Możliwość dofinansowania

Identyfikowanie i analizowanie oszustw komputerowych w MŚP

Numer usługi 2026/09/07/205802/3794001

1 040,00 PLN brutto
1 040,00 PLN netto
130,00 PLN brutto/h
130,00 PLN netto/h
261,33 PLN cena rynkowa

AD-TRADE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
08:00 h
01.12.2026 do 01.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników mikro, małych i średnich przedsiębiorstw ze wszystkich branż, w szczególności do firm sektora finansowego i ubezpieczeniowego (PKD sekcja K, działy 64, 65 i 66) — banków, w tym banków spółdzielczych, SKOK, zakładów ubezpieczeń, agencji i multiagencji ubezpieczeniowych, brokerów, pośredników kredytowych, firm pożyczkowych, leasingowych i faktoringowych, domów maklerskich, TFI oraz podmiotów świadczących działalność wspomagającą usługi finansowe. Adresatami są wszyscy pracownicy korzystający w pracy z poczty elektronicznej, komputera lub telefonu służbowego: obsługa klienta, sprzedaż, księgowość, kadry, zaplecze operacyjne, kadra kierownicza oraz właściciele firm. Usługa nie jest adresowana do personelu IT i nie wymaga wiedzy informatycznej ani przygotowania technicznego.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	24-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Usługa przygotowuje pracownika MŚP do samodzielnego rozpoznawania oszustw komputerowych kierowanych do przedsiębiorstwa i analizowania ich przebiegu. Uczestnik odróżnia phishing, smishing i vishing, rozpoznaje fałszywe strony logowania i płatności, ocenia wiarygodność linków i załączników, wyjaśnia mechanizm Business Email Compromise oraz omawia trzy scenariusze oszustwa: przejęcie poczty, fałszywą fakturę i podszycie się pod przełożonego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1.1. Charakteryzuje najczęściej występujące rodzaje oszustw komputerowych	Wyjaśnia pojęcia phishing, smishing i vishing oraz wskazuje różnice między nimi; rozróżnia oszustwa komputerowe masowe i ukierunkowane, z uwzględnieniem ich charakterystycznych cech; wskazuje najczęstsze cele oszustw komputerowych w przedsiębiorstwach, w tym wyłudzanie danych, środków finansowych oraz dostępu do systemów; opisuje aktualne trendy w oszustwach komputerowych, w tym złośliwe wykorzystanie sztucznej inteligencji; wyjaśnia konsekwencje oszustw dla funkcjonowania przedsiębiorstwa (finansowe, operacyjne, reputacyjne); komunikuje współpracownikom informacje o rozpoznanych zagrożeniach związanych z oszustwami komputerowymi	Test teoretyczny z wynikiem generowanym automatycznie
1.2. Rozpoznaje elementy ostrzegawcze w komunikacji elektronicznej	Wskazuje cechy charakterystyczne fałszywych stron logowania i płatności; ocenia wiarygodność linków i załączników w komunikacji elektronicznej za pomocą dostępnych narzędzi; identyfikuje cechy wiadomości phishingowych; wyjaśnia mechanizm Business Email Compromise (BEC) i identyfikuje typowe schematy wykorzystania; wskazuje kanały komunikacji w przedsiębiorstwach z sektora MŚP, które są wykorzystywane przez cyberprzestępców do realizacji oszustw komputerowych; dzieli się wiedzą i umiejętnościami w rozpoznawaniu elementów ostrzegawczych z innymi pracownikami	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1.3. Analizuje realne scenariusze oszustw komputerowych	Omawia scenariusz oszustwa polegającego na przejęciu dostępu do poczty elektronicznej, wskazując jego przebieg oraz możliwe skutki; omawia scenariusz oszustwa polegającego na wyłudzeniu pieniędzy z wykorzystaniem fałszywej faktury; omawia scenariusz oszustwa polegającego na podszywaniu się pod przełożonego lub współpracownika; wskazuje dominujące typy oszustw komputerowych w przedsiębiorstwach sektora MŚP; identyfikuje główne przyczyny podatności przedsiębiorstw sektora MŚP; dzieli się wnioskami z analiz scenariuszy oszustw z innymi pracownikami	Test teoretyczny z wynikiem generowanym automatycznie

Cel biznesowy

Usługa ogranicza ryzyko strat finansowych i operacyjnych wynikających z oszustw komputerowych kierowanych do przedsiębiorstwa. Pracownik, który rozpoznaje elementy ostrzegawcze w komunikacji elektronicznej i zna mechanizm Business Email Compromise, przerywa scenariusz oszustwa na etapie, na którym nie doszło jeszcze do wypłaty środków ani do przekazania danych dostępowych. Szkolenie zmniejsza także liczbę zgłoszeń kierowanych do obsługi informatycznej i skraca czas reakcji na podejrzaną korespondencję.

