Możliwość dofinansowania

Szkolenie - Świadomość zagrożeń cybernetycznych – phishing, malware, bezpieczne hasła i ochrona tożsamości cyfrowej.

Numer usługi 2026/01/28/206997/3290494

900,00 PLN brutto
900,00 PLN netto
81,82 PLN brutto/h
81,82 PLN netto/h

DIGITAL SECURITY MACIEJ RADZIWIŁKO

Brak ocen dla tego dostawcy

Romanowce
Usługa szkoleniowa
stacjonarna
11:00 h
17.08.2026 do 17.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa skierowana jest do dorosłych użytkowników Internetu – pracowników biurowych, administracyjnych, osób prowadzących działalność gospodarczą oraz użytkowników prywatnych, którzy korzystają z komputera, poczty elektronicznej, bankowości elektronicznej i mediów społecznościowych. Szkolenie przeznaczone jest dla osób na poziomie podstawowym, które chcą zwiększyć świadomość zagrożeń cybernetycznych oraz nauczyć się praktycznych zasad bezpiecznego korzystania z sieci.
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 edukacyjnym usługi jest przygotowanie uczestników do świadomego i bezpiecznego korzystania z komputera, Internetu, poczty elektronicznej, bankowości elektronicznej oraz mediów społecznościowych. Po zakończeniu szkolenia uczestnik potrafi rozpoznawać najczęstsze zagrożenia cybernetyczne (phishing, malware, fałszywe strony), tworzyć i stosować silne hasła, korzystać z uwierzytelniania dwuskładnikowego oraz stosować podstawowe zasady ochrony tożsamości cyfrowej w życiu zawodowym i prywatnym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpoznaje najczęstsze rodzaje zagrożeń cybernetycznych (phishing, malware, fałszywe strony www).	Uczestnik klasyfikuje przykładowe wiadomości i strony jako bezpieczne lub niebezpieczne.	Test teoretyczny
Uczestnik tworzy silne hasła i potrafi korzystać z menedżera haseł.	Uczestnik tworzy przykładowe silne hasło oraz zapisuje je w menedżerze haseł zgodnie z instrukcją trenera.	Obserwacja w warunkach symulowanych
Uczestnik stosuje podstawowe zasady ochrony tożsamości cyfrowej (bezpieczne logowanie, 2FA, ostrożność przy udostępnianiu danych).	Uczestnik wskazuje poprawne działania zabezpieczające w przedstawionych scenariuszach oraz samodzielnie proponuje sposób zabezpieczenia konta.	Obserwacja w warunkach symulowanych
Uczestnik wykazuje odpowiedzialność za bezpieczeństwo cyfrowe organizacji oraz gotowość do krytycznej oceny interakcji online, promując bezpieczne nawyki w środowisku pracy i reagując zgodnie z procedurami na próby manipulacji.	Identyfikuje własną rolę w systemie bezpieczeństwa firmy i wykazuje gotowość do brania odpowiedzialności za ochronę danych przed skutkami błędów ludzkich.	Obserwacja w warunkach symulowanych
	Inicjuje działania zapobiegawcze poprzez zgłaszanie podejrzanych incydentów (np. próby phishingu) odpowiednim osobom lub działom wewnątrz organizacji.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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

TAK

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

TAK

Program

Zakres tematyczny:

1. Wprowadzenie do cyberbezpieczeństwa i aktualnych zagrożeń w sieci, omówienie najczęstszych błędów użytkowników i ich konsekwencji dla firmy.

2. Ataki „oczami hakera” – phishing, malware, przejęcia kont, kradzież tożsamości.

3. Zabezpieczanie urządzeń, haseł, poczty i komunikatorów w życiu prywatnym i zawodowym.

4. Social engineering – manipulacje na emocjach, presja czasu, fałszywy autorytet.

5. Rozpoznawanie podejrzanych wiadomości, stron i ogłoszeń, ćwiczenia na realnych przykładach.

6. Bezpieczna komunikacja online i nawyki „cyber-higieny” na co dzień.

7. Podsumowanie, test wiedzy i omówienie dobrych praktyk do wdrożenia w firmie.

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.

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Wprowadzenie do cyberbezpieczeństwa, najczęstsze błędy użytkowników i ich konsekwencje dla firmy	Maciej Radziwiłko	17-08-2026	09:00	10:30	01:30
2 z 10 Przerwa	Maciej Radziwiłko	17-08-2026	10:30	10:45	00:15
3 z 10 Ataki oczami hakera – phishing, malware, przejęcia kont, kradzież tożsamości	Maciej Radziwiłko	17-08-2026	10:45	12:15	01:30
4 z 10 Przerwa	Maciej Radziwiłko	17-08-2026	12:15	13:00	00:45
5 z 10 Social engineering – manipulacje na emocjach, presja czasu, fałszywy autorytet	Maciej Radziwiłko	17-08-2026	13:00	14:30	01:30
6 z 10 Przerwa	Maciej Radziwiłko	17-08-2026	14:30	14:45	00:15
7 z 10 Rozpoznawanie podejrzanych wiadomości, stron i ogłoszeń, ćwiczenia na realnych przykładach	Ewelina Natkowska	17-08-2026	14:45	15:30	00:45
8 z 10 Przerwa	Ewelina Natkowska	17-08-2026	15:30	15:45	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 10 Bezpieczna komunikacja online i nawyki cyber-higieny, podsumowanie i test wiedzy	Ewelina Natkowska	17-08-2026	15:45	16:30	00:45
10 z 10 Walidacja w formie testu oraz obserwacje w warunkach symulowanych	-	17-08-2026	16:30	17:15	00:45

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 i stron do samodzielnego przećwiczenia, dostęp do krótkiego testu online sprawdzającego wiedzę po szkoleniu.

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