Możliwość dofinansowania

Cyberbezpieczeństwo i Higiena w Sieci - usługa zdalna w czasie rzeczywistym

Numer usługi 2024/07/17/161638/2225283

4 950,00 PLN brutto
4 950,00 PLN netto
206,25 PLN brutto/h
206,25 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
02.09.2024 do 04.09.2024

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	01-09-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
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

1. Podstawy Cyberbezpieczeństwa oraz Higiena Cyfrowa - Praktyczne Aspekty

1. Wprowadzenie do Cyberbezpieczeństwa
2. Zagrożenia w sieci i ich wpływ na firmy MSP
3. Podstawowe terminy i koncepcje (np. malware, phishing, ransomware)
4. Znaczenie higieny cyfrowej w kontekście biznesowym
5. Hasła i zarządzanie nimi

2. Zaawansowane Techniki Ochrony

1. Bezpieczne korzystanie z Internetu i e-maila
2. Ochrona przed phishingiem i innymi formami socjotechniki
3. Podstawy bezpiecznej pracy zdalnej
4. Zaawansowana ochrona przed złośliwym oprogramowaniem
5. Szyfrowanie danych i komunikacji
6. Bezpieczeństwo sieci firmowych i domowych

3. Przygotowanie do Realnych Wyzwań

1. Wprowadzenie do bezpieczeństwa urządzeń mobilnych
2. Tworzenie i wdrażanie polityki bezpieczeństwa w firmie
3. Symulacje ataków cybernetycznych i reakcje

4. Przygotowanie planu reagowania na incydenty
5. Podsumowanie i najlepsze praktyki
6. 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: 23

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 23 Wprowadzenie do Cyberbezpieczeństwa	Wojciech Graczyk	02-09-2024	08:00	09:00	01:00
2 z 23 Zagrożenia w sieci i ich wpływ na firmy MSP	Wojciech Graczyk	02-09-2024	09:00	10:30	01:30
3 z 23 Przerwa	Wojciech Graczyk	02-09-2024	10:30	11:00	00:30
4 z 23 Podstawowe terminy i koncepcje (np. malware, phishing, ransomware)	Wojciech Graczyk	02-09-2024	11:00	12:30	01:30
5 z 23 Przerwa	Wojciech Graczyk	02-09-2024	12:30	13:00	00:30
6 z 23 Znaczenie higieny cyfrowej w kontekście biznesowym	Wojciech Graczyk	02-09-2024	13:00	14:00	01:00
7 z 23 Hasła i zarządzanie nimi	Wojciech Graczyk	02-09-2024	14:00	15:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 23 Zaawansowana ochrona przed złośliwym oprogramowaniem	Wojciech Graczyk	03-09-2024	08:00	09:00	01:00
9 z 23 Bezpieczne korzystanie z Internetu i e-maila	Wojciech Graczyk	03-09-2024	09:00	10:30	01:30
10 z 23 Przerwa	Wojciech Graczyk	03-09-2024	10:30	11:00	00:30
11 z 23 Ochrona przed phishingiem i innymi formami socjotechniki	Wojciech Graczyk	03-09-2024	11:00	12:30	01:30
12 z 23 Przerwa	Wojciech Graczyk	03-09-2024	12:30	13:00	00:30
13 z 23 Podstawy bezpiecznej pracy zdalnej	Wojciech Graczyk	03-09-2024	13:00	13:30	00:30
14 z 23 Szyfrowanie danych i komunikacji	Wojciech Graczyk	03-09-2024	13:30	14:00	00:30
15 z 23 Bezpieczeństwo sieci firmowych i domowych	Wojciech Graczyk	03-09-2024	14:00	15:00	01:00
16 z 23 Wprowadzenie do bezpieczeństwa urządzeń mobilnych	Wojciech Graczyk	04-09-2024	08:00	09:00	01:00
17 z 23 Tworzenie i wdrażanie polityki bezpieczeństwa w firmie	Wojciech Graczyk	04-09-2024	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 23 Przerwa	Wojciech Graczyk	04-09-2024	10:30	11:00	00:30
19 z 23 Symulacje ataków cybernetycznych i reakcje	Wojciech Graczyk	04-09-2024	11:00	12:30	01:30
20 z 23 Przerwa	Wojciech Graczyk	04-09-2024	12:30	13:00	00:30
21 z 23 Przygotowanie planu reagowania na incydenty	Wojciech Graczyk	04-09-2024	13:00	13:30	00:30
22 z 23 Podsumowanie i najlepsze praktyki	Wojciech Graczyk	04-09-2024	13:30	14:00	00:30
23 z 23 Test pisemny	-	04-09-2024	14:00	15:00	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	206,25 PLN
Koszt osobogodziny netto	206,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Wojciech Graczyk

Wojciech Graczyk – trener wystąpień publicznych z 3-letnim doświadczeniem oraz prezes zarządu firmy szkoleniowo-wydawniczej KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. Włożył istotny wpływ w rozwój w poznańskiej filii organizacji zrzeszającej mówców Toastmasters International. Autor książki pt. „Wystąpienia publiczne”, w której w prosty sposób przekazuje swoją wiedzę oraz doświadczenie z tematyki wystąpień publicznych. Pełni funkcję prezesa zarządu Fundacji „Postaw na Przedsiębiorczość”, której celem jest popularyzacja przedsiębiorczości wśród młodzieży. Wierzy, że siła tkwi w prostocie i w mądrej pracy. Uważa, że wystąpienia publiczne to jedna z kompetencji XXI wieku, której może nauczyć się każdy. Jego motto życiowe brzmi: „Marzenia się nie spełniają, marzenia są po to, by je spełniać”. Szkoleniowiec ma doświadczenie w prowadzeniu szkoleń dla MMŚP oraz osób indywidualnych głownie z zakresu efektywnej komunikacji, automotywacji oraz marketingu internetowego. Jego specjalnością są szkolenia menadżerskie przygotowujące uczestników do objęcia stanowiska kierowniczego. Trener posiada doświadczenie min 120h w wymaganej tematyce w ciągu ostatnich 24 m-cy przed szkoleniem

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%.

Przerwy ustalane są z uczestnikami przed rozpoczęciem szkolenia.

Warunki techniczne

1. platforma komunikacyjna - microsoft teams
2. wymagania sprzętowe: komputer stacjonarny/laptop, 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.szkolenia@interia.pl

Telefon (+48) 698 291 420