Możliwość dofinansowania

PHRS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

680 ocen

Szkolenie - Cyberbezpieczeństwo w sieci - moduł zaawansowany

Numer usługi 2026/04/30/135866/3524881

5 450,00 PLN brutto
5 450,00 PLN netto
181,67 PLN brutto/h
181,67 PLN netto/h
261,33 PLN cena rynkowa

Ruska Wieś
Usługa szkoleniowa
mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
30:00 h
27.05.2026 do 29.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Grupę docelową usługi stanowią seniorzy chcący zgłębić wiedzę w obszarze cyberbezpieczeństwa.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	26-05-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	30
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest rozwinięcie zaawansowanych kompetencji uczestników w zakresie samodzielnego zarządzania bezpieczeństwem cyfrowym, identyfikowania złożonych zagrożeń oraz podejmowania skutecznych działań zapobiegawczych i reakcyjnych, a także świadomego funkcjonowania w środowisku cyfrowym z uwzględnieniem ochrony tożsamości i danych.Szkolenie wpisuje się w kategorię usług istotnych dla przemysłu w regionie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Uczestnik charakteryzuje złożone mechanizmy cyberzagrożeń (np. socjotechnika, ataki wieloetapowe).	- wskazuje elementy składowe minimum 2 typów ataków, - poprawnie analizuje minimum 4 z 6 przykładów.	Test teoretyczny z wynikiem generowanym automatycznie Wywiad swobodny
Wiedza: Uczestnik wyjaśnia zasady ochrony tożsamości cyfrowej oraz zarządzania dostępem.	-wskazuje minimum 3 metody ochrony tożsamości, przyporządkowuje rozwiązania do właściwych sytuacji.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik analizuje złożone sytuacje zagrożeń cyfrowych.	-identyfikuje zagrożenia w minimum 3 z 4 scenariuszy, wskazuje wieloetapowy przebieg ataku.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik zarządza ustawieniami bezpieczeństwa i prywatności na różnych urządzeniach.	- poprawnie konfiguruje minimum 3 ustawienia bezpieczeństwa, dostosowuje poziom zabezpieczeń do sytuacji.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik stosuje zaawansowane metody ochrony (np. menedżery haseł, 2FA, kopie zapasowe).	-poprawnie wdraża minimum 2 rozwiązania zabezpieczające, wskazuje ich zastosowanie w praktyce.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik reaguje kompleksowo na incydenty bezpieczeństwa.	- wskazuje właściwą sekwencję działań w minimum 2 przypadkach, dobiera odpowiednie środki reakcji.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje Społeczne: Uczestnik stosuje zasady odpowiedzialnego korzystania z technologii.	- wskazuje minimum 2 konsekwencje niebezpiecznych działań, unika ryzykownych zachowań w ćwiczeniach.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Uczestnik wspiera innych użytkowników w zakresie cyberbezpieczeństwa.	- przekazuje minimum 2 zasady bezpieczeństwa innym, proponuje rozwiązania w sytuacjach problemowych.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień 1: Zaawansowane zagrożenia i socjotechnika

Czas: 12 godzin dydaktycznych (z przerwami)

Cel dnia: Celem pierwszego dnia szkolenia jest rozwinięcie zdolności uczestników do identyfikowania i analizowania złożonych zagrożeń cyfrowych, w szczególności opartych na socjotechnice i wieloetapowych scenariuszach ataków, a także pogłębienie świadomości w zakresie ochrony tożsamości cyfrowej i zarządzania bezpieczeństwem danych.

Plan dnia:

1. **Godzina** 09:00 – 11:00 - Socjotechnika i manipulacja
2. **Godzina** 11:00 – 11:15 - Przerwa kawowa
3. **Godzina** 11:15 – 13:15 - Ataki wieloetapowe
4. **Godzina** 13:15 - 13:45 - Przerwa obiadowa
5. **Godzina** 13:45 - 15:45 - Tożsamość cyfrowa
6. **Godzina** 15:45 - 16:00 - Przerwa kawowa
7. **Godzina** 16:00 - 18:00 - Zarządzanie bezpieczeństwem

Dzień 2: Narzędzia bezpieczeństwa i praktyka

Czas: 12 godzin dydaktycznych (z przerwami)

Cel dnia: Celem drugiego dnia szkolenia jest rozwinięcie praktycznych kompetencji uczestników w zakresie stosowania narzędzi i metod zabezpieczania danych oraz bezpiecznego korzystania z usług cyfrowych, w tym finansowych, a także przygotowanie do podejmowania właściwych działań w sytuacjach zagrożeń i incydentów bezpieczeństwa.

