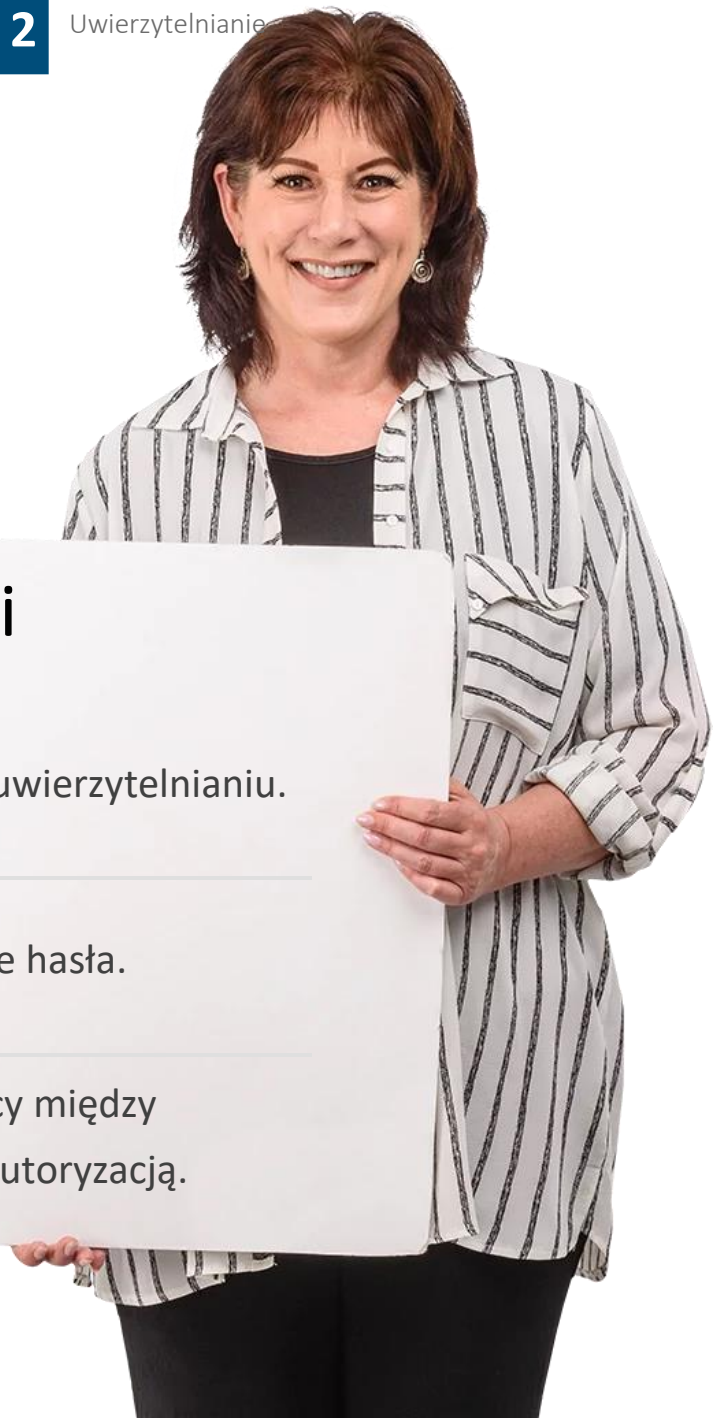
Łatwo jest pomylić uwierzytelnianie, które identyfikuje użytkownika, z autoryzacją, która następuje później.

Podsumowanie rozdziału

1. Dowiedziałaś/eś się o uwierzytelnianiu i jak jest ono wykorzystywane do ochrony dostępu i informacji.
2. Poznałaś/eś wiele rodzajów uwierzytelniania.
3. Nauczyłaś/eś się jak tworzyć i zapamiętywać hasła.
4. Postaraj się wykorzystać możliwe zabezpieczenia swojego urządzenia mobilnego. One go ochronią.
5. Mamy nadzieję, że będziesz ćwiczyć technikę tworzenia haseł, aby tworzyć bezpieczne hasła.

Rozdział zakończony!

Gratulacje! Udało Ci się ukończyć ten rozdział!



Nabyte umiejętności

1. Dowiedziałaś/eś się o uwierzytelnianiu.
2. Wiesz, jak tworzyć silne hasła.
3. Nauczyłaś/eś się różnicy między uwierzytelnianiem, a autoryzacją.

Co dalej?

Teraz możesz powtórzyć ten rozdział lub przejść do kolejnego rozdziału korzystając z przycisków:

Powtórz

Dalej

INTELIGENTNE TECHNOLOGIE | MODUŁ 4 | ROZDZIAŁ 3

Ochrona urządzenia mobilnego

W świecie fizycznym Twoje rzeczy, w tym urządzenie mobilne, może zostać skradzione. W świecie cyfrowym Twoje urządzenie jest również narażone na ataki hakerskie i wirusy. Ten rozdział dotyczy tego, jak chronić swój smartfon, prywatność i informacje przed cyberatakami, takimi jak wirusy.

Czego nauczysz się w tym rozdziale

1. Jak chronić swoje urządzenia przed nieautoryzowanym dostępem.
2. Jak chronić swoje urządzenia przed wirusami.
3. O ransomware, malware (złośliwe oprogramowanie) i DDoS.
4. Jak bezpiecznie korzystać z hot spotów.

Ochrona urządzenia mobilnego przed nieuprawionym dostępem

1

2

3

Zabezpiecz swoje urządzenie mobilne

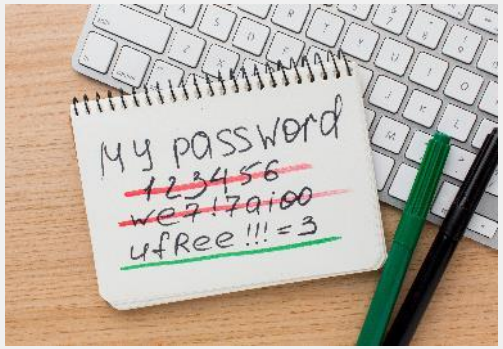
Zabezpiecz swoje urządzenie mobilne za pomocą haseł lub jeszcze lepiej, włączonym uwierzytelnianiem biometrycznym. Zablokuj kartę SIM za pomocą kodu PIN i przechowuj kody PIN i PUK w łatwym do zapamiętania, ale bezpiecznym miejscu.

