Możliwość dofinansowania

Bezpieczny w sieci – praktyczny przewodnik cyberbezpieczeństwa dla mikrofirm i MŚP - kurs

Numer usługi 2025/04/01/28897/2663660

5 000,00 PLN brutto
5 000,00 PLN netto
500,00 PLN brutto/h
500,00 PLN netto/h

TEB EDUKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,8 / 5

23 oceny

Gdańsk / stacjonarna
Usługa szkoleniowa
10 h
15.09.2025 do 16.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• Właściciele mikroprzedsiębiorstw i przedstawiciele MŚP. • Pracownicy biurowi, handlowcy oraz osoby przetwarzające dane klientów. • Osoby odpowiedzialne za organizację pracy w firmie, niezależnie od działu.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	07-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Kurs Bezpieczny w sieci – praktyczny przewodnik cyberbezpieczeństwa dla mikrofirm i MŚP przygotowuje do samodzielnego działania w zakresie ochrony danych i bezpieczeństwa cyfrowego w mikroprzedsiębiorstwach oraz sektorze MŚP.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
charakteryzyje podstawowe zagrożenia cyfrowe skierowane przeciwko małym firmom	definiuje aktualne zagrożenia w Polsce i na świecie	Test teoretyczny
	rozróżnia mechanizmy działania najpopularniejszych ataków cyfrowych na firmy	Test teoretyczny
planuje zasady bezpiecznej pracy z danymi i urządzeniami	definiuje wymogi prawne i standardy bezpieczeństwa w firmie	Test teoretyczny
	definiuje zasady zarządzania nośnikami danych i polityki czystego biurka	Test teoretyczny
obsługuje zabezpieczanie kont, systemów i dostępów do informacji	definiuje sposoby na zabezpieczenie dostępu do systemów i kont	Test teoretyczny
	definiuje środki ostrożności przy pracy na różnych urządzeniach	Test teoretyczny
Tworzy plan działań zwiększający bezpieczeństwo firmy (checklista cyberbezpieczeństwa)	opracowuje i obsługuje indywidualne procedury bezpieczeństwa	Test teoretyczny

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

Kurs skierowany jest do właścicieli i pracowników mikroprzedsiębiorstw i przedstawicieli MŚP oraz innych osób zajmujących sie przetwarzaniem danych klientów.

Usługa prowadzona jest w systemie godzin dydaktycznych.

Przerwy wliczone są w całkowity czas trwania usługi.

Walidacja, w formie testu teoretycznego, przeprowadzona jest po przeprowadzeniu całości szkolenia.

Dzień 1

1.Wprowadzenie do cyberbezpieczeństwa – pojęcia, zagrożenia, statystyki

- Ogólne zasady i definicje w cyberbezpieczeństwie
- Przegląd aktualnych zagrożeń w Polsce i na świecie

2.Najczęstsze ataki na firmy – phishing, malware, ransomware, fałszywe faktury

- Mechanizmy działania najpopularniejszych ataków
- Jak rozpoznawać potencjalnie niebezpieczne wiadomości i załączniki?

3.Hasła, logowanie, MFA – jak zadbać o dostęp do systemów i kont?

- Tworzenie i zarządzanie silnymi hasłami
- Wykorzystanie uwierzytelniania wieloskładnikowego (MFA)

4.Zasady bezpiecznej pracy online i zdalnej – e-maile, urządzenia, Wi-Fi

- Rola szyfrowania i zabezpieczania sieci
- Podstawowe środki ostrożności przy pracy na różnych urządzeniach

Dzień 2

5.Ochrona danych klientów i firmy – RODO, backupy, przechowywanie

- Minimalne wymogi prawne i standardy bezpieczeństwa
- Tworzenie i przechowywanie kopii zapasowych

6.Praca z urządzeniami – laptopy, smartfony, USB, pendrive'y

- Zarządzanie nośnikami danych i polityka czystego biurka
- Sposoby szyfrowania i bezpiecznego przechowywania plików

