



Europejska Agencja
Rozwoju Mirosław
Kopik



CYBERBEZPIECZEŃSTWO. STRATEGIE ZAPOBIEGANIA I REAKCJI NA INCYDENTY

Numer usługi 2025/03/20/27209/2639126

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 10 h

📅 10.06.2025 do 10.06.2025

2 340,00 PLN brutto

2 340,00 PLN netto

234,00 PLN brutto/h

234,00 PLN netto/h

Informacje podstawowe

Kategoria	Biznes / Sprzedaż
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Właściciele firm, menadżerowie, kierownicy działów handlowych, liderzy, handlowcy, przedstawiciele handlowi, sprzedawcy, kadra zarządzająca handlem, pracownicy działu obsługi klienta, technicy, doradcy, marketerzy, specjaliści ds. logistyki, handlu, obsługi klienta, księgowości, rozliczeń, finansów, produkcji, zakupów, rozwoju, obsługi biura, obsługi informatycznej, menadżerowie produktów i projektów oraz osoby zainteresowane zdobyciem nowych kompetencji w zakresie sprzedaży.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	24
Data zakończenia rekrutacji	09-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje do: rozpoznawania cybernetycznych zagrożeń w sektorze handlowym; stosowania strategii zapobiegania i reakcji na incydenty, stosowania zasad bezpiecznych transakcji online w handlu, bezpiecznego przeglądania sprzedażowych zasobów Internetu, ochrony przed złośliwym oprogramowaniem i atakami poprzez przeglądarkę, unikania ataków phishingowych w handlu, do stosowania bezpiecznych płatności elektronicznych podczas sprzedaży, ochrony danych klientów w handlu elektronicznym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje zagrożenia cybernetyczne w sektorze handlowym.	Opisuje zasady bezpiecznej transakcji online w handlu.	Test teoretyczny
	Definiuje zagrożenia cybernetyczne w sektorze handlowym.	Test teoretyczny
	Wybiera bezpieczne narzędzia i rozszerzenia do przeglądarki.	Test teoretyczny
	Opisuje bezpieczne sposoby przeglądania sprzedażowych zasobów Internetu.	Test teoretyczny
	Zna strategie zapobiegania i reakcji na incydenty.	Test teoretyczny
Skutecznie chroni się przed złośliwym oprogramowaniem i atakami poprzez przeglądarkę.	Określa sposoby ochrony przed złośliwym oprogramowaniem i atakami phishingowymi.	Test teoretyczny
	Opisuje sposób weryfikacji tożsamości kontrahenta przed przeprowadzeniem transakcji.	Test teoretyczny
	Opisuje bezpieczne stosowanie płatności elektronicznych.	Test teoretyczny
Chroni dane klienta w handlu elektronicznym.	Opisuje sposoby ochrony danych klienta w handlu elektronicznym.	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, dokument potwierdzający uzyskanie kompetencji (certyfikat) zawiera opis efektów uczenia się.

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

Tak, dokument (certyfikat) potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak, dokument (certyfikat) potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Przywitanie, kontrakt z uczestnikami. Pre-test.

Moduł 1. Wprowadzenie do Cyberbezpieczeństwa. Definicja cyberbezpieczeństwa i jego kluczowe znaczenie dla sektora handlowego. Bezpieczne zarządzanie hasłami i dostępem w procesie sprzedaży. Zarządzanie Ryzykiem Cyberbezpieczeństwa w dziale handlowym. Zarządzanie Incydentami Cyberbezpieczeństwa.

Metody pracy: Wykład. Prezentacja multimedialna. Wyjaśnianie.

Moduł 2. Tożsamość Cyfrowa. Znaczenie tożsamości cyfrowej dla sektora handlowego. Strategie monitorowania aktywności w sieci w kontekście zapewniania bezpieczeństwa. Narzędzia i strategie zapewniające prywatność i bezpieczeństwo podczas korzystania z Internetu w sektorze handlowym. Praktyczne wskazówki dotyczące bezpiecznego surfowania w sieci w kontekście działań handlowych.

Metody pracy: Wykład interaktywny. Prezentacja multimedialna.

Moduł 3. Incydenty związane z cyberbezpieczeństwem w działaniach handlowych - przykłady. Phishing, Vishing, socjotechnika. Ransomware. Studium przypadków związanych z phishingiem w handlu. Praktyczne wskazówki dotyczące identyfikacji i unikania zagrożeń phishingowych.

Metody pracy: Wykład. Prezentacja multimedialna. Wyjaśnianie.

Moduł 4. Bezpieczeństwo transakcji handlowych. Zasady bezpiecznych transakcji online w handlu. Sposoby weryfikacji tożsamości kontrahenta przed przeprowadzeniem transakcji. Bezpieczeństwo danych handlowych. Strategie tworzenia, przechowywania i przywracania kopii zapasowych danych sprzedażowych. Techniki automatyzacji procesów tworzenia kopii zapasowych.

Metody pracy: Wykład. Prezentacja multimedialna. Wyjaśnianie.

Podsumowanie i ewaluacja szkolenia. Post test.