Ochrona urządzenia mobilnego przed nieuprawionym dostępem

1

2

3



Używaj silnych haseł

W poprzednim rozdziale nauczyłeś się tworzyć i używać silnych haseł, z dużymi i małymi literami, cyframi i znakami specjalnymi. Warto usiąść z długopisem i papierem by stworzyć takie hasło.

Ochrona urządzenia mobilnego przed nieuprawionym dostępem

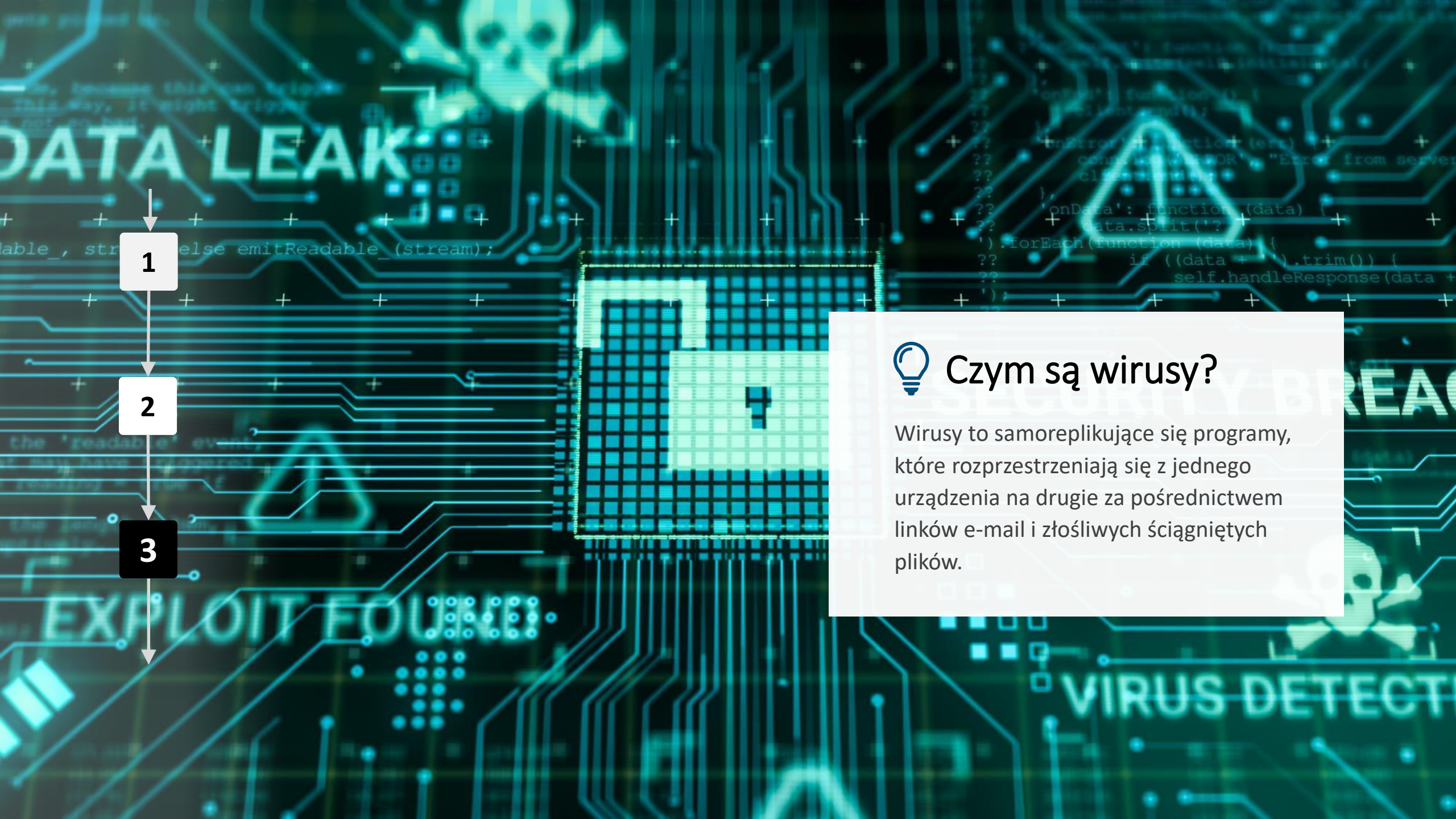
1

2

3

Uważaj na pobierane pliki

Pobieraj pliki, takie jak dokumenty, filmy, muzyka lub obrazy, tylko z zaufanych witryn, takich jak producenci urządzeń, duże firmy produkujące oprogramowanie lub firmy medialne. Niektóre pliki pobierane z niezaufanych stron mogą zawierać wirusy i uszkodzić Twój sprzęt. Witryny z adresami zaczynającymi się od **https** chronią przed tym.



Czym są wirusy?

Wirusy to samoreplikujące się programy, które rozprzestrzeniają się z jednego urządzenia na drugie za pośrednictwem linków e-mail i złośliwych ściągniętych plików.

Ochrona urządzenia mobilnego przed nieuprawionym dostępem

4

5

6

Aktualizuj urządzenie

Producent urządzeń mobilnych będzie wysyłał powiadomienia o nowych aktualizacjach oprogramowania. Aktualizacje pomagają chronić urządzenie przed lukami w zabezpieczeniach, które mogłyby umożliwić komuś przejęcie danych z urządzenia. Pobierz aktualizację oprogramowania na urządzenie i przeprowadź jego aktualizację.

