Możliwość dofinansowania

Cyberzagrożenia – ochrona danych osobistych i firmowych

Numer usługi 2025/06/06/135305/2798369

1 900,00 PLN brutto
1 900,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

UCZELNIA NAUK SPOŁECZNYCH

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
19 h
04.08.2025 do 05.08.2025

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	**Pracownicy firm i instytucji**, którzy mają dostęp do danych osobowych lub firmowych i chcą zwiększyć świadomość zagrożeń cybernetycznych w codziennej pracy. **Właściciele małych i średnich przedsiębiorstw**, którzy odpowiadają za bezpieczeństwo informacji w swoich organizacjach i chcą ograniczyć ryzyko wycieku danych. **Osoby odpowiedzialne za IT i ochronę danych**, które chcą poszerzyć wiedzę na temat aktualnych zagrożeń, narzędzi ochrony oraz reagowania na incydenty. **Każdy, kto korzysta z internetu i nowoczesnych technologii**, chcąc lepiej chronić swoje dane osobowe przed atakami hakerów, wyłudzeniami oraz innymi formami cyberprzestępczości.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	01-08-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	19
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)

Zakres uprawnień	Kursy i szkolenia

Cel

Cel edukacyjny

Celem edukacyjnym szkolenia „Cyberzagrożenia – ochrona danych osobistych i firmowych” jest zwiększenie świadomości uczestników na temat zagrożeń cyfrowych oraz wyposażenie ich w praktyczną wiedzę i umiejętności niezbędne do skutecznej ochrony danych w życiu zawodowym i prywatnym. Szkolenie uczy identyfikowania potencjalnych cyberzagrożeń, reagowania na incydenty oraz stosowania zasad bezpiecznego korzystania z technologii, aby minimalizować ryzyko wycieku, kradzieży lub utraty danych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: • Uczestnik rozpoznaje podstawowe mechanizmy psychologiczne mające wpływ na decyzje i zachowania w biznesie • Zna różnice indywidualne (osobowościowe, poznawcze) wpływające na funkcjonowanie zespołów • Rozumie rolę emocji, motywacji i postaw w pracy zawodowej		Test teoretyczny
Umiejętności: • Potrafi zastosować techniki skutecznej komunikacji i aktywnego słuchania • Analizuje i rozwiązuje konflikty z wykorzystaniem narzędzi psychologicznych • Stosuje psychologiczne techniki wpływu i negocjacji w sposób etyczny • Zarządza stresem i emocjami w sytuacjach zawodowych	Ankieta diagnostyczna przed szkoleniem • Test wiedzy i mini-quizy podczas szkolenia • Obserwacja zadań warsztatowych przez trenera • Feedback grupowy i indywidualny • Formularz ewaluacyjny z samooceną nabytych umiejętności	Obserwacja w warunkach symulowanych
Kompetencje społeczne: • Uczestnik buduje relacje oparte na zaufaniu i empatii • Wykazuje gotowość do refleksji nad własnym stylem zarządzania i komunikacji • Potrafi dostosować zachowanie do zróżnicowanych odbiorców (zespół, klienci, współpracownicy)		Wywiad swobodny

Cel biznesowy

Celem biznesowym szkolenia jest wsparcie organizacji w budowaniu skutecznych systemów ochrony informacji, co bezpośrednio przekłada się na ograniczenie ryzyka strat finansowych, reputacyjnych oraz operacyjnych związanych z

incydentami cyberbezpieczeństwa. Szkolenie umożliwia firmom i instytucjom wdrożenie dobrych praktyk w zakresie zabezpieczania danych osobowych i firmowych, co jest kluczowe zarówno dla utrzymania płynności działania, jak i ochrony przed konsekwencjami prawnymi wynikającymi z naruszenia przepisów, takich jak RODO.

