Możliwość dofinansowania

Cyberbezpieczeństwo — usługa szkoleniowa

Numer usługi 2025/07/17/180138/2885020

4 000,00 PLN brutto
4 000,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

HC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★ 5,0 / 5

644 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
01.09.2025 do 05.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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	31-08-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
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

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

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

Dzień 2:

1. ćwiczenie: phishing
2. przestępstwa finansowe w przestrzeni cyfrowej
3. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
4. jak działa i jak wybrać menadżera haseł?
5. dlaczego tak często hakerzy łamią hasła?

Dzień 3:

1. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
2. szyfrowanie plików,folderów i pendrive'ów w praktyce
3. jak chronić dane osobowe zgodnie z RODO?
4. zastrzeż swój PESEL
5. jak robić backup danych?

Dzień 4:

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

Dzień 5:

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 teoretyczny z wynikiem generowanym automatycznie - walidacja

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: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 wprowadzenie do szkolenia	Joanna Dubisz	01-09-2025	08:00	09:00	01:00
2 z 36 audyt cyberbezpieczeństwa	Joanna Dubisz	01-09-2025	09:00	10:00	01:00
3 z 36 Przerwa	Joanna Dubisz	01-09-2025	10:00	10:30	00:30
4 z 36 istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Joanna Dubisz	01-09-2025	10:30	11:30	01:00
5 z 36 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Joanna Dubisz	01-09-2025	11:30	12:30	01:00
6 z 36 Przerwa	Joanna Dubisz	01-09-2025	12:30	13:00	00:30
7 z 36 najpopularniejsze ataki cybernetyczne	Joanna Dubisz	01-09-2025	13:00	15:00	02:00
8 z 36 ćwiczenie: phishing	Joanna Dubisz	02-09-2025	08:00	09:00	01:00
9 z 36 przestępstwa finansowe w przestrzeni cyfrowej	Joanna Dubisz	02-09-2025	09:00	10:00	01:00
10 z 36 Przerwa	Joanna Dubisz	02-09-2025	10:00	10:30	00:30
11 z 36 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Joanna Dubisz	02-09-2025	10:30	11:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 36 jak działa i jak wybrać menadżera haseł?	Joanna Dubisz	02-09-2025	11:30	12:30	01:00
13 z 36 Przerwa	Joanna Dubisz	02-09-2025	12:30	13:00	00:30
14 z 36 dlaczego tak często hakerzy łamią hasła?	Joanna Dubisz	02-09-2025	13:00	15:00	02:00
15 z 36 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Joanna Dubisz	03-09-2025	08:00	09:00	01:00
16 z 36 szyfrowanie plików,folderów i pendrive'ów w praktyce	Joanna Dubisz	03-09-2025	09:00	10:00	01:00
17 z 36 Przerwa	Joanna Dubisz	03-09-2025	10:00	10:30	00:30
18 z 36 jak chronić dane osobowe zgodnie z RODO?	Joanna Dubisz	03-09-2025	10:30	11:30	01:00
19 z 36 zastrzeż swój PESEL	Joanna Dubisz	03-09-2025	11:30	12:30	01:00
20 z 36 Przerwa	Joanna Dubisz	03-09-2025	12:30	13:00	00:30
21 z 36 jak robić backup danych?	Joanna Dubisz	03-09-2025	13:00	15:00	02:00
22 z 36 dlaczego warto korzystać z„chmury”?	Joanna Dubisz	04-09-2025	08:00	09:00	01:00
23 z 36 wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?	Joanna Dubisz	04-09-2025	09:00	10:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 36 Przerwa	Joanna Dubisz	04-09-2025	10:00	10:30	00:30
25 z 36 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Joanna Dubisz	04-09-2025	10:30	11:30	01:00
26 z 36 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów	Joanna Dubisz	04-09-2025	11:30	12:30	01:00
27 z 36 Przerwa	Joanna Dubisz	04-09-2025	12:30	13:00	00:30
28 z 36 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Joanna Dubisz	04-09-2025	13:00	15:00	02:00
29 z 36 jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?	Joanna Dubisz	05-09-2025	08:00	09:00	01:00
30 z 36 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Joanna Dubisz	05-09-2025	09:00	10:00	01:00
31 z 36 Przerwa	Joanna Dubisz	05-09-2025	10:00	10:30	00:30
32 z 36 ćwiczenie grupowe: symulacje ataków cybernetycznych	Joanna Dubisz	05-09-2025	10:30	11:30	01:00
33 z 36 narzędzia i programy wzmacniające bezpieczeństwo cyfrowe	Joanna Dubisz	05-09-2025	11:30	12:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
34 z 36 Przerwa	Joanna Dubisz	05-09-2025	12:30	13:00	00:30
35 z 36 Podsumowanie	Joanna Dubisz	05-09-2025	13:00	14:00	01:00
36 z 36 Test teoretyczny z wynikiem generowanym automatycznie - walidacja	Joanna Dubisz	05-09-2025	14:00	15:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 000,00 PLN
Koszt przypadający na 1 uczestnika netto	4 000,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Joanna Dubisz

Joanna Dubisz to doświadczona szkoleniowiec specjalizująca się w obszarach sprzedaży oraz obsługi klienta. Swoją edukację rozpoczęła od ukończenia liceum profilowanego o kierunku socjalnym, co dało jej solidne podstawy w zakresie pracy z ludźmi i zrozumienia ich potrzeb. Karierę szkoleniowca rozpoczęła w 2018 roku i od tego czasu nieustannie rozwija swoje umiejętności, zdobywając liczne certyfikaty, w tym z zakresu pracy w zespole oraz radzenia sobie z trudnymi klientami. Joanna zrealizowała ponad 300 godzin szkoleń, prowadząc warsztaty zarówno dla firm, jak i klientów indywidualnych. Jej szkolenia cechują się praktycznym podejściem i są dostosowane do rzeczywistych potrzeb uczestników, dzięki czemu potrafi efektywnie przekazywać wiedzę, jednocześnie budując zaangażowanie i motywację w zespole. Dzięki swojemu doświadczeniu oraz umiejętnościom w zarządzaniu relacjami z klientem, Joanna cieszy się opinią eksperta w zakresie

rozwijania kompetencji sprzedażowych i obsługi klienta." Joanna jest specjalistką do spraw zarządzania cyberbezpieczeństwem w firmach.

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.

Szkolenie skierowane do osób korzystających z bonów rozwojowych

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

Dominik Hamera

E-mail office@hameracapital.eu
Telefon (+48) 888 677 422