Ochrona urządzenia mobilnego przed nieuprawionym dostępem

4

5

6

Szyfruj dane na urządzeniu mobilnym

Większość urządzeń mobilnych posiada opcję szyfrowania danych. Jeśli telefon zostanie skradziony, szyfrowanie utrudni osobie nieuprawnionej wgląd w dane przechowywane na urządzeniu. Uprawniony użytkownik będzie mógł korzystać z urządzenia w normalny sposób.

Czym jest szyfrowanie?

Szyfrowanie to metoda, dzięki której informacje są przekształcane w nieczytelne kody, które ukrywają ich prawdziwe znaczenie, z wyjątkiem dla użytkownika posiadającego klucz.

Należąca do Facebooka aplikacja społecznościowa WhatsApp posiada szyfrowanie end-to-end, dzięki czemu komunikacja między dwoma użytkownikami nie może być "podsłuchana" przez inną osobę.

Ochrona urządzenia mobilnego przed nieuprawionym dostępem

4

5

6

Uważaj na publiczne sieci Wi-Fi

Wi-Fi w miejscach publicznych, takich jak lotniska i kawiarnie, może być niebezpieczne. Czasami to, co uważasz za Wi-Fi kawiarni, jest w rzeczywistości laptopem hakera, który może wykorzystać połączenie z Twoim telefonem do niewłaściwych celów. Jeśli masz wątpliwości, nie łącz się!

Wi-Fi, a przestępczość

Cyberprzestępcy czasami szpiegują publiczne sieci Wi-Fi i zbierają dane, które są przesyłane przez Wi-Fi.

W ten sposób przestępca może zdobyć dane bankowe, hasła i inne wrażliwe informacje.

Czy korzystać z publicznego Wi-Fi czy nie?

Zalety

- Brak opłat
- Brak limitu danych komórkowych
- Łatwe podłączenie
- Dostępność

Wady

- Brak bezpieczeństwa
- Wi-Fi z "hot spotu" organizacji może być sfałszowane
- Zazwyczaj mniejsza prędkość niż w Internecie z własnej komórki

Czym jest atak hakerski?

Zadaniem ataku hakerskiego jest uzyskanie dostępu w celu dokonania złośliwości (różnego typu), kradzieży danych lub zniszczenia danych organizacji.

Malware, Ransomware, DDos

Malware - złośliwe oprogramowanie jest to każde oprogramowanie celowo zaprojektowane w celu wyrządzenia szkody komputerowi, serwerowi, klientowi lub sieci komputerowej. Natomiast oprogramowanie, które powoduje niezamierzone szkody z powodu jakiegoś niedociągnięcia, jest zwykle określane jako błąd w oprogramowaniu. Istnieje wiele różnych typów złośliwego oprogramowania, w tym wirusy komputerowe, robaki, konie trojańskie, ransomware, spyware, adware, wiper i scareware

(Więcej informacji : https://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie)

Ransomware to rodzaj złośliwego oprogramowania, które uniemożliwia użytkownikowi dostęp do wielu plików na jego komputerze. Zwykle jest pobierane za pośrednictwem linku w wiadomości e-mail, na stronie internetowej lub w mediach społecznościowych. Po pobraniu szyfruje wszystkie pliki danych na komputerze, a następnie pojawia się ekran blokujący, żądający zapłacenia okupu, aby umożliwić uwolnienie plików. **NIE** klikaj linków w podejrzanych tekstach lub e-mailach!

(Więcej informacji : https://pl.wikipedia.org/wiki/Ransomware)

Łagodzenie **ataku na system komputerowy** odnosi się do procesu skutecznej ochrony docelowego serwera lub sieci przed atakiem typu **distributed denial-of-service** (**DDoS**). Atak DDoS polega na przeprowadzeniu ataku równocześnie z wielu miejsc (z wielu komputerów). Wykorzystując specjalnie zaprojektowany sprzęt sieciowy lub usługę ochrony w chmurze, użytkownik jest w stanie zmniejszyć nadchodzące zagrożenie.

(Więcej informacji: https://pl.wikipedia.org/wiki/DDoS)

Wykonaj zadanie!

Tom dodał uwierzytelnianie do swojego telefonu. Czy możesz zaproponować inne sposoby ochrony jego danych osobowych?

