Możliwość dofinansowania

Cyber Security dla przedsiębiorstw - Phishing

Numer usługi 2024/08/22/171618/2274865

960,00 PLN brutto
780,49 PLN netto
120,00 PLN brutto/h
97,56 PLN netto/h

BLU PROFESSIONAL SKILLS INSTITUTE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Bydgoszcz / stacjonarna
Usługa szkoleniowa
8 h
10.12.2024 do 10.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Pracownicy średnich i dużych firm, zwłaszcza z działów IT, bezpieczeństwa informacji i administracji sieciowej. • Osoby korzystające z poczty elektronicznej i internetu w ramach obowiązków zawodowych. • Menedżerowie i decydenci odpowiedzialni za politykę bezpieczeństwa w firmie. • Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój;
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	09-12-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Szkolenie ma na celu zapoznanie uczestników z podstawowymi aspektami cyberbez-pieczeństwa, w szczególności z atakami typu Phishing. Kurs przygotowuje do rozpoznawania tego rodzaju ataków oraz pokazuje sposoby unikania ich. Szkolenie uczy również w jaki sposób można raportować wszelkie incydenty związane z atakami, które wykorzystują metody typu Phishing.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia różne rodzaje ataków phishingowych	Definiuje charakterystyczne cechy i metody używane w atakach phishingowych	Test teoretyczny
	Klasyfikuje ataki phishingowe w zależności od zastosowanych technik i narzędzi	Test teoretyczny
Identyfikuje zagrożenia związane z phishingiem	Analizuje potencjalne skutki ataków phishingowych dla organizacji	Test teoretyczny
	Wskazuje przykłady realnych zagrożeń związanych z phishingiem w kontekście bezpieczeństwa informacji	Test teoretyczny
Charakteryzuje metody ochrony przed phishingiem	Projektuje strategie ochrony przed phishingiem, w tym tworzenie silnych haseł i zarządzanie nimi	Test teoretyczny
	Ocenia skuteczność narzędzi anty-phishingowych oraz metod unikania phishingu	Test teoretyczny
Raportuje i reaguje na incydenty phishingowe	Dokumentuje procedury postępowania w przypadku wykrycia phishingu, zgodnie z polityką bezpieczeństwa firmy	Test teoretyczny
	Organizuje odpowiednie działania i komunikację wewnętrzną w odpowiedzi na zidentyfikowany incydent phishingowy	Test teoretyczny

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

Wprowadzenie do Phishingu:

Definicja phishingu. Cele i motywacje atakujących. Rodzaje phishingu.

Poznawanie technik Phishingowych:

Email phishing - charakterystyka wiadomości phishingowych. Elementy uwodzicielskiego e-maila. Złośliwe załączniki i linki.

Spoofing:

Falsyfikacja adresów e-mail i domen. Ukrywanie prawdziwego źródła ataku. Phishing na platformach społecznościowych

Rozpoznawanie i unikanie Phishingu:

Cechy charakterystyczne phishingowych wiadomości. Weryfikacja nadawcy
i adresu URL. Ostrzeżenia przeglądarek i narzędzi anty-phishingowych. Bezpieczne praktyki i zasady postępowania.

Atakowanie phishingowe:

Demonstracja typowych narzędzi używanych przez hakerów. Praktyczne ćwiczenia przeprowadzenia prostego ataku phishingowego. Omówienie skuteczności i konsekwencji takich ataków.

Raportowanie i reagowanie na phishing:

Jak zgłaszać podejrzane wiadomości. Zgłaszanie ataków wewnątrz organizacji. Reakcja na rzeczywiste przypadki phishingu. Ćwiczenia indywidualne i grupowe.

Bezpieczeństwo i edukacja użytkowników:

Wprowadzenie do programów szkoleniowych w organizacji. Jak kształtować świadomość wśród pracowników. Cykliczne szkolenia i testy phishingowe. Wykład i dyskusja moderowana.

Sesja Q&A

Sesja pytań od uczestników oraz dyskusja moderowana.

