Możliwość dofinansowania

edpo.pl Michał Cupiał

★★★★★

Bezpieczeństwo i Higiena w Sieci - szkolenie stacjonarne

Numer usługi 2024/11/14/160750/2411696

Olsztyn / stacjonarna
Usługa szkoleniowa
16 h
18.01.2025 do 19.01.2025

2 600,00 PLN brutto
2 600,00 PLN netto
162,50 PLN brutto/h
162,50 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Grupa docelowa szkolenia to: • pracownicy i/lub właściciele pracujący z komputerem, Internetem ora z urządzeniami mobilnymi • pracownicy z sektora MSP • osoby na co dzień używający zarówno w życiu prywatnym jak zawodowym z komputera, Internetu oraz urządzeń mobilnych Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie. Wymaganiem jest podstawowa znajomość obsługi komputera.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	17-01-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do samodzielnego zwiększenia świadomości i kompetencji w zakresie bezpieczeństwa oraz higieny w sieci, z naciskiem na rozumienie i praktyczne stosowanie najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym i osobistym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawowe pojęcia związane z cyberbezpieczeństw m i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Uczestnik poprawnie definiuje wymienione pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Test teoretyczny
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik wymienia i opisuje co najmniej trzy różne typy zagrożeń, podając przykłady oraz sposoby ich identyfikacji.	Test teoretyczny
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania	Test teoretyczny
Identyfikuje i reaguj na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania na te zagrożenia.	Test teoretyczny
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik potrafi określić bezpieczne skonfigurowanie połączeń sieciowych i zastosować praktyki ochrony prywatności podczas korzystania z sieci publicznych.	Test teoretyczny
Promuje świadomość bezpieczeństwa cyfrowego wśród kolegów i rodziny.	Uczestnik inicjuje rozmowy na temat bezpieczeństwa cyfrowego i dzieli się najlepszymi praktykami z otoczeniem.	Test teoretyczny
Rozwija postawę odpowiedzialności za wspólne bezpieczeństwo cyfrowe.	Uczestnik wykazuje zrozumienie, że bezpieczeństwo cyfrowe jest wspólnym zadaniem i angażuje się w działania promujące bezpieczne zachowania w sieci.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Demonstruje zdolność do krytycznej oceny informacji znalezionych w Internecie i ich źródeł	Uczestnik krytycznie ocenia wiarygodność informacji online, weryfikując je za pomocą zaufanych źródeł i narzędzi.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Dokument potwierdzający uzyskanie kompetencji 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?

Dokument 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?

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Szkolenie ma na celu zapoznanie uczestników z nowoczesnymi praktykami zapewniającymi bezpieczeństwo oraz higienę korzystania z zasobów sieciowych.

Uczestnicy zdobędą wiedzę i umiejętności niezbędne do ochrony swoich danych, urządzeń oraz prywatności podczas pracy online.Program kursu obejmuje 16 godzin dydaktycznych, z czego 1 godzina przeznaczona jest na walidację umiejętności (test pisemny).

Zajęcia prowadzone są stacjonarnie, metodami interaktywnymi, co umożliwia aktywną naukę poprzez ćwiczenia praktyczne i doświadczenie. Uczestnicy pracują na komputerze dostawcy usług.

I dzień: Podstawy cyberbezpieczeństwa

- Wprowadzenie do cyberbezpieczeństwa
- Podstawowe pojęcia i istota cyberbezpieczeństwa
- Podstawy prawne oraz zalecenia ENISA dotyczące cyberbezpieczeństwa
- Cyberataki
  - Omówienie najczęstszych rodzajów ataków
  - Ćwiczenie praktyczne: phishing
  - Przestępstwa finansowe w cyfrowym świecie
- Hasła i menedżer haseł
  - Ćwiczenie praktyczne: Zasady tworzenia silnych haseł zgodnie z aktualnymi standardami bezpieczeństwa
  - Jak działają i jak wybrać odpowiedni menedżer haseł

II dzień: Ochrona przed cyberatakami

- Dlaczego hasło to za mało? Praktyka autoryzacji dwuskładnikowej
- Szyfrowanie danych – plików, folderów i urządzeń przenośnych
- Zastrzeżenie PESEL-u
- Tworzenie kopii zapasowych danych
- Zabezpieczanie urządzeń i prywatności
  - Programy antywirusowe, zapory sieciowe, tryb incognito, pliki cookie, VPN

- Świadomość cyfrowa
  - Jakie informacje mogą o nas zebrać hakerzy?
  - Socjotechnika w praktyce

- Co zrobić w przypadku ataku?
  - Procedury formalne i komunikacyjne po ataku

- Fake newsy i sztuczna inteligencja
  - Ćwiczenie praktyczne: Jak AI jest wykorzystywane do tworzenia dezinformacji?

- Podsumowanie i najlepsze praktyki
- Walidacja zdobytej wiedzy (45minut)

Organizacja szkolenia

Zajęcia są prowadzone w godzinach dydaktycznych (1 godzina = 45 minut) i realizowane przy użyciu metod interaktywnych, umożliwiających naukę poprzez doświadczenie i ćwiczenia praktyczne.

W szkoleniu przewidzianych jest: 10h teorii i 6h praktyki.