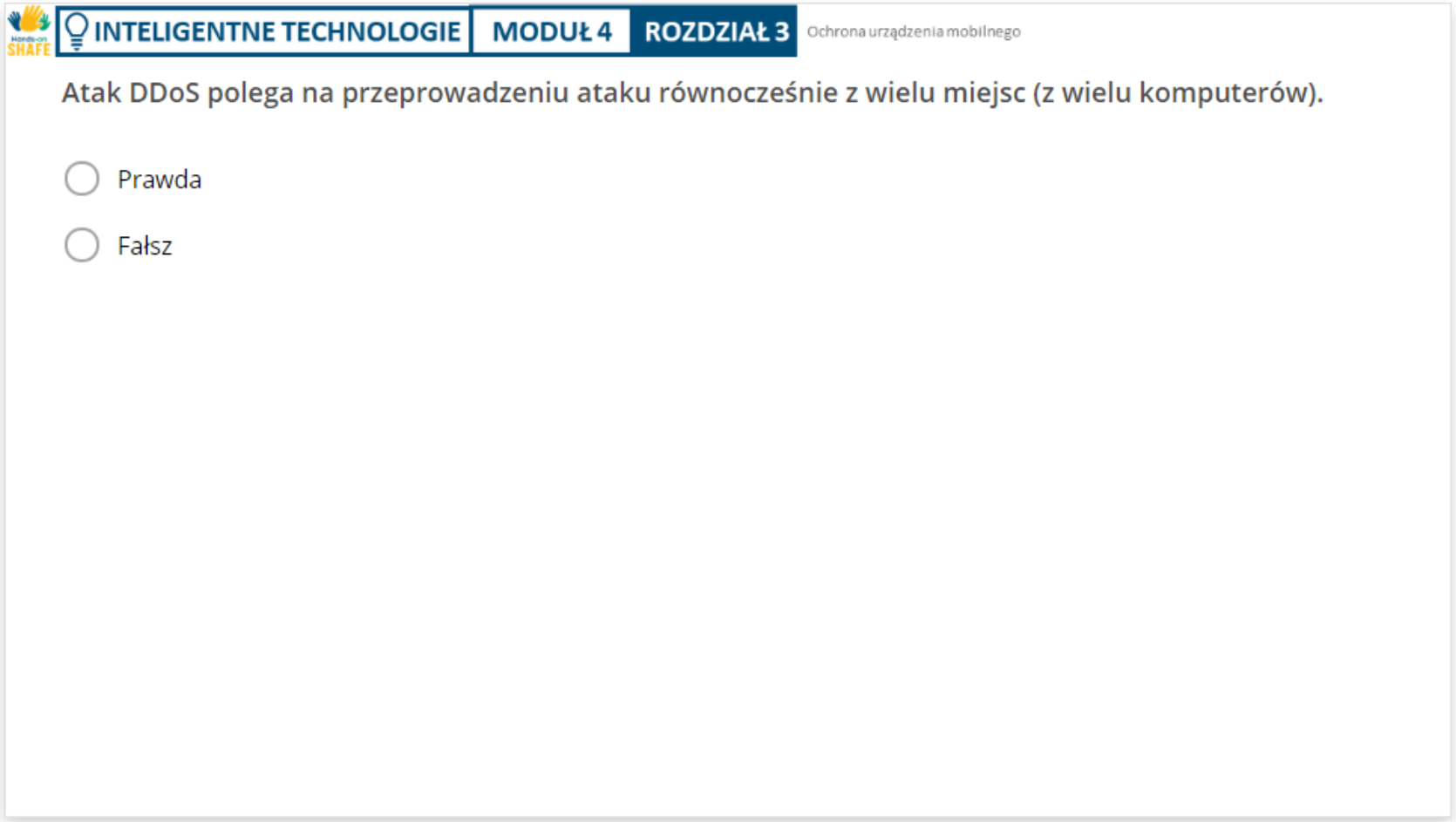
✓Poznaj Toma. Informacje o Tomie możesz znaleźć tutaj.

✓ Tom pracował kiedyś w firmie informatycznej, więc jest doświadczonym użytkownikiem technologii, ale nie jest zaznajomiony z nowoczesnymi metodami uwierzytelniania. Chciałby zabezpieczyć swój smartfon, aby inne osoby nie miały dostępu do jego informacji.

✓Na podstawie informacji, które poznałeś na poprzednich slajdach zaproponuj inne działania, które Tom może podjąć, aby chronić swoje dane.

Quiz

Click the **Quiz** button to edit this object

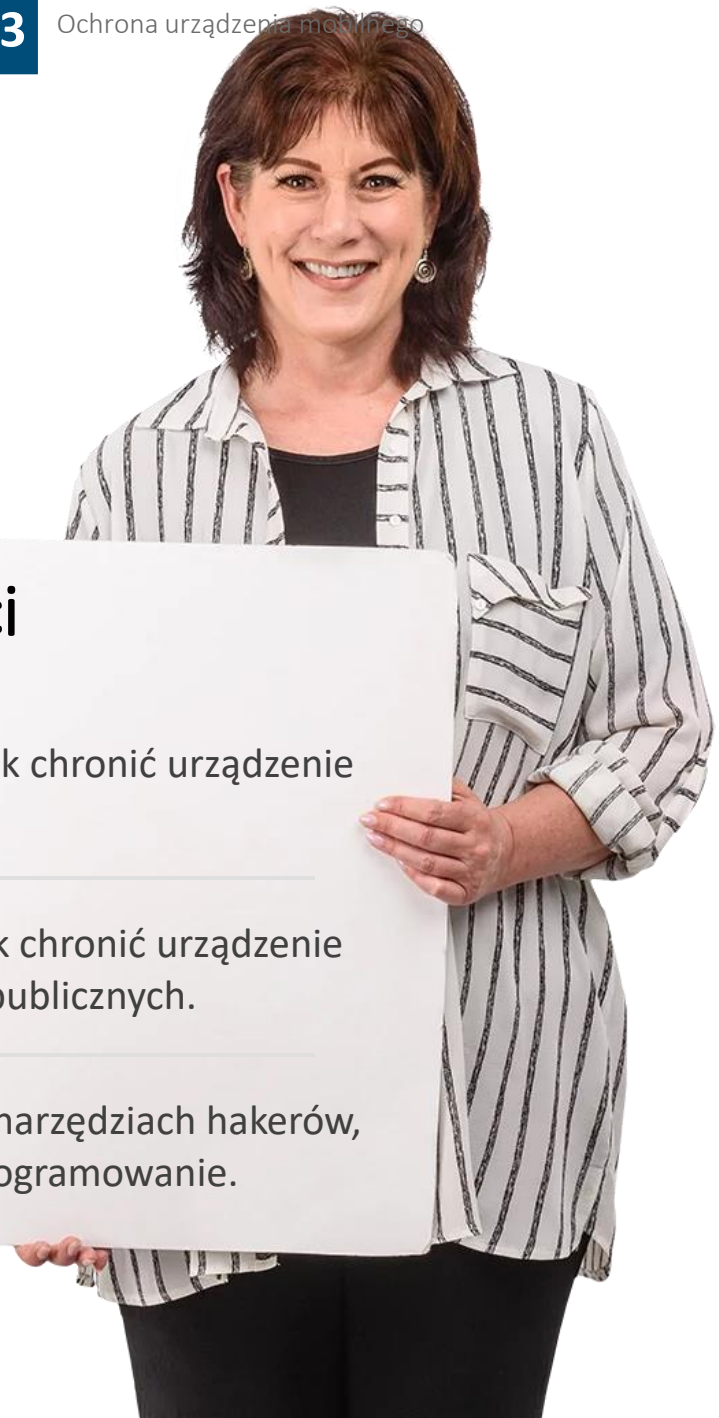


Podsumowanie rozdziału

1. Dowiedziałaś/eś się, jak chronić urządzenie mobilne.
2. Poznałaś/eś różnicę między wirusami, a atakami hakerskimi.
3. Dowiedziałaś/eś się o ransomware, malware i DDoS.
4. Jesteś świadoma/y zagrożeń wynikających z korzystania z publicznych sieci Wi-Fi.