Dodatkowo, udział pracowników w szkoleniu pozwala organizacji na:

Wzmacnianie zaufania klientów, partnerów i kontrahentów poprzez wykazywanie dbałości o bezpieczeństwo informacji i odpowiedzialne zarządzanie danymi,
Zmniejszanie ryzyka przestojów i kosztownych incydentów, które mogą prowadzić do utraty danych, wycieku poufnych informacji czy szantażu ze strony cyberprzestępców,
Optymalizację procesów wewnętrznych poprzez podniesienie kompetencji pracowników, dzięki czemu cała organizacja staje się bardziej odporna na cyberzagrożenia,
Podnoszenie konkurencyjności firmy na rynku, gdzie bezpieczeństwo informacji staje się coraz ważniejszym kryterium przy wyborze partnerów biznesowych.
W efekcie, szkolenie to stanowi inwestycję w rozwój i stabilność firmy, pozwalając na minimalizowanie potencjalnych strat i wzmacnianie pozycji przedsiębiorstwa w środowisku cyfrowym.

Efekt usługi

1. Wiedza:

• Zna podstawowe rodzaje cyberzagrożeń i ich mechanizmy działania (np. phishing, malware, ransomware).

• Rozumie znaczenie ochrony danych osobowych i firmowych w kontekście obowiązujących przepisów (np. RODO).

• Potrafi wskazać najczęstsze słabe punkty w zabezpieczeniach oraz wyjaśnić konsekwencje incydentów bezpieczeństwa.

2. Umiejętności:

• Identyfikuje potencjalne zagrożenia w codziennej pracy i potrafi skutecznie im przeciwdziałać.

• Stosuje zasady bezpiecznego korzystania z poczty elektronicznej, Internetu oraz narzędzi firmowych.

• Reaguje prawidłowo na próby wyłudzenia informacji i zgłasza incydenty zgodnie z obowiązującymi procedurami.

3. Kompetencje społeczne:

• Działa odpowiedzialnie w zakresie ochrony danych osobowych i firmowych, dbając o bezpieczeństwo swoje i zespołu.

• Aktywnie dzieli się wiedzą o cyberzagrożeniach z innymi pracownikami, promując kulturę bezpieczeństwa w miejscu pracy.

• Wykazuje gotowość do ciągłego podnoszenia kwalifikacji z zakresu cyberbezpieczeństwa i ochrony danych.

Metoda potwierdzenia osiągnięcia efektu usługi

• **Ankieta wstępna (pre-test):** określenie poziomu wiedzy i oczekiwań uczestnika przed rozpoczęciem szkolenia.

• **Ćwiczenia warsztatowe:** analiza wypowiedzi, zachowań i decyzji uczestników w trakcie symulacji i pracy w grupach.

• **Obserwacja trenerska:** bieżąca informacja zwrotna udzielana w trakcie zajęć, oparta na konkretnych zachowaniach.

• **Podsumowujący test wiedzy i umiejętności:** quiz wielokrotnego wyboru i zadanie opisowe.

• **Ewaluacja końcowa (post-test):** samoocena nabytych umiejętności oraz deklaracja wdrożenia wiedzy do praktyki zawodowej.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK - zawiera

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK - potwierdza przeprowadzenie walidacji

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument potwierdza rozdzielenie tych procesów

Program

DZIEŃ 1

09:00 – 09:15 – Pre-test wiedzy

• Krótki test wstępny sprawdzający poziom wiedzy uczestników

09:15 – 09:30 – Otwarcie szkolenia

• Powitanie uczestników

• Omówienie programu i celów

• Wprowadzenie do zagadnień cyberzagrożeń

09:30 – 11:00 – Cyberzagrożenia w życiu codziennym i biznesie (2 jednostki)

• Typowe zagrożenia: phishing, oszustwa, ataki socjotechniczne

• Przykłady incydentów – case studies

11:00 – 11:15 – Przerwa kawowa

11:15 – 13:00 – Ochrona tożsamości cyfrowej (2 jednostki)

• Budowanie bezpiecznych haseł

• Dwuskładnikowa autoryzacja

• Rozpoznawanie prób kradzieży tożsamości

13:00 – 14:00 – Przerwa obiadowa

14:00 – 15:45 – Techniki zabezpieczania urządzeń i danych (2 jednostki)