Efekt usługi

Uczestnik samodzielnie rozpoznaje oszustwa komputerowe kierowane do przedsiębiorstwa i analizuje ich przebieg: odróżnia phishing, smishing i vishing, wskazuje elementy ostrzegawcze w wiadomościach i na stronach logowania, ocenia wiarygodność linków i załączników oraz omawia typowe scenariusze oszustwa i przyczyny podatności firm sektora MŚP.

Metoda potwierdzenia osiągnięcia efektu usługi

Efekty uczenia się osiągane są metodą warsztatową opartą na analizie przypadków i ćwiczeniach wykonywanych samodzielnie przez uczestników na materiale zbliżonym do realnej korespondencji służbowej. Osiągnięcie efektów potwierdza test wiedzy w formie elektronicznej — 30 pytań jednokrotnego wyboru, w tym pytania oparte na przypadkach, z progiem zaliczenia 70% — przeprowadzany w narzędziu generującym wynik automatycznie. Każde pytanie przypisane jest do kryteriów weryfikacji konkretnego efektu uczenia się, dzięki czemu wynik testu wskazuje, które efekty uczestnik osiągnął.

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

Szkolenie jednodniowe, 8 godzin zegarowych, realizowane zdalnie w czasie rzeczywistym. Zajęcia prowadzone są metodą warsztatową z wykorzystaniem analizy przypadków i ćwiczeń wykonywanych samodzielnie przez uczestników. Szkolenie nie wymaga wiedzy informatycznej ani przygotowania technicznego. Grupa liczy od 2 do 15 osób.

SESJA 1 — Rodzaje oszustw komputerowych i elementy ostrzegawcze (9:00–13:00, 4 godziny) Rodzaje oszustw komputerowych: phishing, smishing i vishing — różnice i kanały. Oszustwa masowe a ukierunkowane. Cele atakujących: dane, środki finansowe, dostęp do systemów. Aktualne trendy, w tym złośliwe wykorzystanie sztucznej inteligencji. Konsekwencje finansowe, operacyjne i reputacyjne dla przedsiębiorstwa. Elementy ostrzegawcze w komunikacji elektronicznej: cechy fałszywych stron logowania i płatności, ocena wiarygodności linków i załączników dostępnymi narzędziami, cechy wiadomości phishingowych. Mechanizm Business Email Compromise (BEC) i typowe schematy jego wykorzystania. Metody: wykład interaktywny, demonstracja na żywo, analiza przypadków, ćwiczenia w grupach.

SESJA 2 — Analiza scenariuszy i praktyka rozpoznawania (13:30–17:00, 4 godziny wraz z walidacją) Kanały komunikacji wykorzystywane przez cyberprzestępców w przedsiębiorstwach sektora MŚP. Warsztat: analiza trzech scenariuszy oszustwa — przejęcie dostępu do poczty elektronicznej, wyłudzenie pieniędzy z wykorzystaniem fałszywej faktury, podszycie się pod przełożonego lub współpracownika. Dominujące typy oszustw w sektorze MŚP i główne przyczyny podatności przedsiębiorstw. Zadanie praktyczne: klasyfikacja zestawu dwunastu wiadomości elektronicznych wraz ze wskazaniem elementów ostrzegawczych. Metody: warsztat, analiza przypadków, zadanie decyzyjne, dyskusja moderowana.

ROZGRANICZENIE ZAKRESU Blok nr 1 kończy się na rozpoznaniu i analizie oszustwa komputerowego. Mechanizmy socjotechniczne, fazy ataku, techniki manipulacji psychologicznej i nawyki decyzyjne stanowią odrębny blok nr 3 Rekomendacji RPK. Zasady cyberhigieny (hasła, uwierzytelnianie wieloskładnikowe, aktualizacje, sieci, kopie zapasowe) stanowią odrębny blok nr 2. Zasady przetwarzania i udostępniania danych stanowią odrębny blok nr 4. Rozpoznawanie incydentu i postępowanie po jego wykryciu, w tym zgłoszenie do CSIRT, stanowią odrębny blok nr 5. Żaden z tych zakresów nie wchodzi w zakres niniejszej usługi.

WALIDACJA EFEKTÓW UCZENIA SIĘ (16:30–17:00, 30 minut) Walidacja prowadzona jest metodą testu teoretycznego z wynikiem generowanym automatycznie. Test obejmuje 30 pytań jednokrotnego wyboru, w tym pytania oparte na przypadkach — uczestnik ocenia konkretną wiadomość lub sytuację i wskazuje właściwe działanie — i sprawdza wszystkie trzy efekty uczenia się zgodnie z przypisanymi im kryteriami weryfikacji. Test przeprowadzany jest w narzędziu elektronicznym generującym wynik automatycznie, bez udziału osoby oceniającej, co zapewnia rozdzielenie procesu kształcenia od procesu walidacji. Za organizację walidacji, weryfikację warunków przystąpienia i dokumentowanie wyników odpowiada osoba walidująca wskazana w karcie usługi, niebędąca trenerem prowadzącym zajęcia. Uczestnik, który uzyska minimum 70% punktów, otrzymuje zaświadczenie ukończenia szkolenia wystawione przez AD-TRADE Sp. z o.o. / szkolimy24.com, zawierające opis efektów uczenia się, kryteria ich weryfikacji oraz zastosowane metody walidacji.