Rozdział zakończony!

Gratulacje! Udało Ci się ukończyć ten rozdział!



Nabyte umiejętności

1. Dowiedziałaś/eś się, jak chronić urządzenie mobilne.
2. Dowiedziałaś/eś się jak chronić urządzenie mobilne w miejscach publicznych.
3. Dowiedziałaś/eś się o narzędziach hakerów, takich jak złośliwe oprogramowanie.

Co dalej?

Teraz możesz powtórzyć ten rozdział lub przejść do następnego klikając na jeden z przycisków:

Powtórz

Dalej

INTELIGENTNE TECHNOLOGIE | MODUŁ 4 | ROZDZIAŁ 4

Cyberprzemoc i radzenie sobie z nieodpowiednimi treściami

Co powinieneś zrobić, jeśli staniesz się celem cyberprzemocy? Jeśli nie widzimy osoby, łatwiej jest nie zdawać sobie sprawy ze szkód, jakie wyrządza cyberprzemoc. W tym rozdziale dokonamy przeglądu zagadnień związanych z komunikacją cyfrową oraz tego, co jest właściwe, a czego nie należy udostępniać online.

Czego nauczysz się w tym rozdziale

1. Dowiesz się o zjawisku cyberprzemocy.
2. Jak radzić sobie z nieodpowiednimi treściami.
3. Co udostępniać w sieci, a czego nie.
4. Znajomi online: czy to bezpieczne?

Czym jest cyberprzemoc?

Cyberprzemoc definiowana jest jako ***agresywne umyślne działanie prowadzone przez grupę lub osobę, przy użyciu elektronicznych form kontaktu, wielokrotnie i przez dłuższy czas przeciw ofierze, która nie może się skutecznie bronić. - Smith 2018 r.***

Zazwyczaj mówi się, że cyberprzemoc obejmuje trzy elementy:

1. zamiar szkodzenia,
2. nierównowaga sił,
3. powtórzenie czynu.

Rodzaje cyberprzemocy

Cyberprzemoc może odbywać się poprzez wiadomości tekstowe, rozmowy telefoniczne, e-maile, komunikatory, platformy mediów społecznościowych lub na czacie.

Może ona przybrać formę raniących słów, obraźliwych komentarzy, umieszczania fałszywych informacji na publicznych forach lub blogach, włamywania się na konta w celu osobistego grożenia przemocą lub mieć tło seksualne.

- Rao 2018 r.

Jak sobie radzić z cyberprzemocą

Według ekspertów istnieje kilka sposobów na radzenie sobie z cyberprzemocą.

Ignoruj: Jeśli to możliwe, ignoruj i odcinaj się od dręczyciela.

Zapisuj: Notuj czas, datę i treść wszystkich wiadomości związanych z nękaniem, aby w razie potrzeby móc je zgłosić.

Wsparcie przyjaciół: podziel się swoim doświadczeniem z przyjaciółmi i krewnymi, abyś nie czuł się odizolowany.

Zgłoś: Skontaktuj się z moderatorem strony lub forum.

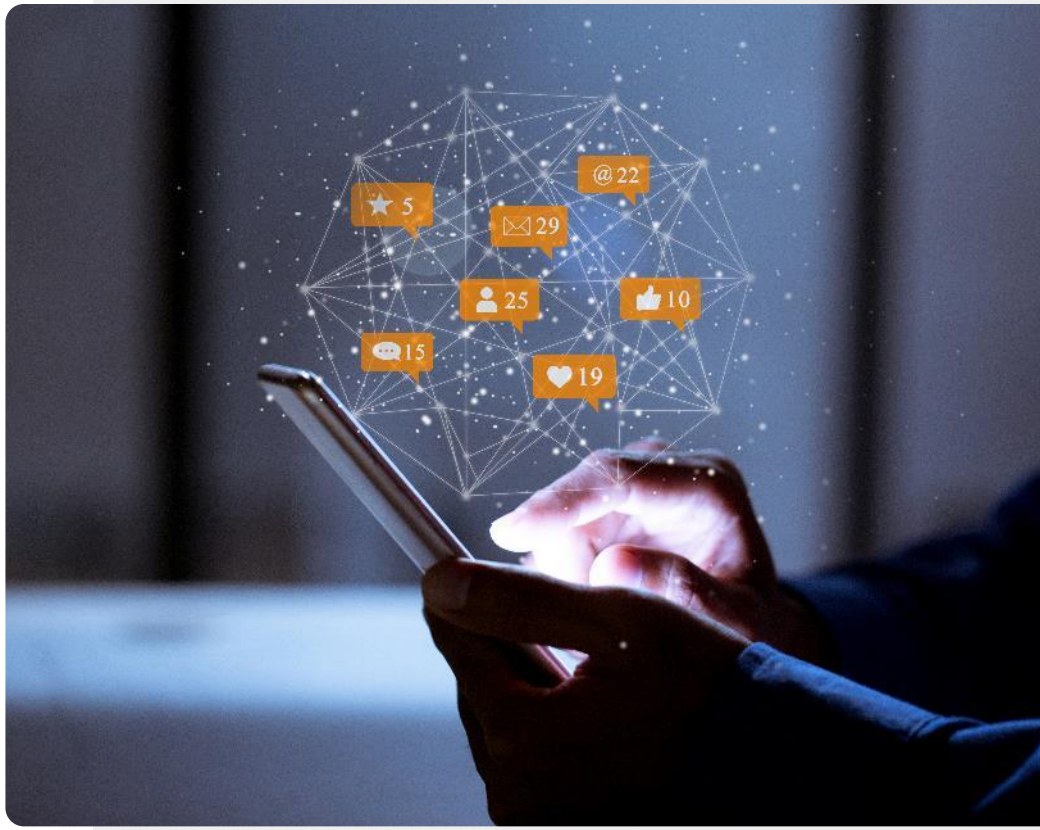
Udostępnianie danych osobowych na portalach społecznościowych

Kiedy udostępniasz informacje w mediach społecznościowych, powinieneś założyć, że będą one tam przez długi czas. Zastanów się, czy Twój post nie spowoduje problemów.

