Możliwość dofinansowania

CYBERBEZPIECZEŃSTWO

Numer usługi 2024/05/27/26483/2162347

2 706,00 PLN brutto
2 200,00 PLN netto
300,67 PLN brutto/h
244,44 PLN netto/h

KREATOR
Przemysław
Oszczapiński

★★★★★

Ełk / mieszana (stacjonarna połączona z usługą zdalną)
Usługa szkoleniowa
9 h
20.08.2024 do 20.08.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Pracownicy administracji rządowej i samorządowej • Przedstawiciele innych instytucji publicznych • Osoby w instytucjach odpowiedzialne za bezpieczeństwo danych • Szkolenie jest skierowane do użytkowników komputerów i innych urządzeń podłączonych do Internetu, a nie do specjalistów od bezpieczeństwa IT
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	19-08-2024
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną)
Liczba godzin usługi	9
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

Szkolenie przygotowuje do samodzielnej obrony przed cyberatakami, a także pozwala rozpoznawać najczęściej praktykowane oszustwa. Celem szkolenia jest zapoznanie uczestników z podstawowymi problemami zabezpieczeń sieci

komputerowych, systemów komputerowych i aplikacji. Uczestnik pozna znaczenie i istotność haseł, zasady poruszania się po sieciach publicznych oraz cechy oszustwa mailowego i w social mediach.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po zakończeniu szkolenia uczestnik posługuje się wiedzą na temat:	Charakteryzuje socjotechniki wykorzystywane przez cyberprzestępców;	Test teoretyczny
	Charakteryzuje różne typy cyberataków i wie, jak się przed nimi chronić;	Test teoretyczny
	Zna najlepsze praktyki dotyczące tworzenia silnych haseł i ochrony danych osobowych;	Test teoretyczny
	Identyfikuje podejrzane aktywności online;	Test teoretyczny
Po zakończeniu szkolenia uczestnik posiada umiejętności:	Umiejętnie korzysta z bezpiecznych praktyk online, takich jak tworzenie silnych haseł i korzystanie z szyfrowania;	Test teoretyczny
	Omawia zagrożenia związane z cyberprzestępczości;	Test teoretyczny
	Podejmuje odpowiednie działania oraz zabezpieczenia w przypadku usiłowania cyberataku;	Test teoretyczny
	Umiejętnie korzysta z bezpiecznych praktyk w mediach społecznościowych;	Test teoretyczny
Po ukończeniu szkolenia uczestnik prezentuje postawę społeczną (nabywa i stosuje kompetencje społeczne):	Pracuje ze świadomością poziomu swojej wiedzy i umiejętności;	Test teoretyczny
	Definiuje swoje potrzeby w zakresie samokształcenia;	Test teoretyczny
	Korzysta z technologii w sposób odpowiedzialny i etyczny.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Zaświadczenie o zakończeniu udziału w usłudze rozwojowej zawiera informacje na temat zakresu usługi rozwojowej oraz opisu efektów uczenia się po ukończeniu usługi rozwojowej.

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

Zaświadczenie o zakończeniu udziału w usłudze rozwojowej zawiera informacje dotyczące spełnienia określonych wymagań.

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

Zaświadczenie o zakończeniu udziału w usłudze rozwojowej potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

1. 1. PODSTAWOWE ZAGADNIENIA BEZPIECZEŃSTWA INFORMACJI

- Bezpieczeństwo informacji w organizacji
- Prawne aspekty związane z bezpieczeństwem informacji, np. wymagania RODO, aktualne akty prawne
- Tworzenie kultury ochrony informacji

1. 2. ZAGROŻENIA BEZPIECZEŃSTWA INFORMACJI

- Cyberzagrożenia
- Przykłady kradzieży i wycieku danych
- Zagrożenia przy korzystaniu z internetu: poczta e-mail, strony www, serwisy społecznościowe

1. 3. HASŁO POWINNO BYĆ BEZPIECZNE

- Czy Twoje hasło do systemów informatycznych jest bezpieczne?
- Jak stworzyć silne hasło i łatwo je zapamiętać?
- Jak bezpiecznie chronić hasła?

