Możliwość dofinansowania

Cyberbezpieczeństwo i Higiena w Sieci - usługa zdalna w czasie rzeczywistym

Numer usługi 2024/10/25/161638/2380166

4 950,00 PLN brutto
4 950,00 PLN netto
190,38 PLN brutto/h
190,38 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
26 h
23.11.2024 do 24.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP **Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.**
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	22-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	26
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa „Cyberbezpieczeństwo i Higiena w Sieci” ma na celu zwiększenie świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa 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 cyberbezpieczeństwem 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 skonfigurować bezpieczne połączenie sieciowe i stosuje 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?

Tak 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?

Tak 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?

Tak dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji

Program

DZIEŃ PIERWSZY (09:00 - 19:30)

1. **Podstawy cyberbezpieczeństwa**

- Wprowadzenie do Cyberbezpieczeństwa
- Istota i podstawowe terminy w zakresie cyberbezpieczeństwa
- Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA

1. **Cyberataki**

- najpopularniejsze ataki cybernetyczne
- ćwiczenie: phishing
- przestępstwa finansowe w przestrzeni cyfrowej

1. **Hasła i menadżer haseł**

- zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
- jak działa i jak wybrać menadżera haseł?

DZIEŃ DRUGI (09:00 - 19:30)

1. **Zabezpieczenia przed cyberatakami**

- dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
- szyfrowanie plików, folderów i pendrive'ów w praktyce
- zastrzeż swój PESEL
- jak robić backup danych?
- jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
- co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
- co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna
- jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
- Podsumowanie i najlepsze praktyki

1. **Walidacja**

- Test pisemny

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

Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 22 wprowadzenie do szkolenia	Wojciech Graczyk	23-11-2024	09:00	09:45	00:45
2 z 22 istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Wojciech Graczyk	23-11-2024	09:45	11:00	01:15
3 z 22 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Wojciech Graczyk	23-11-2024	11:00	12:30	01:30
4 z 22 Przerwa	Wojciech Graczyk	23-11-2024	12:30	13:00	00:30
5 z 22 najpopularniejsze ataki cybernetyczne	Wojciech Graczyk	23-11-2024	13:00	14:00	01:00
6 z 22 ćwiczenie: phishing	Wojciech Graczyk	23-11-2024	14:00	15:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 22 Przerwa	Wojciech Graczyk	23-11-2024	15:00	15:30	00:30
8 z 22 przestępstwa finansowe w przestrzeni cyfrowej	Wojciech Graczyk	23-11-2024	15:30	16:30	01:00
9 z 22 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Wojciech Graczyk	23-11-2024	16:30	18:00	01:30
10 z 22 jak działa i jak wybrać menadżera haseł?	Wojciech Graczyk	23-11-2024	18:00	19:30	01:30
11 z 22 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Wojciech Graczyk	24-11-2024	09:00	10:00	01:00
12 z 22 szyfrowanie plików,folderów i pendrive'ów w praktyce	Wojciech Graczyk	24-11-2024	10:00	11:00	01:00
13 z 22 Przerwa	Wojciech Graczyk	24-11-2024	11:00	11:30	00:30
14 z 22 zastrzeż swój PESEL	Wojciech Graczyk	24-11-2024	11:30	12:00	00:30
15 z 22 jak robić backup danych?	Wojciech Graczyk	24-11-2024	12:00	12:30	00:30
16 z 22 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Wojciech Graczyk	24-11-2024	12:30	14:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 22 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów	Wojciech Graczyk	24-11-2024	14:00	15:00	01:00
18 z 22 przerwa	Wojciech Graczyk	24-11-2024	15:00	15:30	00:30
19 z 22 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Wojciech Graczyk	24-11-2024	15:30	16:30	01:00
20 z 22 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Wojciech Graczyk	24-11-2024	16:30	17:30	01:00
21 z 22 podsumowanie	Wojciech Graczyk	24-11-2024	17:30	18:30	01:00
22 z 22 Test	-	24-11-2024	18:30	19:30	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 950,00 PLN
Koszt przypadający na 1 uczestnika netto	4 950,00 PLN
Koszt osobogodziny brutto	190,38 PLN
Koszt osobogodziny netto	190,38 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Wojciech Graczyk

Wojciech Graczyk – trener kompetencji miękkich oraz mentor w zakresie wystąpień publicznych z 4-letnim stażem.
Włożył istotny wpływ w rozwój w poznańskiej filii organizacji zrzeszającej mówców Toastmasters International.
W ciągu ostatnich trzech lat przeprowadził ponad 1850 godzin zegarowych usług szkoleniowych w zakresie kompetencji miękkich, a także występował w roli prelegenta jako ekspert w zakresie wystąpień publicznych na następujących konferencjach:
– Hackathon Planet-ON'21 Smart & Green Industry
– Spotkanie networkingowe Rozwijalni Kobiet
– Spotkanie networkingowe Biznesowe Śniadania u Ani Diller
oraz w zakresie kompetencji miękkich:
– Konferencja Believe 2021 r.
– spotkanie inauguracyjne Szkoły Liderów Centrum PPP.
Cały czas podnosi swoje kompetencje, uczestnicząc w szkoleniach, kursach i konferencjach w zakresie komunikacji interpersonalnej, wystąpień publicznych i sprzedaży.
Certyfikaty:
– Competent Leader (Toastmasters International);
– Competent Communicator (Toastmasters International);
– Certyfikat uprawniający do prowadzenia szkoleń kwalifikacji zawodowej przedstawiciel handlowy (GCCE sp. z o.o.);
– Certyfikat uprawniający do prowadzenia szkoleń kwalifikacji zawodowej technik sprzedaży (GCCE sp. z o.o.).
Przeprowadził również ponad 200 godzin szkoleń w zakresie bezpieczeństwa cyfrowego oraz uzyskał certyfikat w zakresie zaawansowanych technik cyberbezpieczeństwa, ze szczególnym uwzględnieniem prawnych aspektów cyberbezpieczeństwa oraz ustalania haseł.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany na maila każdego z czestników szkolenia. Będą to podręczniki wraz z prezentacjami danego szkolenia.

Informacje dodatkowe

Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku testu sprawdzającego wiedzę , który odbędzie się na ostatnich zajęciach. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest pozytywny wynik testu końcowego oraz frekwencja na minimalnym poziomie 80%.

Warunki techniczne

1. platforma komunikacyjna - microsoft teams

2. wymagania sprzętowe: komputer stacjonarny/laptop, kamera, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/MacOS High Sierra, min 2 GB pamięci RAM, pamięć dysku minimum 10GB,

3. sieć: łącze internetowe minimum 50 kb/s,

4. system operacyjny minimum Windows XP/MacOS High Sierra, przeglądarka internetowa (marka nie ma znaczenia)

5. okres ważności linku: od 1 h przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny po zakończeniu szkoleń w dniu ostatnim

Kontakt

Wojciech Graczyk

E-mail wojciech.graczyk@korycki-graczyk.pl
Telefon (+48) 698 291 420