Możliwość dofinansowania

DIGITAL SECURITY MACIEJ RADZIWIŁKO

Brak ocen dla tego dostawcy

Nie daj się oskubać – jak rozpoznać zagrożenia w sieci i chronić się przed oszustwami

Numer usługi 2026/01/30/206997/3296864

Romanowce / stacjonarna

Usługa szkoleniowa

11 h

18.08.2026 do 18.08.2026

900,00 PLN brutto

900,00 PLN netto

81,82 PLN brutto/h

81,82 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa skierowana jest do dorosłych użytkowników Internetu – osób prywatnych, pracowników małych i dużych firm, urzędów i instytucji publicznych, a także osób 50+ oraz seniorów, którzy korzystają z bankowości elektronicznej, zakupów online, poczty elektronicznej, telefonu oraz mediów społecznościowych. Szkolenie przeznaczone jest dla osób na poziomie podstawowym i średniozaawansowanym, które chcą lepiej rozumieć współczesne oszustwa internetowe i telefoniczne, w tym wykorzystujące portale społecznościowe, nauczyć się rozpoznawać próby wyłudzeń oraz stosować praktyczne zasady bezpiecznego postępowania, aby chronić swoje dane i pieniądze – zarówno w życiu prywatnym, jak i w środowisku pracy.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	08-08-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	11
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie uczestników do rozpoznawania i unikania współczesnych oszustw internetowych, telefonicznych oraz tych wykorzystujących media społecznościowe. Uczestnicy poznają mechanizmy manipulacji stosowane przez oszustów, nauczą się krok po kroku weryfikować wiarygodność wiadomości, stron i rozmówców, a także reagować na podejrzane sytuacje. Kurs kładzie nacisk na praktyczne zasady bezpiecznego postępowania, które pozwalają zminimalizować ryzyko utraty danych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje najczęściej występujące metody oszustw w sieci i offline.	Uczestnik wskazuje co najmniej 4 cechy charakterystyczne dla prób oszustwa na podstawie przedstawionych przykładów.	Analiza dowodów i deklaracji
Analizuje przykłady phishingu, smishingu i vishingu oraz identyfikuje elementy manipulacji.	Uczestnik prawidłowo rozróżnia phishing, smishing i vishing w minimum 3 z 4 zaprezentowanych sytuacji.	Analiza dowodów i deklaracji
Ocenia wiarygodność wiadomości, stron internetowych, ofert oraz rozmówców.	Uczestnik stosuje minimum 3 zasady weryfikacji wiarygodności podczas analizy przykładowej wiadomości lub oferty.	Analiza dowodów i deklaracji
Stosuje zasady bezpiecznego postępowania w sytuacji podejrzenia oszustwa.	Uczestnik wskazuje poprawną sekwencję działań w przypadku próby wyłudzenia danych lub pieniędzy.	Analiza dowodów i deklaracji
Wykonuje podstawowe procedury reagowania po wykryciu oszustwa lub próby oszustwa.	Uczestnik wymienia właściwe instytucje i formy zgłoszenia dla co najmniej 2 sytuacji zagrożenia.	Analiza dowodów i deklaracji

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Współczesne oszustwa w sieci i offline – przegląd metod.

2. Phishing, smishing, vishing – analiza prawdziwych przykładów.

3. Fałszywe sklepy, inwestycje i „okazje”.

4. Zasady weryfikacji wiarygodności wiadomości, stron i rozmówców.

5. Procedury reagowania – zgłoszenia do banku, policji, innych instytucji.

6. Ćwiczenia na realnych scenariuszach, podsumowanie, test.

Szkolenie trwa **11 godzin dydaktycznych**.

Kurs składa się z:

5 godzin dydaktycznych teorii

3 godzin dydaktycznych praktyki,

3 godzin dydaktycznych przerw oraz walidacji.

W liczbę godzin szkolenia wliczone są przerwy. Przerwy uwzględnione są również w harmonogramie.

Szkolenie odbywa się stacjonarnie.

Szkolenie ma charakter warsztatowy. Jest skierowane do osób dorosłych.

Walidacja zostanie przeprowadzona w oparciu o obserwacje w warunkach symulowanych oraz test teoretyczny. Walidator nie jest jednocześnie trenerem prowadzącym szkolenie. Wprowadzona została rozdzielność.

Przed i po szkoleniu obowiązuje test wiedzy.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	900,00 PLN

Koszt przypadający na 1 uczestnika netto	900,00 PLN
Koszt osobogodziny brutto	81,82 PLN
Koszt osobogodziny netto	81,82 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

Maciej Radziwiłko

Trener z zakresu cyberbezpieczeństwa i kompetencji cyfrowych. Pokazuje zagrożenia „oczami hakera” – omawia realne scenariusze ataków (phishing, malware, przejęcia kont) oraz uczy praktycznych sposobów zabezpieczania urządzeń, haseł i tożsamości cyfrowej. Posiada doświadczenie w pracy z osobami dorosłymi, w tym użytkownikami nietechnicznymi, którym tłumaczy złożone kwestie bezpieczeństwa w prosty, zrozumiały sposób.

2 z 2

Ewelina Natkowska

Trenerka z doświadczeniem w pracy edukacyjnej z dorosłymi i młodzieżą, specjalizująca się w social engineering. Pokazuje, jak oszuści wykorzystują emocje, zaufanie i presję czasu do wyłudzania danych oraz pieniędzy, a także uczy, jak budować bezpieczne nawyki komunikacji online. Prowadzi warsztaty nastawione na ćwiczenie reakcji w typowych scenariuszach ataków socjotechnicznych i wzmacnianie świadomości zagrożeń.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają prezentację ze szkolenia w formacie PDF, checklistę bezpiecznych zachowań w sieci (do wykorzystania w firmie i prywatnie), zestaw przykładowych fałszywych wiadomości, stron internetowych i postów z mediów społecznościowych do samodzielnego przećwiczenia, dostęp do krótkiego testu online sprawdzającego wiedzę po szkoleniu oraz prosty plan działań po szkoleniu, który pomoże wdrożyć zdobytą wiedzę w życiu prywatnym i w miejscu pracy.

Informacje dodatkowe

Informacje dodatkowe:

- *W razie potrzeby szkolenie zostanie dostosowane do osób z niepełnosprawnościami.*
- *Harmonogram godzinowy szkolenia każdorazowo dostosowywany jest do grupy szkoleniowej.*
- *Godziny realizacji poszczególnych modułów szkolenia mogą ulec zmianie.*

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - w przypadku dofinansowania w co najmniej 70%

Przed złożeniem wniosku o dofinansowanie prosimy o kontakt, w celu rezerwacji miejsca.

Adres

Romanowce
16-500 Romanowce
woj. podlaskie

Szkolenie realizowane jest na terenie całej Polski, w salach szkoleniowych zapewnianych przez Dostawcę Usługi lub w siedzibie Zleceniodawcy. Dokładny adres każdej edycji szkolenia jest każdorazowo przekazywany uczestnikom przed rozpoczęciem usługi.

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

MACIEJ RADZIWIŁKO

E-mail maciejradziwilko@gmail.com
Telefon (+48) 605 326 008