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Wprowadzenie do cyberbezpieczeństwa. Podstawowe pojęcia i istota cyberbezpieczeństwa	Marcin Smoliński	18-01-2025	08:00	08:45	00:45
2 z 15 Podstawy prawne oraz zalecenia ENISA dotyczące cyberbezpieczeństwa	Marcin Smoliński	18-01-2025	08:45	09:30	00:45
3 z 15 Cyberataki- Omówienie najczęstszych rodzajów ataków	Marcin Smoliński	18-01-2025	09:45	11:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 15 Ćwiczenie praktyczne: phishing	Marcin Smoliński	18-01-2025	11:15	12:00	00:45
5 z 15 Przestępstwa finansowe w cyfrowym świecie	Marcin Smoliński	18-01-2025	12:00	12:45	00:45
6 z 15 Hasła i menedżer haseł. Jak działają i jak wybrać odpowiedni menedżer haseł	Marcin Smoliński	18-01-2025	12:45	13:30	00:45
7 z 15 Ćwiczenie praktyczne :Zasady tworzenia silnych haseł zgodnie z aktualnymi standardami bezpieczeństwa	Marcin Smoliński	18-01-2025	14:00	15:30	01:30
8 z 15 Dlaczego hasło to za mało? Praktyka autoryzacji dwuskładnikowej . Szyfrowanie danych – plików, folderów i urządzeń przenośnych	Marcin Smoliński	19-01-2025	08:00	08:45	00:45
9 z 15 Zastrzeżenie PESEL-u. Tworzenie kopii zapasowych danych	Marcin Smoliński	19-01-2025	08:45	09:30	00:45
10 z 15 Zabezpieczanie urządzeń i prywatności. Programy antywirusowe, zapory sieciowe, tryb incognito, pliki cookie, VPN	Marcin Smoliński	19-01-2025	09:45	11:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 15 Świadomość cyfrowa, Jakie informacje mogą o nas zebrać hakerzy? Socjotechnika w praktyce	Marcin Smoliński	19-01-2025	11:15	12:00	00:45
12 z 15 Co zrobić w przypadku ataku? Procedury formalne i komunikacyjne po ataku	Marcin Smoliński	19-01-2025	12:00	12:45	00:45
13 z 15 Fake newsy i sztuczna inteligencja. Ćwiczenie praktyczne: Jak AI jest wykorzystywane do tworzenia dezinformacji?	Marcin Smoliński	19-01-2025	12:45	13:30	00:45
14 z 15 Podsumowanie i najlepsze praktyki	Marcin Smoliński	19-01-2025	14:00	15:15	01:15
15 z 15 Walidacja zdobytej wiedzy (45minut)	-	19-01-2025	15:15	16:00	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 600,00 PLN
Koszt przypadający na 1 uczestnika netto	2 600,00 PLN
Koszt osobogodziny brutto	162,50 PLN
Koszt osobogodziny netto	162,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Marcin Smoliński

Absolwent uczelni wyższych na kierunkach Administracja, Informatyka (zastosowanie technologii informacyjnych), studiów podyplomowych z zakresu ochrony danych oraz administratora danych, jak i efektywnej administracji systemami Linuksowymi. Zdobytą wiedzę potwierdzają także liczne certyfikaty międzynarodowe, min. ISTQB Certified Tester, ITIL Foundation v.3, PRINCE2. Jest również Audytorem Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-ENISO/IEC27001. Kierownik kilkunastu projektów w zakresie wdrożenia i uruchomienia systemów dziedzinowych, systemu obiegu dokumentów, systemów informacji przestrzennych w jednostkach samorządu terytorialnego oraz biznesu w tym koordynator dostaw sprzętu i usług szkoleniowych. Współautor oprogramowania dedykowanego Inspektorom Ochrony Danych oraz Sygnalistom. Prowadzi warsztaty z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa. W latach 2022-2024 przeprowadził łącznie około 70 godzin warsztatowych. Pasjonat rozwiązań AI, stosujący je w codziennej pracy.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy po zakończeniu usługi otrzymają prezentację szkoleniową, która zostanie wysłana na podany adres e-mail.

Warunki uczestnictwa

Warunkiem uczestnictwa jest zarejestrowanie i założenie konta w Bazie Usług Rozwojowych, zapisanie się na usługę szkoleniową za pośrednictwem Bazy i przypisanego ID wsparcia oraz spełnienie wszystkich warunków uczestnictwa w projekcie określonych przez Operatora.

Uczestnik usługi rozwojowej otrzyma zaświadczenie o ukończeniu usługi dopiero po pozytywnym wyniku testu sprawdzającego wiedzę, który odbędzie się na ostatnich zajęciach.

Warunkiem otrzymania zaświadczenia o ukończeniu usługi rozwojowej jest pozytywny wynik testu końcowego

Uczestnicy muszą posiadać podstawową wiedzę na temat obsługi komputera.

Informacje dodatkowe

Usługa rozwojowa odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut.

Koszt usługi rozwojowej nie zawiera kosztów dojazdu, wyżywienia i noclegu.

Adres

ul. Maurycego Mochnackiego 10/1
10-037 Olsztyn
woj. warmińsko-mazurskie

Szkolenie odbędzie się w siedzibie firmy Centrum Nauka Jazdy

Kontakt

Anna Smolińska

E-mail anna.smolinska@edpo.pl

Telefon (+48) 723 893 532