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Przywitanie Kontrakt z uczestnikami. Pre-test.	-	10-06-2025	09:00	09:20	00:20

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 9 Moduł 1. Wprowadzenie do Cyberbezpieczeństwa.	Dawid Koziorowski	10-06-2025	09:20	10:50	01:30
3 z 9 Przerwa	Dawid Koziorowski	10-06-2025	10:50	11:05	00:15
4 z 9 Moduł 2. Tożsamość Cyfrowa.	Dawid Koziorowski	10-06-2025	11:05	12:35	01:30
5 z 9 Przerwa	Dawid Koziorowski	10-06-2025	12:35	12:50	00:15
6 z 9 Moduł 3. Incydenty związane z cyberbezpieczeństwem...	Dawid Koziorowski	10-06-2025	12:50	14:20	01:30
7 z 9 Przerwa obiadowa	Dawid Koziorowski	10-06-2025	14:20	14:50	00:30
8 z 9 Moduł 4. Bezpieczeństwo transakcji handlowych.	Dawid Koziorowski	10-06-2025	14:50	16:20	01:30
9 z 9 Podsumowanie i ewaluacja szkolenia. Post test.	-	10-06-2025	16:20	16:30	00:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 340,00 PLN
Koszt przypadający na 1 uczestnika netto	2 340,00 PLN
Koszt osobogodziny brutto	234,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Dawid Koziorowski

Trener IT z ponad 10 letnim doświadczeniem, certyfikowany „etyczny haker” oraz instruktor EC-COUNCIL. Na co dzień zajmuje się realizacją testów penetracyjnych symulujących realne ataki hakerskie na infrastrukturę sieciowe oraz aplikacje webowe. Specjalizuje się w socjotechnice oraz działaniach typu Red Team. Jako trener realizował szkolenia z zakresu cyberbezpieczeństwa m.in. dla specjalnych (CBZC, ABW, CBA), oraz dla administracji (m.in. Krajowa Izba Skarbowa). Obszar specjalizacji: Cyberbezpieczeństwo, Osint (Biały wywiad), inżynieria społeczna, Phishing, Hacking. Założyciel i właściciel Akademii Portal – Centrum Szkoleń IT.

Wykształcenie: wyższe informatyczne, specjalizacja: Cyberbezpieczeństwo i Informatyka Śledcza

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik szkolenia otrzyma autorskie materiały szkoleniowe (prezentacja multimedialna, skrypt itp.) drogą mailową na dzień przed rozpoczęciem szkolenia.

Warunki uczestnictwa

Osoba zainteresowana skorzystaniem z usługi rozwojowej z dofinansowaniem musi zarejestrować się w Bazie Usług Rozwojowych oraz dokonać zapisu na usługę przed jej rozpoczęciem, z użyciem numeru ID wsparcia.

Każdy uczestnik szkolenia otrzyma link aktywacyjny do platformy szkoleniowej, aktywacja umożliwi uczestnictwo w szkoleniu.

Podczas logowania się do platformy (system prosi tylko o podanie: imienia, e-maila i hasła) w celu jednoznacznego zidentyfikowania uczestnika szkolenia wymagane jest podanie imienia i nazwiska uczestnika.

Lista obecności na szkoleniu będzie sporządzona na podstawie pisemnych potwierdzeń uczestników szkolenia o ich uczestnictwie w szkoleniu oraz dodatkowo na podstawie potwierdzenia obecności na czacie.

Informacje dodatkowe

Czas trwania usługi szkoleniowej to 10 godzin dydaktycznych (1 godzina dydaktyczna= 45 minut). Szkolenie jest jednodniowe, ujęte w 4 moduły. Planujemy przerwy pomiędzy modułami.

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Warunki techniczne

Szkolenia odbywają się na platformie ClickMeeting w formie Webinaru.

Warunki techniczne niezbędne do udziału w usłudze:

Każdy komputer używany na co dzień będzie wystarczający do uczestnictwa w usłudze rozwojowej. Rekomendujemy udział w szkoleniu za pośrednictwem komputera. Tablet a zwłaszcza smartfon może być mniej praktyczny ze względu na wielkość ekranu.

1. Komputer/laptop – najlepiej, procesor Intel Core od i3 w górę, zalecane 4 GB RAM lub więcej, tablet 3 GB RAM lub smartfon.
2. Stałe łącze internetowe w dowolnej technologii – światłowod, GSM 3G lub 4G/LTE, Internet kablowy, zalecane min. 3 Mb/s w zakresie pobierania i wysyłania danych.
3. W miarę możliwości najnowszy system operacyjny: Windows 10 lub 8, 7, Vista z SP1; macOS X z macOS 10.7 lub nowszy, iOS 10 lub nowszy lub dedykowana aplikacja mobilna z AppStore lub GooglePlay, Android w wersji 4.0.4 lub nowszy w przypadku tabletów lub inne systemy operacyjne dające pewność odbioru transmisji bez zakłóceń.
4. Dowlona przeglądarka internetowa (zalecana Chrome lub Mozilla FireFox).
5. Głośniki lub słuchawki.

W trakcie szkolenia dostęp do wizji i dźwięku mają tylko trenerzy, uczestnicy szkolenia mogą komunikować się jedynie za pomocą czatu. Link umożliwiający uczestnictwo w spotkaniu on-line ważny jest tylko w dniu szkolenia. Do każdego szkolenia przypisany jest oddzielny link. Nad sprawnym przebiegiem szkolenia będzie czuwać trener organizacyjny.

Kontakt



Mirosław Kopik

E-mail mirek.kopik@eurodotacje.pl

Telefon (+48) 505 060 800