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Rodzaje oszustw komputerowych: phishing, smishing i vishing — cele atakujących i aktualne trendy	Zajęcia	Daniel Kacprowicz	01-12-2026	09:00	11:00	02:00
2 z 8 -	Przerwa	-	01-12-2026	11:00	11:15	00:15
3 z 8 Elementy ostrzegawcze w komunikacji elektronicznej i mechanizm Business Email Compromise	Zajęcia	Daniel Kacprowicz	01-12-2026	11:15	13:00	01:45
4 z 8 -	Przerwa	-	01-12-2026	13:00	13:30	00:30
5 z 8 Warsztat: analiza trzech scenariuszy oszustwa — przejęcie poczty, fałszywa faktura, podszycie się pod przełożonego	Zajęcia	Daniel Kacprowicz	01-12-2026	13:30	15:15	01:45
6 z 8 -	Przerwa	-	01-12-2026	15:15	15:30	00:15
7 z 8 Zadanie praktyczne: klasyfikacja zestawu dwunastu wiadomości elektronicznych ze wskazaniem elementów ostrzegawczych	Zajęcia	Daniel Kacprowicz	01-12-2026	15:30	16:30	01:00
8 z 8 -	Walidacja	-	01-12-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:30
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 040,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	1 040,00 PLN
Koszt osobogodziny brutto	130,00 PLN
Koszt osobogodziny netto	130,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Kacprowicz

Prezes Zarządu AD-TRADE Sp. z o.o., właściciel marki szkoleniowej szkolimy24.com. Trener z udokumentowanym doświadczeniem ponad 290 godzin przeprowadzonych szkoleń z zakresu kompetencji cyfrowych, obsługi komputera i internetu oraz cyberbezpieczeństwa (potwierdzone referencjami: ODZ BHP Ekspert, MOPR Włocławek, MAXDOM, Klub Senior+). Prowadzi szkolenia z praktycznego zastosowania narzędzi sztucznej inteligencji dla pracowników administracji publicznej, jednostek pomocy społecznej, placówek oświatowych oraz firm sektora MŚP — m.in. szkolenie z cyberbezpieczeństwa, ochrony danych osobowych i narzędzi AI dla 52 pracowników Miejskiego Ośrodka Pomocy Rodzinie we Włocławku oraz szkolenia z AI i narzędzi wizualnych dla placówek oświatowych. Specjalizacja: wdrażanie narzędzi generatywnej sztucznej inteligencji (ChatGPT, Microsoft Copilot, Google Gemini) w pracy biurowej i administracyjnej, prompt engineering, bezpieczeństwo danych w środowisku AI oraz automatyzacja powtarzalnych zadań biurowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik otrzymuje pakiet materiałów przygotowanych przez szkolimy24.com: skrypt PDF „Oszustwa komputerowe w MŚP", katalog elementów ostrzegawczych wiadomości i stron logowania, zestaw dwunastu wiadomości do klasyfikacji wraz z kluczem, trzy opisy scenariuszy oszustw do analizy, listę narzędzi do weryfikacji linków i załączników oraz nagrania obu sesji. Materiały przekazywane są w formie cyfrowej w dniu szkolenia i pozostają dostępne przez 12 miesięcy.

Warunki techniczne

Usługa realizowana zdalnie w czasie rzeczywistym na platformie Zoom — spotkanie z rejestracją uczestników i funkcją nagrywania.

Minimalne wymagania sprzętowe: komputer klasy PC lub Mac z procesorem dwurdzeniowym 2 GHz i pamięcią 4 GB RAM, kamera internetowa, mikrofon oraz głośniki lub zestaw słuchawkowy.

Minimalne wymagania dotyczące parametrów łącza sieciowego: łącze internetowe o przepustowości minimum 5 Mb/s dla pobierania i 2 Mb/s dla wysyłania.

Niezbędne oprogramowanie: przeglądarka internetowa w aktualnej wersji (Google Chrome, Microsoft Edge lub Mozilla Firefox) albo aplikacja Zoom; pakiet biurowy oraz konto w narzędziu AI (ChatGPT, Microsoft Copilot lub Google Gemini) — wystarczające są konta w wersjach bezpłatnych.

Okres ważności linku: link do spotkania jest aktywny przez cały czas trwania usługi i zostaje przesłany uczestnikom pocztą elektroniczną najpóźniej 24 godziny przed rozpoczęciem zajęć.

Sposób weryfikacji obecności: rejestr wejść i wyjść uczestników generowany przez platformę, weryfikacja tożsamości na podstawie włączonej kamery podczas zajęć oraz podczas walidacji efektów uczenia się.

Przebieg usługi jest rejestrowany (nagrywany) w celu udokumentowania jej realizacji zgodnie z wymogami obowiązującymi dla usług zdalnych w Bazie Usług Rozwojowych.

Kontakt

Daniel Kacprowicz

E-mail biuro@szkolimy24.com

Telefon (+48) 508 325 677