Harmonogram

Liczba przedmiotów/zajęć: 12

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Wprowadzenie do Phishingu	Jacek Kapelski	10-12-2024	08:00	08:45	00:45
2 z 12 Poznawanie technik Phishingowych	Jacek Kapelski	10-12-2024	08:45	09:30	00:45
3 z 12 Poznawanie technik Phishingowych (cd.)	Jacek Kapelski	10-12-2024	09:30	10:00	00:30
4 z 12 Spoofing	Jacek Kapelski	10-12-2024	10:00	11:00	01:00
5 z 12 Rozpoznawanie i unikanie Phishingu	Jacek Kapelski	10-12-2024	11:00	11:45	00:45
6 z 12 Rozpoznawanie i unikanie Phishingu (cd.)	Jacek Kapelski	10-12-2024	11:45	12:15	00:30
7 z 12 Atakowanie phishingowe	Jacek Kapelski	10-12-2024	12:45	13:45	01:00
8 z 12 Atakowanie phishingowe (cd.)	Jacek Kapelski	10-12-2024	13:45	14:15	00:30
9 z 12 Rapostowanie i reagowanie na phishing	Jacek Kapelski	10-12-2024	14:15	14:45	00:30
10 z 12 Raportowanie i reagowanie na phishing (cd.)	Jacek Kapelski	10-12-2024	14:45	15:15	00:30
11 z 12 Bezpieczeństwo i edukacja użytkowników	Jacek Kapelski	10-12-2024	15:30	16:00	00:30
12 z 12 Sesja Q&A	Jacek Kapelski	10-12-2024	16:00	16:15	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	960,00 PLN
Koszt przypadający na 1 uczestnika netto	780,49 PLN
Koszt osobogodziny brutto	120,00 PLN
Koszt osobogodziny netto	97,56 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jacek Kapelski

Jacek Kapelski to doświadczony ekspert w dziedzinie cyberbezpieczeństwa, z pasją do technologii informatycznych, którą rozwijał przez wiele lat pracy w różnych sektorach IT. Jego kariera zawodowa rozpoczęła się w dużej korporacji, gdzie pełnił rolę administratora IT, zdobywając bezcenne doświadczenie w zarządzaniu rozbudowanymi infrastrukturami sieciowymi i serwerowymi. Dzięki swojej wiedzy i zaangażowaniu, Jacek szybko stał się nieocenionym członkiem zespołu odpowiedzialnego za bezpieczeństwo i stabilność systemów informatycznych firmy.
Jacek jest certyfikowanym specjalistą Windows Server, co potwierdza jego głęboką znajomość technologii Microsoft oraz umiejętność zarządzania serwerami na najwyższym poziomie. Jego podejście do cyberbezpieczeństwa cechuje się precyzją i dbałością o najmniejsze detale, co sprawia, że potrafi przewidzieć potencjalne zagrożenia i skutecznie im przeciwdziałać. Jacek wierzy, że kluczem do sukcesu w dzisiejszym cyfrowym świecie jest ciągłe doskonalenie umiejętności oraz poszerzanie wiedzy, co przekłada na swoje szkolenia, które prowadzi z pełnym zaangażowaniem i profesjonalizmem.
Prywatnie Jacek jest entuzjastą nowinek technologicznych i chętnie dzieli się swoją wiedzą z innymi, pomagając im lepiej zrozumieć skomplikowane zagadnienia związane z cyberbezpieczeństwem. Na jego szkoleniach uczestnicy mogą liczyć nie tylko na solidną dawkę wiedzy teoretycznej, ale także na praktyczne wskazówki i rozwiązania, które mogą od razu wdrożyć w swoich firmach.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podczas szkolenia uczestnicy otrzymują: skrypt szkoleniowy, prezentację multimedialną, indywidualne długopisy, kartki i inne jednorazowe pomoce dydaktyczne a także certyfikat ukończenia szkolenia.

Warunki uczestnictwa

- Uczestnikiem szkolenia może być każda osoba, która spełnia wymagania wiekowe oraz posiada podstawową wiedzę na temat systemów Windows oraz klientów pocztowych.
- Uczestnik powinien posiadać własny komputer przenośny z systemem Windows, który umożliwi mu praktyczne wykonywanie ćwiczeń podczas szkolenia.
- Uczestnicy powinni zachować odpowiedni poziom kultury i szacunku wobec prowadzącego oraz innych uczestników szkolenia.
- Uczestnik zobowiązany jest do aktywnego uczestnictwa w szkoleniu i wykonywania zadań praktycznych, które są częścią programu szkolenia.

Informacje dodatkowe

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój

Adres

ul. Kijowska

85-703 Bydgoszcz

woj. kujawsko-pomorskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Michał Majcherek

E-mail szkolenia@bpsi.edu.pl

Telefon (+48) 537 770 040