



Cyberbezpieczeństwo – usługa szkoleniowa

Numer usługi 2025/05/09/180138/2735667

4 000,00 PLN brutto

4 000,00 PLN netto

100,00 PLN brutto/h

100,00 PLN netto/h

HC SPÓŁKA Z
OGRA NICZONĄ
ODPOWIEDZIALNOŚ
CIĄ



📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 40 h

📅 02.06.2025 do 06.06.2025

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	10
Data zakończenia rekrutacji	01-06-2025
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, 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

Dzień 2:

1. ćwiczenie: phishing
2. przestępstwa finansowe w przestrzeni cyfrowej
3. zasady ustalania hasła zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
4. jak działa i jak wybrać menadżera hasła?
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	Dominik Hamera	02-06-2025	14:00	14:45	00:45
2 z 36 audyt cyberbezpieczeństwa	Dominik Hamera	02-06-2025	14:45	16:00	01:15
3 z 36 Przerwa	Dominik Hamera	02-06-2025	16:00	16:30	00:30
4 z 36 istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Dominik Hamera	02-06-2025	16:30	17:30	01:00
5 z 36 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Dominik Hamera	02-06-2025	17:30	19:00	01:30
6 z 36 Przerwa	Dominik Hamera	02-06-2025	19:00	19:30	00:30
7 z 36 najpopularniejsze ataki cybernetyczne	Dominik Hamera	02-06-2025	19:30	21:00	01:30
8 z 36 ćwiczenie: phishing	Dominik Hamera	03-06-2025	14:00	14:45	00:45
9 z 36 przestępstwa finansowe w przestrzeni cyfrowej	Dominik Hamera	03-06-2025	14:45	16:00	01:15
10 z 36 Przerwa	Dominik Hamera	03-06-2025	16:00	16:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 36 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Dominik Hamera	03-06-2025	16:30	17:30	01:00
12 z 36 jak działa i jak wybrać menadżera haseł?	Dominik Hamera	03-06-2025	17:30	19:00	01:30
13 z 36 Przerwa	Dominik Hamera	03-06-2025	19:00	19:30	00:30
14 z 36 dlaczego tak często hakerzy łamią hasła?	Dominik Hamera	03-06-2025	19:30	21:00	01:30
15 z 36 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Dominik Hamera	04-06-2025	14:00	14:45	00:45
16 z 36 szyfrowanie plików, folderów i pendrive'ów w praktyce	Dominik Hamera	04-06-2025	14:45	16:00	01:15
17 z 36 Przerwa	Dominik Hamera	04-06-2025	16:00	16:30	00:30
18 z 36 jak chronić dane osobowe zgodnie z RODO?	Dominik Hamera	04-06-2025	16:30	17:30	01:00
19 z 36 zastrzeż swój PESEL	Dominik Hamera	04-06-2025	17:30	19:00	01:30
20 z 36 Przerwa	Dominik Hamera	04-06-2025	19:00	19:30	00:30
21 z 36 jak robić backup danych?	Dominik Hamera	04-06-2025	19:30	21:00	01:30
22 z 36 dlaczego warto korzystać z „chmury”?	Dominik Hamera	05-06-2025	14:00	14:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 36 wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?	Dominik Hamera	05-06-2025	14:45	16:00	01:15
24 z 36 Przerwa	Dominik Hamera	05-06-2025	16:00	16:30	00:30
25 z 36 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Dominik Hamera	05-06-2025	16:30	17:30	01:00
26 z 36 co o nas wiemy? - socjotechniki wykorzystywane przez hakerów	Dominik Hamera	05-06-2025	17:30	19:00	01:30
27 z 36 Przerwa	Dominik Hamera	05-06-2025	19:00	19:30	00:30
28 z 36 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Dominik Hamera	05-06-2025	19:30	21:00	01:30
29 z 36 jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?	Dominik Hamera	06-06-2025	14:00	14:45	00:45
30 z 36 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Dominik Hamera	06-06-2025	14:45	16:00	01:15
31 z 36 Przerwa	Dominik Hamera	06-06-2025	16:00	16:30	00:30
32 z 36 ćwiczenie grupowe: symulacje ataków cybernetycznych	Dominik Hamera	06-06-2025	16:30	17:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
33 z 36 narzędzia i programy wzmacniające bezpieczeństwo cyfrowe	Dominik Hamera	06-06-2025	17:30	19:00	01:30
34 z 36 Przerwa	Dominik Hamera	06-06-2025	19:00	19:30	00:30
35 z 36 Podsumowanie	Dominik Hamera	06-06-2025	19:30	20:00	00:30
36 z 36 Test teoretyczny z wynikiem generowanym automatycznie - walidacja	Dominik Hamera	06-06-2025	20:00	21:00	01:00

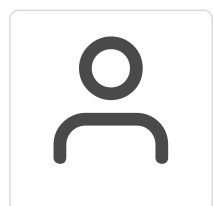
Cennik

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

Dominik Hamera

Jestem doświadczonym szkoleniowcem i doradcą biznesowym z 10-letnim stażem, specjalizującym się w pozyskiwaniu funduszy (ponad 200 mln zł dla klientów) oraz kompleksowym wsparciu w zarządzaniu, motywacji i optymalizacji procesów organizacyjnych. Absolwent AWF Warszawa (kierunek: Wychowanie Fizyczne, specjalność: Menedżer), łączę wiedzę akademicką z praktyką biznesową, prowadząc szkolenia z zakresu tworzenia dokumentów unijnych, automotywacji, radzenia sobie ze stresem oraz skutecznego zarządzania dla właścicieli firm, kadry kierowniczej i

sektora MŚP. Z ponad 2000 godzin szkoleń i 3000 przeszkolonych osób, oferuję spersonalizowane rozwiązania, które przekładają się na mierzalne sukcesy – od pozyskania finansowania po wzrost efektywności zespołów. Moja misja? Przekazywać wiedzę, która napędza rozwój zarówno firm, jak i ich zespołów.

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, 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