Możliwość dofinansowania

Szkolenie podstawowe z zakresu cyberbezpieczeństwa IT

Numer usługi 2025/07/30/168107/2911744

1 180,80 PLN brutto
960,00 PLN netto
147,60 PLN brutto/h
120,00 PLN netto/h

Neuros Seweryn Stachowicz

Brak ocen dla tego dostawcy

Mielec / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

Usługa szkoleniowa

8 h

13.08.2025 do 13.08.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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	8
Data zakończenia rekrutacji	12-08-2025
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	8
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
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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
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?

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

1. Wprowadzenie do cyberbezpieczeństwa (1,5 godz.)

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

2. Główne zagrożenia i sposoby ataków (1,5 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 (1,5 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: 6

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 6 Wprowadzenie do cyberbezpieczeństwa (1,5 godz.)	Seweryn Stachowicz	13-08-2025	07:00	08:30	01:30	Tak
2 z 6 2. Główne zagrożenia i sposoby ataków (1,5 godz.)	Seweryn Stachowicz	13-08-2025	08:30	10:00	01:30	Tak
3 z 6 3. Bezpieczna praca z danymi (1,5 godz.)	Seweryn Stachowicz	13-08-2025	10:00	11:30	01:30	Tak
4 z 6 4. Praktyczne warsztaty (1,5 godz.)	Seweryn Stachowicz	13-08-2025	11:30	13:00	01:30	Tak
5 z 6 5. Zasady bezpiecznego korzystania z narzędzi IT (1,5 godz.)	Seweryn Stachowicz	13-08-2025	13:00	14:30	01:30	Tak
6 z 6 6. Podsumowanie i sesja Q&A (0,5 godz.)	Seweryn Stachowicz	13-08-2025	14:30	15:00	00:30	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 180,80 PLN
Koszt przypadający na 1 uczestnika netto	960,00 PLN
Koszt osobogodziny brutto	147,60 PLN

Koszt osobogodziny netto	120,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Seweryn Stachowicz

20 lat jako inżynier administrujący serwerami i sieciami komputerowymi.
Prowadzący meetup dla społeczności It jak i szkolenia cyberhigiena dla dzieci.
Promujący wiedzę z chmur publicznych.
Wiedza techniczna to pasja.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały ze szkoleń zostaną udostępnione, są to autorskie materiały.

Warunki techniczne

Szkolenie zostanie przeprowadzone w budynku Intech.

Adres

ul. Wojska Polskiego 9
39-300 Mielec
woj. podkarpackie

Usługa realizowana w budynku Intech.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja

Kontakt

Seweryn Stachowicz

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