"Chociaż może się wydawać, że informacje są udostępniane tylko znajomym i rodzinie, mogą być również udostępniane hakerom i oszustom, którzy trollują strony mediów społecznościowych".

"Kiedy twoje dane znajdą się na wolności mogą być wykorzystane przez dowolną liczbę pozbawionych skrupułów postaci".

Joseph Turow - Penn State



Gdzie zgłosić cyberprzemoc

Twój dostawca usług lub sieć mediów społecznościowych może pomóc Ci w zablokowaniu niechcianych wiadomości i połączeń.

Jeśli sytuacja jest poważniejsza zgłoś sprawę na policję aby zbadała komunikaty o groźbach.

Usuwanie tożsamości online

W aplikacjach społecznościowych często można zmienić swój profil, tak aby nie był on widoczny dla ogółu.

Nie zawsze możliwe jest usunięcie swoich postów w mediach społecznościowych czy na forum internetowym, ale można usunąć swoją tożsamość, dzięki czemu posty stają się anonimowe.

W niektórych przypadkach możesz wysłać prośbę do **wyszukiwarki,** takiej jak Google, aby Twoje dane nie pojawiały się w wynikach wyszukiwania.

Czy zostałeś oszukany?

Jeśli ktoś uzyska dostęp do Twojego konta e-mail lub konta w mediach społecznościowych, może wykorzystać je do wysyłania fałszywych e-maili do Twoich kontaktów bądź powodowania innych problemów. Nazywa się to pwning (wymawa: połning).

Jeśli używasz tego samego hasła do różnych kont mailowych, to Twoje konto może zostać zhakowane.

Ostrożnie wybieraj internetowych przyjaciół

Wybór przyjaciół online: sprawdź informacje, które otrzymałeś od "nowych" przyjaciół.

Nie udostępniaj swoich danych osobowych, prowadź neutralne rozmowy.

Nie pożyczaj pieniędzy żadnemu "nowemu" znajomemu.

Prawdziwy przyjaciel będzie chciał poznać Twoje zainteresowania, a nie wykorzystywać Cię do rozwiązywania swoich problemów.

Zawieranie nowych znajomości w sieci

Zalety

- Możesz połączyć się z ludźmi na całym świecie.
- W sieci możesz odkryć o wiele więcej znajomych, niż w lokalnej społeczności, którzy podzielają Twoje zainteresowania.
- Czaty online mogą być wygodniejsze niż spotkania bezpośrednie.
- Możesz zamknąć okno czatu, jeśli coś pójdzie nie tak.

Wady

- Być może wolisz komunikację osobistą, odległość może być problemem.
- Trzeba uważać, aby nie ujawniać danych osobowych nieznajomym. Ich identyfikator może być fałszywy.
- Ludziom łatwiej jest obrażać innych w sieci, gdy nikt ich nie widzi.

Czym jest nieodpowiednia treść?

Nieodpowiednie treści obejmują materiały filmowe o "*atakach terrorystycznych, egzekucjach i bombardowaniach; okrucieństwie wobec ludzi i zwierząt; strony poświęcone samookaleczeniom; treści związane z anoreksją i zaburzeniami odżywiania; treści związane z samobójstwami; wykorzystywaniem seksualnym i gwałtami; przemocą; strony pełne nienawiści; porno online".*

W slangu internetowym osoba, która zamieszcza nieodpowiednie treści z zamiarem sprowokowania lub obrażenia innych czytelników, nazywana jest **trollem.**

Radzenie sobie z nieodpowiednimi treściami

Większość dostawców usług wyszukiwania ma funkcje wspierające radzenie sobie z nieodpowiednimi treściami. Na przykład SafeSearch firmy Google znajduje się pod adresem https://www.google.com/preferences.

Otwórz tę stronę i kliknij ikonę znajdującą się obok "Włącz filtr SafeSearch”.

Można też wybrać blokadę SafeSearch, wówczas Google będzie blokować zarówno teksty na stronach dla dorosłych, jak i obrazy związane z tymi stronami.

Wykonaj zadanie!

Teresa jest zdenerwowana incydentem związanym z cyberprzemocą. Czy możesz jej pomóc?

✓Poznaj Teresę. Informacje o Teresie można znaleźć tutaj.

