Możliwość dofinansowania

Jak nie dać się oszukać w sieci – praktyczne podstawy cyberbezpieczeństwa

Numer usługi 2026/04/21/218350/3504202

6 000,00 PLN brutto
6 000,00 PLN netto
375,00 PLN brutto/h
375,00 PLN netto/h
261,33 PLN cena rynkowa

GRUPA ETH Kamil Bany

Brak ocen dla tego dostawcy

Siedlce
Usługa szkoleniowa
stacjonarna
16:00 h
01.07.2026 do 02.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób dorosłych, które chcą zwiększyć swoje bezpieczeństwo w Internecie i nauczyć się rozpoznawać najczęstsze oszustwa internetowe. Usługa jest przeznaczona w szczególności dla właścicieli firm, pracowników biurowych, osób korzystających z poczty elektronicznej, bankowości internetowej, zakupów online i mediów społecznościowych, a także dla wszystkich osób, które chcą zdobyć praktyczne umiejętności ochrony swoich danych, pieniędzy i kont internetowych. Szkolenie nie wymaga specjalistycznej wiedzy informatycznej.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	21-06-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
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 nabycie przez uczestników praktycznych kompetencji w zakresie podstaw cyberbezpieczeństwa, rozpoznawania najczęstszych oszustw internetowych oraz stosowania zasad bezpiecznego korzystania z poczty elektronicznej, bankowości internetowej, mediów społecznościowych i urządzeń mobilnych. Po ukończeniu szkolenia uczestnik potrafi identyfikować zagrożenia cyfrowe, oceniać ryzyko, stosować podstawowe metody ochrony danych i kont oraz właściwie reagować w sytuacji podejrzenia oszust

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpoznaje podstawowe zagrożenia występujące w cyberprzestrzeni, w szczególności phishing, smishing, vishing, fałszywe sklepy internetowe oraz próby wyłudzenia danych i środków finansowych.	Uczestnik: rozróżnia podstawowe rodzaje oszustw internetowych, wskazuje cechy charakterystyczne podejrzanych wiadomości, stron internetowych i komunikatów, identyfikuje sygnały ostrzegawcze świadczące o próbie wyłudzenia.	Test teoretyczny

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

Dzień 1

Moduł 1. Wprowadzenie do cyberbezpieczeństwa

- podstawowe pojęcia związane z cyberbezpieczeństwem,
- najczęstsze zagrożenia występujące w Internecie,
- jak dochodzi do wyłudzeń danych i środków finansowych,

- omówienie najczęstszych błędów użytkowników.

Moduł 2. Najpopularniejsze oszustwa internetowe

- phishing, smishing, vishing,
- fałszywe wiadomości e-mail, SMS i połączenia telefoniczne,
- oszustwa „na dopłatę", „na kuriera", „na pracownika banku",
- rozpoznawanie prób manipulacji i presji.

Moduł 3. Bezpieczne korzystanie z poczty elektronicznej i Internetu

- bezpieczne otwieranie wiadomości, linków i załączników,
- rozpoznawanie podejrzanych stron internetowych,
- zasady bezpiecznego przeglądania Internetu,
- ćwiczenia na przykładach.

Moduł 4. Ochrona kont i urządzeń

- tworzenie silnych haseł,
- uwierzytelnianie dwuskładnikowe,
- podstawowe zasady zabezpieczania komputera i smartfona,
- aktualizacje, kopie zapasowe i ochrona dostępu do kont.

Dzień 2

Moduł 5. Bezpieczne zakupy i płatności online

- jak rozpoznać fałszywy sklep internetowy,
- bezpieczne metody płatności,
- zagrożenia związane z bankowością elektroniczną i BLIK,
- analiza rzeczywistych scenariuszy oszustw.

Moduł 6. Bezpieczeństwo w mediach społecznościowych i komunikatorach

- fałszywe profile i próby przejęcia kont,
- ochrona prywatności i danych osobowych,
- bezpieczne korzystanie z komunikatorów i portali społecznościowych,
- najczęstsze zagrożenia w codziennej komunikacji online.

Moduł 7. Reagowanie na incydenty bezpieczeństwa

- co zrobić po kliknięciu w podejrzany link,
- co zrobić po podaniu danych lub wykonaniu podejrzanej płatności,
- zabezpieczenie konta i urządzenia po incydencie,
- gdzie i w jaki sposób zgłaszać oszustwa internetowe.

Moduł 8. Utrwalenie wiedzy i przygotowanie do walidacji

- powtórzenie najważniejszych zagadnień,
- omówienie dobrych praktyk bezpieczeństwa,
- analiza przypadków,
- przygotowanie do walidacji efektów uczenia się.

Walidacja efektów uczenia się

- test wiedzy,
- analiza krótkich scenariuszy sytuacyjnych.

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	6 000,00 PLN
Koszt przypadający na 1 uczestnika netto	6 000,00 PLN
Koszt osobogodziny brutto	375,00 PLN
Koszt osobogodziny netto	375,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma materiały szkoleniowe w formie elektronicznej i/lub papierowej, obejmujące: prezentację szkoleniową, checklistę zasad bezpiecznego korzystania z Internetu, przykłady najczęstszych oszustw internetowych, zestaw praktycznych wskazówek dotyczących ochrony danych, kont i urządzeń, a także materiały pomocnicze do samodzielnego wykorzystania po zakończeniu szkolenia. Materiały zostaną przygotowane w sposób przystępny i praktyczny, tak aby uczestnik mógł wykorzystać je w codziennym życiu oraz pracy zawodowej.

Warunki uczestnictwa

Warunkiem uczestnictwa w usłudze jest zgłoszenie udziału zgodnie z zasadami rekrutacji oraz podstawowa umiejętność korzystania z komputera, smartfona, poczty elektronicznej i Internetu. Szkolenie nie wymaga specjalistycznej wiedzy informatycznej ani wcześniejszego doświadczenia w obszarze cyberbezpieczeństwa.

Informacje dodatkowe

Usługa realizowana jest w formie stacjonarnej przez 2 dni. Szkolenie ma charakter praktyczny i obejmuje analizę przykładów, omówienie rzeczywistych scenariuszy oszustw internetowych oraz ćwiczenia dotyczące rozpoznawania zagrożeń i właściwego reagowania na incydenty bezpieczeństwa. Po zakończeniu usługi uczestnik przystępuje do walidacji efektów uczenia się. Warunkiem uzyskania certyfikatu jest udział w szkoleniu oraz pozytywne zaliczenie walidacji.

Adres

Siedlce

Siedlce

woj. mazowieckie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

KAMIL BANY

E-mail banykamil@gmail.com

Telefon (+48) 798 519 531