Możliwość dofinansowania

Cyberbezpieczeństwo — usługa szkoleniowa

Numer usługi 2025/03/04/180138/2596933

4 500,00 PLN brutto
4 500,00 PLN netto
140,63 PLN brutto/h
140,63 PLN netto/h

HC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
32 h
02.04.2025 do 05.04.2025

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	20
Data zakończenia rekrutacji	01-04-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

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 z wynikiem generowanym automatycznie
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 z wynikiem generowanym automatycznie
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Test teoretyczny z wynikiem generowanym automatycznie
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 z wynikiem generowanym automatycznie
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 z wynikiem generowanym automatycznie

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
7. przestępstwa finansowe w przestrzeni cyfrowej

Dzień 2:

1. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
2. jak działa i jak wybrać menadżera haseł?
3. dlaczego tak często hakerzy łamią hasła?
4. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
5. szyfrowanie plików,folderów i pendrive'ów w praktyce
6. jak chronić dane osobowe zgodnie z RODO?
7. zastrzeż swój PESEL

Dzień 3:

1. jak robić backup danych?
2. dlaczego warto korzystać z„chmury”?
3. wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?
4. jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
5. co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
6. co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna

Dzień 4:

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

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

Przerwy ujęte w harmonogramie nie są wliczane w czas trwania szkolenia.

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: 34

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 34 wprowadzenie do szkolenia - chat	Dominik Hamera	02-04-2025	08:00	09:00	01:00
2 z 34 audyt cyberbezpieczeństwa - chat	Dominik Hamera	02-04-2025	09:00	10:00	01:00
3 z 34 Przerwa	Dominik Hamera	02-04-2025	10:00	10:30	00:30
4 z 34 istota i podstawowe terminy w zakresie cyberbezpieczeństwa - chat	Dominik Hamera	02-04-2025	10:30	11:30	01:00
5 z 34 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA - chat	Dominik Hamera	02-04-2025	11:30	12:30	01:00
6 z 34 Przerwa	Dominik Hamera	02-04-2025	12:30	13:00	00:30
7 z 34 najpopularniejsze ataki cybernetyczne - chat	Dominik Hamera	02-04-2025	13:00	14:00	01:00
8 z 34 ćwiczenie: phishing - ćwiczenia	Dominik Hamera	02-04-2025	14:00	15:00	01:00
9 z 34 przestępstwa finansowe w przestrzeni cyfrowej - chat	Dominik Hamera	03-04-2025	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 34 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego - chat	Dominik Hamera	03-04-2025	09:00	10:00	01:00
11 z 34 Przerwa	Dominik Hamera	03-04-2025	10:00	10:30	00:30
12 z 34 jak działa i jak wybrać menadżera haseł? - chat	Dominik Hamera	03-04-2025	10:30	11:30	01:00
13 z 34 dlaczego tak często hakerzy łamią hasła? - chat	Dominik Hamera	03-04-2025	11:30	12:30	01:00
14 z 34 Przerwa	Dominik Hamera	03-04-2025	12:30	13:00	00:30
15 z 34 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce - ćwiczenia	Dominik Hamera	03-04-2025	13:00	14:00	01:00
16 z 34 szyfrowanie plików,folderów i pendrive'ów w praktyce - ćwiczenia	Dominik Hamera	03-04-2025	14:00	14:30	00:30
17 z 34 jak chronić dane osobowe zgodnie z RODO? - chat	Dominik Hamera	03-04-2025	14:30	15:00	00:30
18 z 34 zastrzeż swój PESEL - chat	Dominik Hamera	04-04-2025	08:00	09:00	01:00
19 z 34 jak robić backup danych? - ćwiczenia	Dominik Hamera	04-04-2025	09:00	10:00	01:00
20 z 34 Przerwa	Dominik Hamera	04-04-2025	10:00	10:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 34 dlaczego warto korzystać z„chmury”? - chat	Dominik Hamera	04-04-2025	10:30	11:30	01:00
22 z 34 wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać? - chat	Dominik Hamera	04-04-2025	11:30	12:30	01:00
23 z 34 Przerwa	Dominik Hamera	04-04-2025	12:30	13:00	00:30
24 z 34 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN - chat	Dominik Hamera	04-04-2025	13:00	14:00	01:00
25 z 34 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów - chat	Dominik Hamera	04-04-2025	14:00	15:00	01:00
26 z 34 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna - chat	Dominik Hamera	05-04-2025	08:00	09:00	01:00
27 z 34 jak wzmocnić kulturę cyberbezpieczeństwa w organizacji? - chat	Dominik Hamera	05-04-2025	09:00	10:00	01:00
28 z 34 Przerwa	Dominik Hamera	05-04-2025	10:00	10:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
29 z 34 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? - chat	Dominik Hamera	05-04-2025	10:30	11:30	01:00
30 z 34 ćwiczenie grupowe: symulacje ataków cybernetycznych - ćwiczenia	Dominik Hamera	05-04-2025	11:30	12:30	01:00
31 z 34 Przerwa	Dominik Hamera	05-04-2025	12:30	13:00	00:30
32 z 34 narzędzia i programy wzmacniające bezpieczeństwo cyfrowe - chat	Dominik Hamera	05-04-2025	13:00	14:00	01:00
33 z 34 Podsumowanie - chat	Dominik Hamera	05-04-2025	14:00	14:30	00:30
34 z 34 Test teoretyczny z wynikiem generowanym automatyczne - walidacja	Dominik Hamera	05-04-2025	14:30	15:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 500,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	140,63 PLN
Koszt osobogodziny netto	140,63 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Dominik Hamera

Posiada 9 lat doświadczenia w pozyskiwaniu funduszy. Firma, którą prowadzi pozyskała ponad 100 000 000 zł dla swoich klientów. Specjalizuje się w doradztwie biznesowym, unijnym, w zakresie pozyskiwania funduszy zewnętrznych, zarządzaniu, procesami motywacyjnymi. Prowadzi szkolenia z indywidualne oraz grupowe m.in. „Motywacja pracowników w zarządzaniu zespołem" „Zarządzanie procesami w biznesie" „Budowanie motywacji i zaangażowania pracowników" „Pozyskiwanie funduszy unijnych", „Automotywacja pracowników".
Od ponad 8 lat prowadzi przedsiębiorstwo doradcze w zakresie pozyskiwania funduszy unijnych, zarządzania strategicznego w firmie. Zajmuje się oceną i kontroli systemu organizacji procesów zachodzących w firmie.
Posiada wykształcenie wyższe zdobyte na AWF Warszawa, kierunek wychowanie fizyczne, specjalizacja menedżer. Współpracuje z Ministerstwem Sportu i Turystyki.
Przeprowadził ponad 1000 godzin szkoleń dla firm z sektora MŚP oraz organizacji pozarządowych. Współpracuje z podmiotami ekonomii społecznej. Prowadzi diagnozy potrzeb rozwojowych oraz szkoleniowych. Prowadzi szkolenia dla właścicieli firm oraz kadry kierowniczej z zarządzania strategicznego w firmie, zarządzania procesami oraz motywacyjne.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

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

1. skrypty

2. materiały video

Informacje dodatkowe

Do wybranej metody walidacji nie jest potrzebny walidator, ponieważ uczestnicy dostają link do wypełnienia testu

Warunki techniczne

1. platforma komunikacyjna – Microsoft Teams.

2. wymagania sprzętowe: komputer stacjonarny/laptop, mikrofon, kamera, 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

Jakub Mencfeld

E-mail jakubhg40@gmail.com
Telefon (+48) 661 336 370