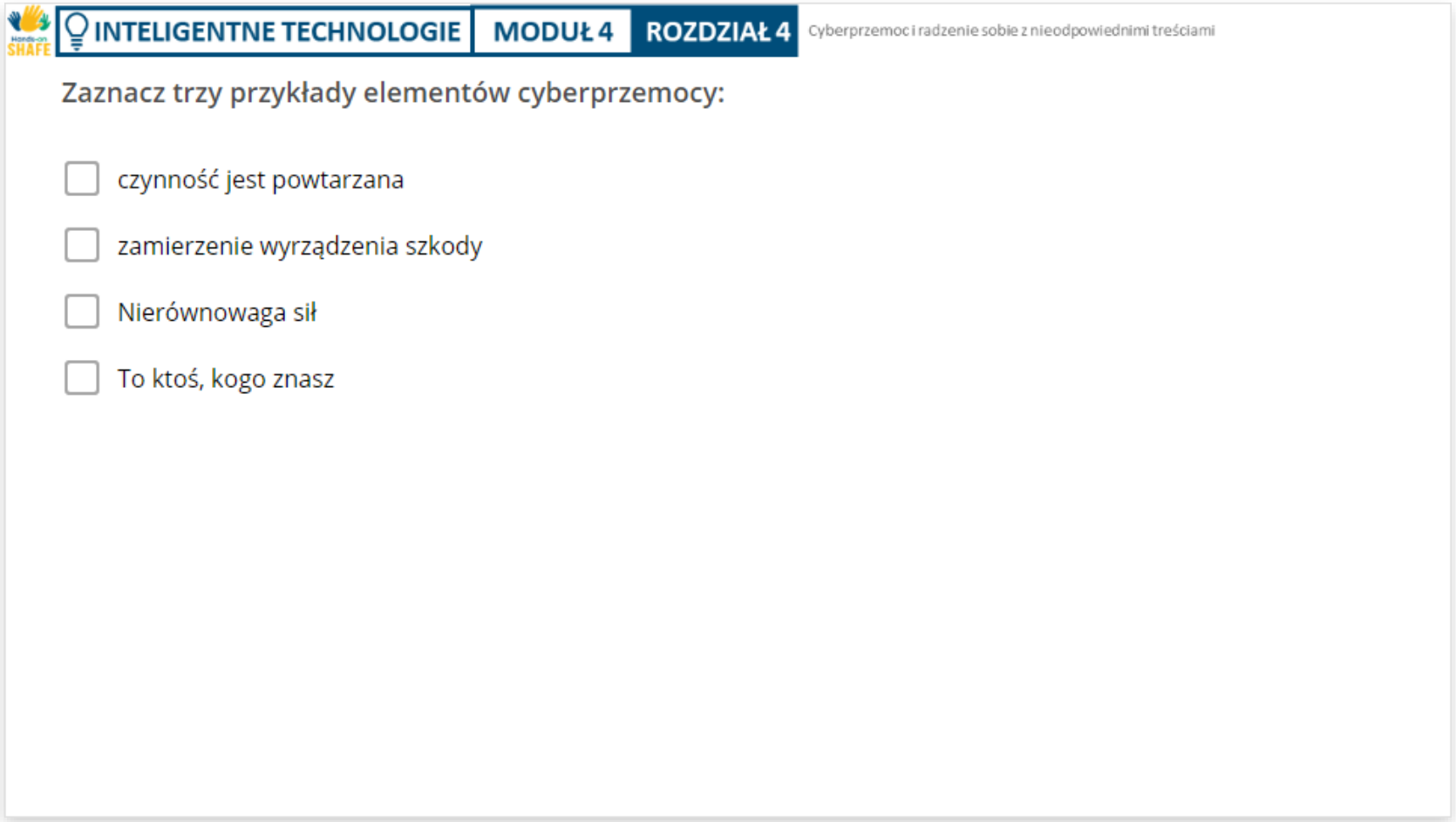
✓ Teresa używa technologii do utrzymywania kontaktu ze swoimi przyjaciółmi, ale ostatnio spotkało ją nieprzyjemne zdarzenie związane z cyberprzemocą. Jak na razie nie jest to poważny przypadek, ale mimo to chciałaby wiedzieć, jak sobie z nim poradzić w przyszłości, jeśli będzie się powtarzał.

✓Na podstawie informacji, które poznałeś na poprzednich slajdach, przedstaw Teresie rady dotyczące postępowania w przypadku cyberprzemocy.

✓Z kim powinna skontaktować się Teresa, jeśli ataki cyberprzemocy staną się poważniejsze?

