Możliwość dofinansowania

Neuros Seweryn Stachowicz

Brak ocen dla tego dostawcy

Szkolenie podstawowe z zakresu cyberbezpieczeństwa IT

Numer usługi 2025/05/12/168107/2738973

553,50 PLN brutto
450,00 PLN netto
92,25 PLN brutto/h
75,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
6 h
25.06.2025 do 31.07.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	1. **Działy Marketingu** • **Opis**: Pracownicy działów marketingu często korzystają z różnych narzędzi online, co czyni ich podatnymi na ataki phishingowe i inne formy oszustw internetowych. 2. **Działy Eksportu** • **Opis**: Osoby zajmujące się eksportem często muszą zarządzać poufnymi informacjami oraz komunikować się z partnerami zagranicznymi, co stawia je w obliczu ryzyka wyłudzenia danych. 3. **Działy Księgowości** • **Opis**: Pracownicy księgowości mają dostęp do wrażliwych informacji finansowych, co czyni ich celem dla cyberprzestępców. 4. **Działy HR** • **Opis**: Działy HR zarządzają danymi osobowymi pracowników oraz procesami rekrutacyjnymi, co również wiąże się z dużym ryzykiem wyłudzeń. 5. **Działy R&D** **Opis**: Działy R&D zarządzają danymi firmowymi, często stanowiące własność intelektualną firmy kradzież takich danych naraża firmę na straty.

Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	24-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	6
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem edukacyjnym szkolenia z zakresu cyberbezpieczeństwa jest:

Zwiększenie świadomości, wiedzy i umiejętności uczestników w zakresie identyfikacji oraz przeciwdziałania zagrożeniom cyberbezpieczeństwa, z uwzględnieniem specyficznych potrzeb działów HR, eksportu i księgowości.

Składniki celu edukacyjnego
Wiedza:
Uczestnicy poznają:

Kluczowe zagrożenia cyberbezpieczeństwa, takie jak phishing, ransomware, ataki socjotechniczne.
Zasady ochrony danych osobowych (zgodność z RODO) oraz danych

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozumie znaczenie cyberbezpieczeństwa w organizacji i potrafi wskazać jego wpływ na funkcjonowanie firmy.	Uczestnik rozumie, dlaczego przestrzeganie zasad bezpieczeństwa IT jest kluczowe.	Debata swobodna
Uczestnik zna podstawowe rodzaje zagrożeń, takie jak phishing, ransomware i ataki socjotechniczne.	Uczestnik rozpoznaje elementy charakterystyczne dla ataków socjotechnicznych.	Analiza dowodów i deklaracji
Potrafi stosować procedury bezpieczeństwa w pracy z danymi odpowiednimi dla swojego działu.	Uczestnik poprawnie wskazuje procedury ochrony danych odpowiednie dla swojej roli.	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi rozpoznać próbę phishingu i stworzyć mocne hasła. Zwiększona czujność na ataki socjotechniczne i współpraca w zgłaszaniu incydentów.	Uczestnik konfiguruje uwierzytelnianie 2FA.	Obserwacja w warunkach rzeczywistych
Uczestnik zna zasady bezpiecznego korzystania z e-maila, chmury (np. Azure) i urządzeń mobilnych. Potrafi zastosować poznane metody ochrony w praktyce, np. szyfrowanie danych.	Poprawne rozpoznanie ryzyk związanych z urządzeniami prywatnymi w pracy zdalnej.	Prezentacja

Cel biznesowy

Głównym celem usługi szkolenia wstępnego z zakresu cyberbezpieczeństwa IT, szczególnie w kontekście wyłudzania danych, jest zwiększenie świadomości i umiejętności pracowników w zakresie ochrony informacji oraz zapobiegania zagrożeniom związanym z cyberprzestępczością.

Zrozumienie zagrożeń: Uczestnicy szkolenia będą mieli okazję poznać różne formy ataków cybernetycznych, takie jak phishing, ransomware, malware i inne techniki wyłudzania danych.

Identyfikacja zagrożeń: Uczestnicy nauczą się rozpoznawać podejrzane e-maile, wiadomości i inne formy komunikacji, które mogą być próbami wyłudzenia danych.

Zwiększenie odpowiedzialności: Uczestnicy będą świadomi swojej roli w zapewnieniu bezpieczeństwa informacji, co przyczyni się do budowania kultury bezpieczeństwa w firmie.

Zgodność z przepisami: Uczestnicy zdobędą wiedzę na temat obowiązujących przepisów dotyczących ochrony danych osobowych (np. RODO), co pomoże organizacji uniknąć potencjalnych sankcji prawnych.

