Możliwość dofinansowania

Świadomość cyfrowego bezpieczeństwa (cyberbezpieczeństwo) - szkolenie.

Numer usługi 2024/11/07/148637/2400864

1 100,00 PLN brutto
1 100,00 PLN netto
183,33 PLN brutto/h
183,33 PLN netto/h

INSTYTUT ROZWOJU SEB-TEAM Piotr Jaworski

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
6 h
29.11.2024 do 29.11.2024

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	Szkolenie dedykowane dla kadry zarządzającej oraz pracowników administracyjnych, użytkowników komputerów i innych urządzeń z dostępem do Internetu oraz innych osób niebędących specjalistami z zakresu bezpieczeństwa IT. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	22-11-2024
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 szkolenia jest poszerzenie wiedzy Uczestników na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy oraz poza nim, rozpoznanie i zapobieganie ewentualnym zagrożeniom.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zna socjotechniki wykorzystywane przez cyberprzestępców.	Charakteryzuje socjotechniki wykorzystywane przez cyberprzestępców.	Test teoretyczny
Definiuje najważniejszych technik cyberataków.	Charakteryzuje najważniejsze techniki cyberataków.	Test teoretyczny
Rozpoznaje i zapobiega zagrożeniom związanym z cyberprzestępczością.	Omawia zagrożenia związane z cyberprzestępczością.	Test teoretyczny
Podejmuje odpowiednie działania oraz zabezpieczenia w przypadku usiłowania cyberataku.	Planuje odpowiednie działania w przypadku cyberataku.	Obserwacja w warunkach symulowanych

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. Wstęp
* co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa,
* polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola,
* incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować,
normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001.

2. Ataki „na człowieka" tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)
* ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców,
* sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty,
* jak rozpoznać, że jest się celem ataku socjotechnicznego,
* jak prawidłowo reagować na ataki socjotechniczne,
* jak i skąd atakujący zbierają dane na twój temat,
* miejsca, w których zostawiamy swoje dane świadomie i nieświadomie,
* jak świadomie udostępniać informacje w sieci.

3. Atak „na komputery" – objaśnienie
* ataki przez sieci bezprzewodowe (wifi, bluetooth, nfc),
* ataki przez pocztę e-mail (fałszywe e-maile),
* ataki przez strony www - jak nie dać się zainfekować, fałszywe strony,
* ataki przez komunikatory (skype, facebook),
* ataki przez telefon (fałszywe sms-y, przekierowania rozmów, itp.),
* ataki: phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów
* polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych,
* bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty,
* bezpieczna praca z urządzeniami mobilnymi (smartfon, laptop),
* problem aktualnego oprogramowania i kopii zapasowych,
* bezpieczna praca z pakietem biurowym Microsoft Office,
* bezpieczna praca z programem pocztowym,
* bezpieczna praca z przeglądarką internetową,
* zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty).

5. Aspekty prawne
* odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji,
* nieautoryzowane użycie systemów komputerowych,
* rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego,
* dane osobowe i dane wrażliwe.

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	1 100,00 PLN
Koszt przypadający na 1 uczestnika netto	1 100,00 PLN
Koszt osobogodziny brutto	183,33 PLN
Koszt osobogodziny netto	183,33 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe (autorskie skrypty, udostępnione w formie prezentacji) i piśmiennicze.

Każdy uczestnik szkolenia otrzyma imienny certyfikat ukończenia szkolenia.

Warunki uczestnictwa

Warunkiem uczestnictwa jest założenia konta na BUR i zapisanie się na usługę.

Informacje dodatkowe

Istnieje możliwość organizacji szkolenia dedykowanego, według Państwa zapotrzebowania w miejscu i czasie wskazanym przez Państwa. W razie zainteresowania ofertą indywidualną, prosimy o kontakt.

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

Szkolenie trwa 6 godzin zegarowych z uwzględnieniem czasu na przerwy.

Warunki techniczne

Szkolenie będzie prowadzone w formie zdalnej rzeczywistej na platformie ClickMeeting.

Kazdy zgłoszony uczestnik otzryma link do szkolenia.

Wymagania techniczne:
1. dostęp do Internetu (prędkość łącza - min. 2 Mbps),
2. przeglądarka internetowa (Chrome, Edge lub Firefox),

3. mikrofon, głośniki.

Kontakt

Magdalena Wielgosz

E-mail szkolenia@seb-team.pl
Telefon (+48) 661 991 681