Quiz

Click the **Quiz** button to edit this object

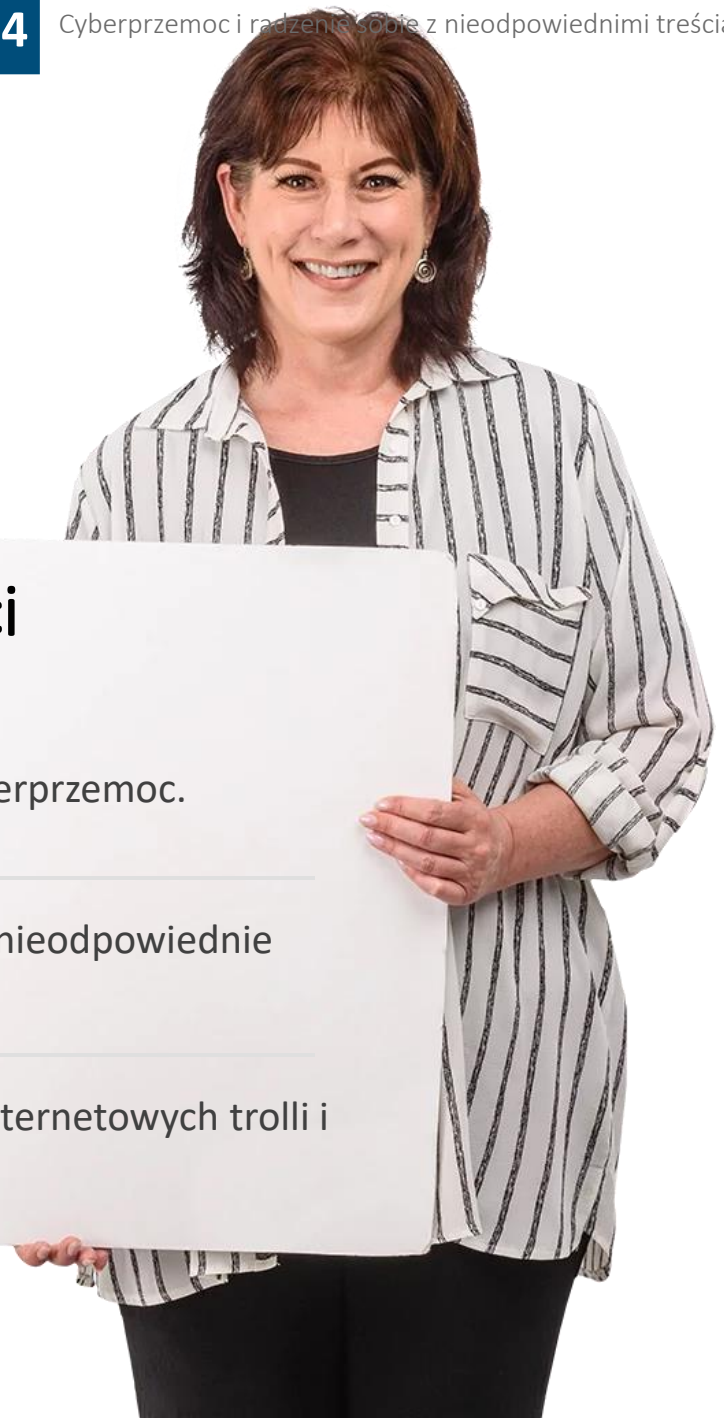


Podsumowanie rozdziału

1. Dowiedziałaś/eś się o cyberprzemocy, jak ją rozpoznać i zgłosić.
2. Dowiedziałaś/eś się czym są nieodpowiednie treści i jak je blokować.
3. Dowiedziałaś/eś się, jak być bezpiecznym podczas poznawania nowych znajomych online.
4. Nauczyłeś się uważać na udostępnianie danych w sieci - raz zamieszczone trudno usunąć.
5. Jeśli coś Ci się nie podoba: możesz to zablokować, zgłosić lub zamknąć swoje konto.

Rozdział zakończony!

Gratulacje! Udało Ci się ukończyć ten rozdział!



Nabyte umiejętności

1. Umiesz rozpoznać cyberprzemoc.
2. Wiesz jak zablokować nieodpowiednie treści.
3. Wiesz jak rozpoznać internetowych trolli i nie wpaść w ich sidła.

Co dalej?

Teraz możesz powtórzyć ten rozdział lub przejść do następnego klikając na jeden z przycisków:

Powtórz

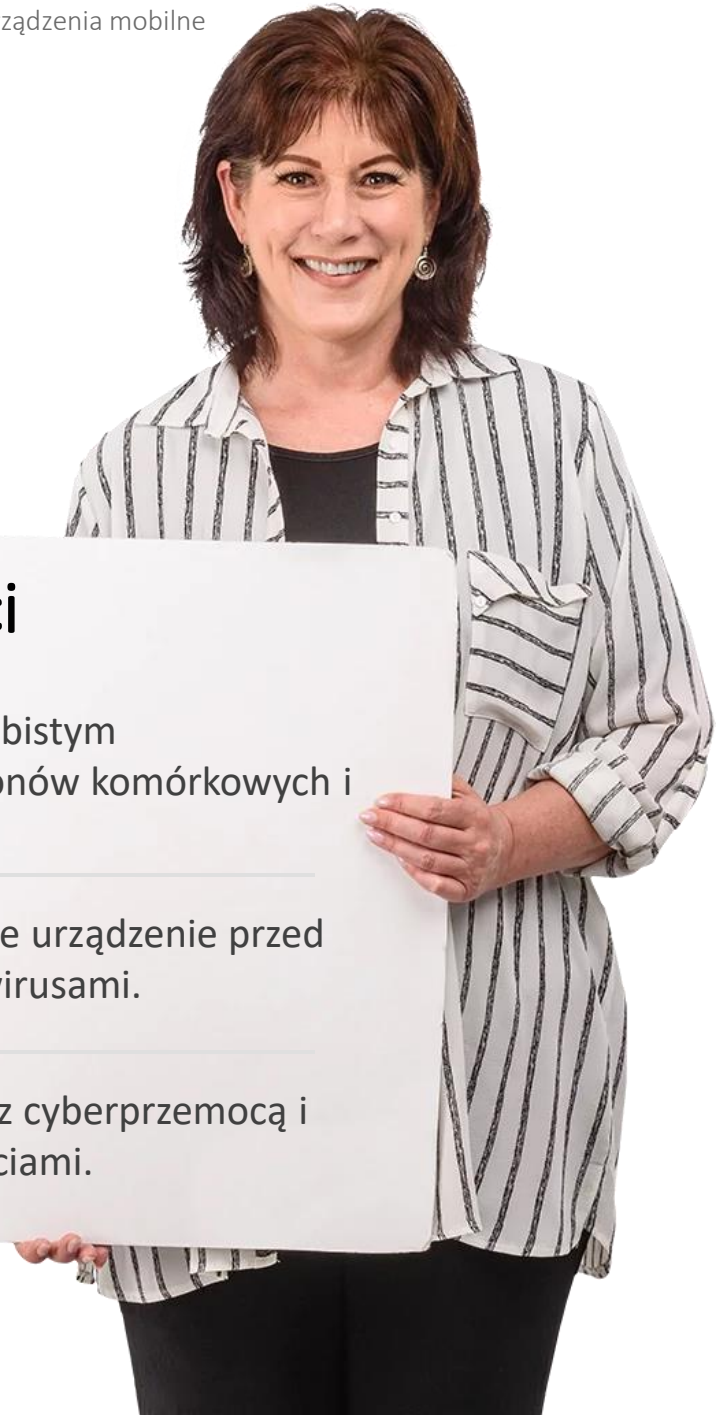
Dalej

Podsumowanie modułu

1. Dowiedziałaś/eś się o bezpieczeństwie telefonów komórkowych.
2. Dowiedziałaś/eś się o RODO.
3. Dowiedziałaś/eś się o rodzajach uwierzytelniania.
4. Dowiedziałaś/eś się, jak tworzyć silne hasła.
5. Poznałaś/eś narzędzia ataków hakerskich: malware, ransomware, DDoS.
6. Dowiedzieliście się o cyberprzemocy i jak nie stać się jej ofiarą.
7. Dowiedziałeś się, jak dostosować ustawienia SafeSearch Google, aby zapobiec nieodpowiednim treściom.

Moduł zakończony!

Gratulacje! Udało Ci się ukończyć ten moduł!



Nabyte umiejętności

1. Dowiedziałeś się o osobistym bezpieczeństwie telefonów komórkowych i RODO.
2. Wiesz jak chronić swoje urządzenie przed atakami hakerskimi i wirusami.
3. Wiesz jak radzić sobie z cyberprzemocą i nieodpowiednimi treściami.

Co dalej?

Teraz możesz powtórzyć ten moduł lub przejść do następnego klikając na jeden z przycisków:

Powtórz

Dalej