1. 4. ATAKI HACKERSKIE / SOCJOTECHNICZNE

- Przykłady ataków socjotechnicznych: spoofing /phishing (testy na żywo)
- Podejrzane e-maile, czyli przykłady realnych zagrożeń, np. ransomware
- Informacje o podmiocie świadczącym usługę
- Cel usługi
- Szczegółowe informacje o usłudze
- Czy pendrive od znajomego może być niebezpieczny?
- Etyczny hacking, czyli jak skutecznie sprawdzić naszą organizację
- Skuteczne metody ochrony przed atakami

1. 5. POLITYKA BEZPIECZEŃSTWA

- Polityka Bezpieczeństwa Informacji jako skuteczne narzędzie ochrony informacji
- Skuteczne procedury ochrony danych

Harmonogram

Liczba przedmiotów/zajęć: 7

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 7 PODSTAWOWE ZAGADNIENIA BEZPIECZEŃSTWA INFORMACJI.	Przemysław Oszczapiński	20-08-2024	09:00	11:00	02:00
2 z 7 ZAGROŻENIA BEZPIECZEŃSTWA INFORMACJI.	Przemysław Oszczapiński	20-08-2024	11:00	13:30	02:30
3 z 7 Przerwa.	Przemysław Oszczapiński	20-08-2024	13:30	14:00	00:30
4 z 7 HASŁO POWINNO BYĆ BEZPIECZNE.	Przemysław Oszczapiński	20-08-2024	14:00	15:30	01:30
5 z 7 ATAKI HACKERSKIE / SOCJOTECHNICZNE.	Przemysław Oszczapiński	20-08-2024	15:30	17:00	01:30
6 z 7 POLITYKA BEZPIECZEŃSTWA.	Przemysław Oszczapiński	20-08-2024	17:00	17:30	00:30
7 z 7 Walidacja efektów uczenia się.	-	20-08-2024	17:30	18:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 706,00 PLN
Koszt przypadający na 1 uczestnika netto	2 200,00 PLN
Koszt osobogodziny brutto	300,67 PLN
Koszt osobogodziny netto	244,44 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Przemysław Oszczapiński

Specjalizacja to informatyka, bezpieczeństwo, szkolenia z zakresu informatyki, Druk 3D
Od 11.2005 – do chwili obecnej - Własna działalność gospodarcza "KREATOR" - obsługa informatyczna firm, szkolenia , doradztwo, wdrożenia.
Od 2010 – do 2016 Sygnity S.A. – Inżynier Serwisu – wsparcie i obsługa informatyczna placówek bankowych
Szkolenia i wdrożenia Informatyczne
Szkolenia i wdrożenia Social Media
Szkolenia i wdrożenia Druk 3D – egzaminator
Szkolenia i wdrożenia z zakresu bezpieczeństwa informacji – RODO
Szkolenia i wdrożenia z zakresu informatycznych systemów zarządzania.
Analizy szkoleniowe przedsiębiorstw.
Analizy finansowe przedsiębiorstw.

Wykształcenie wyższe: inż. informatyk
Wieloletnie doświadczenie w zakresie szkoleń i wdrożeń z zakresu informatyki, druku 3d, bezpieczeństwa danych i innych.
Od 2005roku w ramach własnej działalności gospodarczej oraz na zlecenie wielu firm m.in. Sygnity S.A., Asseco BS , oraz jednostek samorządu terytorialnego, sektora bankowego, rządowego, szkolnego, medycznego, biznesowego, a w szczególności szkół z trenu powiatu Ełckiego zajmuje się: wykonywaniem zleceń obsługi i szkoleń z zakresu informatyki, rozwiązywaniem problemów informatycznych, nawiązywaniem relacji i kontaktów z klientami, prowadzenia negocjacji, budowania wizerunku marki wśród klientów, bezpieczeństwa i ochrony danych osobowych, analizą marketingową, analizą przedsiębiorstwa, sprzedaży bezpośredniej, marketingu internetowego, marketingu bezpośredniego, i wielu innych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacja, materiały szkoleniowe w formie skryptu.

Warunki techniczne

Każda zgłoszona osoba musi dysponować komputerem lub innym urządzeniem mobilnym z wbudowaną kamerą i mikrofonem oraz dostępem do Internetu.

Minimalne wymagania dotyczące parametrów łącza sieciowego - nie mniejszego jak 3MB/s.

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów - przeglądarka Internet Explorer, Chrome, Firefox ,Opera lub aplikacja Microsoft Teams zainstalowana na komputerze z systemem Windows, Mac, Linux oraz na telefonie z systemem IOS lub Android

https://teams.microsoft.com/downloads#allDevicesSection

Adres

Ełk
19-300 Ełk
woj. warmińsko-mazurskie

Kontakt

Ewa Malinowska

E-mail kontakt4@szkoleniakreator.pl
Telefon (+48) 797 747 077