Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo.

Numer usługi 2024/09/25/161638/2327175

7 500,00 PLN brutto
7 500,00 PLN netto
187,50 PLN brutto/h
187,50 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
04.11.2024 do 08.11.2024

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	03-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa 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

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 1

1. wprowadzenie do szkolenia
2. audyt cyberbezpieczeństwa
3. istota i podstawowe terminy w zakresie cyberbezpieczeństwa
4. podstawy prawne cyberbezpieczeństwa i zalecenia ENISA
5. najpopularniejsze ataki cybernetyczne
6. ćwiczenie: phishing

Dzień 2

1. przestępstwa finansowe w przestrzeni cyfrowej
2. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
3. jak działa i jak wybrać menadżera haseł?
4. dlaczego tak często hakerzy łamią hasła?
5. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
6. szyfrowanie plików,folderów i pendrive'ów w praktyce

Dzień 3

1. jak chronić dane osobowe zgodnie z RODO?
2. zastrzeż swój PESEL
3. jak robić backup danych?
4. dlaczego warto korzystać z„chmury”?
5. wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?

Dzień 4

1. jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
2. co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
3. co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna
4. jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?

Dzień 5

1. jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
2. ćwiczenie grupowe: symulacje ataków cybernetycznych
3. narzędzia i programy wzmacniające bezpieczeństwo cyfrowe
4. Podsumowanie
5. Test

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

W ciągu dnia zostały uwzględnione 2 przerwy po 30 minut które nie są wliczane do czasu trwania usługi.

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: 26

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 wprowadzenie do szkolenia	Mateusz Szczygieł	04-11-2024	08:00	08:45	00:45
2 z 26 audyt cyberbezpieczeństwa	Mateusz Szczygieł	04-11-2024	08:45	10:00	01:15
3 z 26 istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Mateusz Szczygieł	04-11-2024	10:00	11:30	01:30
4 z 26 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Mateusz Szczygieł	04-11-2024	11:30	13:00	01:30
5 z 26 najpopularniejsze ataki cybernetyczne	Mateusz Szczygieł	04-11-2024	13:00	14:00	01:00
6 z 26 ćwiczenie: phishing	Mateusz Szczygieł	04-11-2024	14:00	15:00	01:00
7 z 26 przestępstwa finansowe w przestrzeni cyfrowej	Mateusz Szczygieł	05-11-2024	08:00	08:45	00:45
8 z 26 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Mateusz Szczygieł	05-11-2024	08:45	10:00	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 26 jak działa i jak wybrać menadżera haseł?	Mateusz Szczygieł	05-11-2024	10:00	11:30	01:30
10 z 26 dlaczego tak często hakerzy łamią hasła?	Mateusz Szczygieł	05-11-2024	11:30	13:00	01:30
11 z 26 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Mateusz Szczygieł	05-11-2024	13:00	14:00	01:00
12 z 26 szyfrowanie plików,folderów i pendrive'ów w praktyce	Mateusz Szczygieł	05-11-2024	14:00	15:00	01:00
13 z 26 jak chronić dane osobowe zgodnie z RODO?	Mateusz Szczygieł	06-11-2024	08:00	08:45	00:45
14 z 26 zastrzeż swój PESEL	Mateusz Szczygieł	06-11-2024	08:45	10:00	01:15
15 z 26 jak robić backup danych?	Mateusz Szczygieł	06-11-2024	10:00	11:30	01:30
16 z 26 dlaczego warto korzystać z„chmury”?	Mateusz Szczygieł	06-11-2024	11:30	13:00	01:30
17 z 26 wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?	Mateusz Szczygieł	06-11-2024	13:00	15:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 26 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Mateusz Szczygieł	07-11-2024	08:00	09:00	01:00
19 z 26 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów	Mateusz Szczygieł	07-11-2024	09:00	11:00	02:00
20 z 26 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Mateusz Szczygieł	07-11-2024	11:00	13:00	02:00
21 z 26 jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?	Mateusz Szczygieł	07-11-2024	13:00	15:00	02:00
22 z 26 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Mateusz Szczygieł	08-11-2024	08:00	10:00	02:00
23 z 26 ćwiczenie grupowe: symulacje ataków cybernetycznych	Mateusz Szczygieł	08-11-2024	10:00	12:00	02:00
24 z 26 narzędzia i programy wzmacniające bezpieczeństwo cyfrowe	Mateusz Szczygieł	08-11-2024	12:00	13:00	01:00
25 z 26 Podsumowanie	Mateusz Szczygieł	08-11-2024	13:00	14:00	01:00
26 z 26 Test	-	08-11-2024	14:00	15:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 500,00 PLN
Koszt przypadający na 1 uczestnika netto	7 500,00 PLN
Koszt osobogodziny brutto	187,50 PLN
Koszt osobogodziny netto	187,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Mateusz Szczygieł

Od 2012 roku logistyk w firmie WZPOW Kwidzyn Sp. z.o.o, gdzie jego głównym obowiązkiem był kontakt telefoniczny/zdalny z kontrahentami w celu zawarcia umów w sprzedaży hurtowej produktów spożywczych. Był także odpowiedzialny za odbiór i dostawę produktów spożywczych, czyli za prawidłową pracę przewoźników. Jako logistyk zdobył dużą wiedzę teoretyczną i praktyczną w sprzedaży i obsłudze klienta, także poszerzył umiejętności praktyczne w obsłudze programów pakietu Office 365. Od 2020 roku specjalista IT/analityk branżowy w firmie RuccolPublicRelations Dorota Szczygieł. Trener od 2021 roku w RuccolPublicRelations Sp. z o.o., tworzący swoje autorskie programy i materiały szkoleniowe. Szkoleniowiec (ponad 300 h szkoleń przeprowadzonych wewnętrznych w firmie oraz dla klientów firmy); zajmuję się tworzeniem stron internetowych, dba o bezpieczeństwo kont firmowych, prowadzi szkolenia indywidualne oraz grupowe w kilku następujących obszarach tematycznych: - organizacja i zarządzanie firmą; - strategie marketingowe, reklama, PR; - negocjacje, komunikacja, perswazja; - analizy finansowe, controlling; - pozyskiwanie i obsługa klienta; - procesy rekrutacyjne i selekcyjne; - kierowanie i szkolenie zespołów pracowniczych. Trener posiada wiedzę w zakresie teoretycznych aspektów zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie. Bardzo dobrze potrafi obsługiwać programy do komunikacji zdalnej np. MS Teams, Zoom, ClickMeeting. Wykształcenie: średnie

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przesłane drogą mailową w formacie pdf. Uczestnik otrzyma:

1. skrypty

2. materiały video

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