7.Zarządzanie zagrożeniami – symulacja incydentu i plan reakcji

- Krok po kroku: reagowanie na atak i ograniczanie szkód
- Ćwiczenia w grupach i omawianie scenariuszy

8.Twoja firma – warsztat: stworzenie własnej checklisty cyberbezpieczeństwa

- Identyfikacja kluczowych obszarów narażonych na ryzyko
- Opracowanie indywidualnych procedur bezpieczeństwa

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Wprowadzenie do cyberbezpieczeństwa – pojęcia, zagrożenia, statystyki	Tomasz Czabajski	15-09-2025	15:00	15:45	00:45
2 z 10 Najczęstsze ataki na firmy – phishing, malware, ransomware, fałszywe faktury	Tomasz Czabajski	15-09-2025	16:00	16:45	00:45
3 z 10 Hasła, logowanie, MFA – jak zadbać o dostęp do systemów i kont?	Tomasz Czabajski	15-09-2025	17:00	17:45	00:45
4 z 10 Zasady bezpiecznej pracy online i zdalnej – e-maile, urządzenia, Wi-Fi	Tomasz Czabajski	15-09-2025	18:00	18:45	00:45
5 z 10 Zasady bezpiecznej pracy online i zdalnej – e-maile, urządzenia, Wi-Fi	Tomasz Czabajski	15-09-2025	19:00	19:45	00:45
6 z 10 Ochrona danych klientów i firmy – RODO, backupy, przechowywanie	Tomasz Czabajski	16-09-2025	15:00	15:45	00:45
7 z 10 Praca z urządzeniami – laptopy, smartfony, USB, pendrive'y	Tomasz Czabajski	16-09-2025	16:00	16:45	00:45
8 z 10 Zarządzanie zagrożeniami – symulacja incydentu i plan reakcji	Tomasz Czabajski	16-09-2025	17:00	17:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 10 Twoja firma – warsztat: stworzenie własnej checklisty cyberbezpieczeństwa	Tomasz Czabajski	16-09-2025	18:00	19:30	01:30
10 z 10 walidacja: test teoretyczny	Tomasz Czabajski	16-09-2025	19:45	20:15	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	500,00 PLN
Koszt osobogodziny netto	500,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Tomasz Czabajski

Ekspert, szkoleniowiec i wykładowca TEB Edukacja Sp. Z.o.o, Fullstack developer, posiadający ponad 20-letnie doświadczenie w tworzeniu aplikacji webowych i mobilnych. Specjalista w dziedzinie cyberbezpieczeństwa aplikacji z wykorzystaniem technologii AI. Jego praca w tym obszarze obejmuje rozwój rozwiązań, które wykorzystują integrację sztucznej inteligencji w celu zwiększenia bezpieczeństwa i efektywności aplikacji internetowych

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały:

Prezentacje

Arkusze ćwiczeń

Pliki dokumentów przygotowanych w dowolnym formacie

materiały wliczone w cenę kursu

Warunki uczestnictwa

Uczestnikiem kursu może zostać każda osoba która jest pełnoletnia.

Uczestnicy nie muszą mieć specjalistycznej wiedzy technicznej.

Szkolenie prowadzone z wykorzystaniem przykładów z życia, w prostym i przystępnym języku.

Informacje dodatkowe

Istnieje możliwość uzyskania dofinansowania szkolenia w wysokości do 95% wartości w ramach programu:

Agencja Rozwoju Pomorza S.A. (lider projektu) realizuje projekt „WEKTOR. Metropolitalny System Finansowania Kształcenia.”, który jest współfinansowany ze środków Unii Europejskiej w ramach programu Fundusze Europejskie dla Pomorza 2021-2027.

Więcej o projekcie : https://www.arp.gda.pl/2506,o-projekcie

Adres

ul. Romana Dmowskiego 16A
80-264 Gdańsk
woj. pomorskie

zajęcia będą się odbywać w siedzibie palcówki w Gdańsku Wrzeszczu przy ul. Dmowskiego 16 A
lub al. Grunwaldzkiej 103

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt

Roksana Beben

E-mail roksana.beben@teb-edukacja.pl
Telefon (+48) 571 312 548