• Bezpieczne korzystanie z komputerów i smartfonów

• Szyfrowanie danych i tworzenie kopii zapasowych

• Ochrona sieci Wi-Fi

15:45 – 16:00 – Przerwa

16:00 – 17:00 – Praktyczne wskazówki na każdy dzień (1,5 jednostki)

• Bezpieczne zachowania online

• Jak chronić prywatność w mediach społecznościowych

• Sesja pytań i odpowiedzi

DZIEŃ 2

09:00 – 10:45 – Co robić w przypadku cyberataku? (2 jednostki)

• Reagowanie na atak: pierwsze kroki

• Zgłaszanie incydentów

• Współpraca z działem IT/policją

10:45 – 11:00 – Przerwa kawowa

11:00 – 13:00 – Warsztat praktyczny: scenariusze ataków i obrona (2 jednostki)

• Analiza przypadków – ćwiczenia w grupach

• Rozpoznawanie i przeciwdziałanie zagrożeniom

13:00 – 14:00 – Przerwa obiadowa

14:00 – 15:45 – Utrwalenie i rozwój nawyków bezpieczeństwa (2 jednostki)

• Tworzenie własnego planu bezpieczeństwa

• Narzędzia do monitorowania i kontroli zagrożeń

• Aktualne trendy w cyberbezpieczeństwie

15:45 – 16:00 – Przerwa

16:00 – 17:00 – Post-test wiedzy

• Test podsumowujący zdobyte umiejętności i wiedzę

• Omówienie wyników

17:00 – 17:15 – Podsumowanie i zakończenie szkolenia

• Najważniejsze wnioski

• Pytania i odpowiedzi

Harmonogram

Liczba przedmiotów/zajęć: 11

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Pre-test wiedzy	-	04-08-2025	09:00	09:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 11 Otwarcie szkolenia	Wioleta Kamińska	04-08-2025	09:15	09:30	00:15
3 z 11 Cyberzagrożenia w życiu codziennym i biznesie	Wioleta Kamińska	04-08-2025	09:30	11:00	01:30
4 z 11 Ochrona tożsamości cyfrowej	Wioleta Kamińska	04-08-2025	11:15	13:00	01:45
5 z 11 Techniki zabezpieczania urządzeń i danych	Wioleta Kamińska	04-08-2025	14:00	15:45	01:45
6 z 11 Praktyczne wskazówki na każdy dzień	Wioleta Kamińska	04-08-2025	16:00	17:00	01:00
7 z 11 Co robić w przypadku cyberataku?	Wioleta Kamińska	05-08-2025	09:00	10:45	01:45
8 z 11 Warsztat praktyczny: scenariusze ataków i obrona	Wioleta Kamińska	05-08-2025	11:00	13:00	02:00
9 z 11 Utrwalenie i rozwój nawyków bezpieczeństwa	Wioleta Kamińska	05-08-2025	14:00	15:45	01:45
10 z 11 Post-test wiedzy	-	05-08-2025	16:00	17:00	01:00
11 z 11 Podsumowanie i zakończenie szkolenia	Wioleta Kamińska	05-08-2025	17:00	17:15	00:15

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	1 900,00 PLN
Koszt przypadający na 1 uczestnika netto	1 900,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Wioleta Kamińska

Trener szkolenia to doświadczony specjalista w dziedzinie cyberbezpieczeństwa, posiadający wieloletnią praktykę zarówno w sektorze biznesowym, jak i edukacyjnym. Prowadził liczne projekty szkoleniowe dla firm i instytucji, wspierając wdrażanie skutecznych procedur ochrony danych oraz reagowania na cyberzagrożenia. Jest ceniony za umiejętność przekazywania skomplikowanej wiedzy w przystępny i praktyczny sposób, z naciskiem na zastosowanie rozwiązań w codziennej pracy.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały po szkoleniu: prezentacje, materiały warsztatowe.

Certyfikat u uczestnictwa oraz zdania egzaminu

Warunki techniczne

Komputer z zainstalowanym MS Teams

Kontakt

Joanna Gosławska

E-mail mba.administarcja@uns.lodz.pl
Telefon (+48) 697 504 463