Minimalizacja ryzyka: Dzięki podniesieniu świadomości i umiejętności pracowników, organizacja będzie lepiej przygotowana do identyfikacji i neutralizacji zagrożeń, co zmniejszy ryzyko udanych ataków.

Efekt usługi

Po ukończeniu szkolenia

co najmniej 90% uczestników poprawnie przejdzie test końcowy z rozpoznawania zagrożeń.

Metoda potwierdzenia osiągnięcia efektu usługi

Przed szkoleniem: Uczestnicy wypełniają krótki test diagnozujący ich wiedzę z zakresu cyberbezpieczeństwa (np. rozpoznawanie phishingu, tworzenie mocnych haseł, zasady RODO).

Powtórzenie testu, aby porównać wyniki i zobaczyć, jak zwiększyła się wiedza.

Efekt: Wzrost liczby poprawnych odpowiedzi o określony procent (np. z 60% do 90%) wskazuje na skuteczność szkolenia.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

certyfikat ukończenia szkolenia zawiera opis efektów uczenia się i jasno wskazuje, jakie umiejętności i wiedza zostały zdobyte podczas szkolenia.

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

Tak, dokument potwierdza walidację na podstawie pre i post test.

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

Tak po każdej lekcji będzie przeprowadzany test walidacji.

Program

1. Wprowadzenie do cyberbezpieczeństwa (1 godz.)

- Znaczenie cyberbezpieczeństwa w organizacji.
- Najnowsze statystyki i przykłady ataków.
- Dlaczego cyberbezpieczeństwo to odpowiedzialność każdego pracownika?

2. Główne zagrożenia i sposoby ataków (1 godz.)

- Phishing, spear-phishing i ransomware – mechanizmy działania.
- Ataki socjotechniczne: manipulacja pracownikami.
- Złośliwe oprogramowanie: jak je rozpoznać?

3. Bezpieczna praca z danymi (1,5 godz.)

- Ochrona danych osobowych (zgodność z RODO) – moduł dedykowany dla działu HR.
- Bezpieczna wymiana informacji w handlu międzynarodowym – moduł dedykowany dla działu eksportu.
- Ochrona danych finansowych i wykrywanie prób oszustw – moduł dedykowany dla działu księgowości.

4. Praktyczne warsztaty (1,5 godz.)

- Rozpoznawanie phishingu, deepfake – analiza przypadków.
- Symulacja ataku socjotechnicznego: testy na czujność.
- Tworzenie mocnych haseł i zarządzanie nimi.
- Konfiguracja dwuskładnikowego uwierzytelniania (2FA).

5. Zasady bezpiecznego korzystania z narzędzi IT (0,5 godz.)

- Bezpieczne korzystanie z e-maila.
- Zarządzanie dokumentami i współdzielenie plików w chmurze. Azure
- Ochrona urządzeń mobilnych i prywatnych komputerów w pracy zdalnej.

6. Podsumowanie i sesja Q&A (0,5 godz.)

- Omówienie najważniejszych zasad.
- Sesja pytań i odpowiedzi.
- Checklist bezpieczeństwa.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	553,50 PLN
Koszt przypadający na 1 uczestnika netto	450,00 PLN
Koszt osobogodziny brutto	92,25 PLN
Koszt osobogodziny netto	75,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Seweryn Stachowicz

20 lat jako inżynier administrujący serwerami i sieciami komputerowymi.
Prowadzący meetupy dla społeczności It jak i szkolenia cyberhigiena dla dzieci.
Promujący wiedzę z chmur publicznych.
Lubiący propagować wiedzę techniczną.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały ze szkoleń zostaną udostępnione, są to autorskie materiały.

Warunki techniczne

Warunki techniczne niezbędne do udziału w usłudze w formie zdalnej:

a) platformę /rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa - **Microsoft MS Teams,** użytkownik będzie się podłączał jako gość

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji - przeglądarka internetowa Google Chrome , Safari, Opera lub Mozilla Firefox w najnowszych wersjach. Mikrofon, głośnik lub zestaw słuchawkowy

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: łącze inernetowe: min download: 768 Mb/s, min upload: 384 Mb/s.

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: komputer PC z systemem Operacyjnym Windows 7/8.x/10 (za wyjątkiem Windows 10 S) albo komputer MacBook z systemem Mac OS X 10.5 lub wyższy.

e) okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line: link jest ważny od pół godziny przed rozpoczęciem usługi do momentu jej zakończenia

Kontakt

Seweryn Stachowicz

E-mail biuro@neuros.pl
Telefon (+48) 177 707 005