Plan dnia:

1. **Godzina** 09:00 – 11:00 - Narzędzia bezpieczeństwa
2. **Godzina** 11:00 – 11:15 -Przerwa kawowa
3. **Godzina** 11:15 – 13:15 - Bezpieczeństwo w praktyce
4. **Godzina** 13:15 - 13:45 - Przerwa obiadowa
5. **Godzina** 13:45 - 15:45 - Ochrona finansów
6. **Godzina** 15:45 - 16:00 - Przerwa kawowa
7. **Godzina** 16:00 - 18:00 - Reagowanie na incydenty

Dzień 3: Utrwalenie i wdrożenie zasad bezpieczeństwa

Czas: 6 godzin dydaktycznych (z przerwami)

Cel dnia: Celem trzeciego dnia szkolenia jest utrwalenie zdobytej wiedzy i umiejętności poprzez praktyczne zastosowanie w symulowanych sytuacjach oraz przygotowanie uczestników do samodzielnego wdrażania zasad cyberbezpieczeństwa w codziennym życiu i przekazywania ich w swoim otoczeniu.

Plan dnia:

1. **Godzina** 09:00 – 11:00 - Warsztat praktyczny
2. **Godzina** 11:00 – 11:15 -Przerwa kawowa
3. **Godzina** 11:15 – 13:15 - Podsumowanie i plan działania
4. **Godzina** 13:15 - 14:00 - walidacja w formie zdalnej na zoom

Szkolenie realizowane jest w godzinach dydaktycznych (1 godzina dydaktyczna = 45 minut).Przerwy są wliczane do czasu zajęć merytorycznych.Harmonogram może ulec nieznacznym przesunięciom wynikającym z potrzeb grupy przy zachowaniu zakresu merytorycznego i liczby godzin.

Łączna liczba godzin: 30 **godziny dydaktyczne**

W tym:

- zajęcia teoretyczne – 20 godzin
- zajęcia praktyczne – 9,25 godziny
- walidacja – 0,75 godziny
- przerwy – zgodnie z harmonogramem

Podczas szkolenia stosowane są metody aktywizujące:

- wykład interaktywny,
- pokaz,
- instruktaż,
- ćwiczenia praktyczne,
- ćwiczenia indywidualne,
- ćwiczenia grupowe,
- analiza przypadków,
- dyskusja moderowana,
- sesja pytań i odpowiedzi,
- quizy,
- projekt praktyczny.

Harmonogram

Liczba pozycji harmonogramu: 18

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 18 Dzień I - Socjotechnika i manipulacja	Łukasz Falba	27-05-2026	09:00	11:00	02:00	Tak
2 z 18 Dzień I - Przerwa kawowa	Łukasz Falba	27-05-2026	11:00	11:15	00:15	Tak
3 z 18 Dzień I - Ataki wieloetapowe	Łukasz Falba	27-05-2026	11:15	13:15	02:00	Tak

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
4 z 18 Dzień I - Przerwa obiadowa	Łukasz Falba	27-05-2026	13:15	13:45	00:30	Tak
5 z 18 Dzień I - Tożsamość cyfrowa	Łukasz Falba	27-05-2026	13:45	15:45	02:00	Tak
6 z 18 Dzień I - Przerwa Kawowa	Łukasz Falba	27-05-2026	15:45	16:00	00:15	Tak
7 z 18 Dzień I - Zarządzanie bezpieczeństwem	Łukasz Falba	27-05-2026	16:00	18:00	02:00	Tak
8 z 18 Dzień II- Narzędzia bezpieczeństwa	Łukasz Falba	28-05-2026	09:00	11:00	02:00	Tak
9 z 18 Dzień II- przerwa kawowa	Łukasz Falba	28-05-2026	11:00	11:15	00:15	Tak
10 z 18 Dzień II - Bezpieczeństwo w praktyce	Łukasz Falba	28-05-2026	11:15	13:15	02:00	Tak
11 z 18 Dzień II - Przerwa obiadowa	Łukasz Falba	28-05-2026	13:15	13:45	00:30	Tak
12 z 18 Dzień II - Ochrona finansów	Łukasz Falba	28-05-2026	13:45	15:45	02:00	Tak
13 z 18 Dzień II - Przerwa kawowa	Łukasz Falba	28-05-2026	15:45	16:00	00:15	Tak
14 z 18 Dzień II - Reagowanie na incydenty	Łukasz Falba	28-05-2026	16:00	18:00	02:00	Tak
15 z 18 Dzień III - Warsztat praktyczny	Łukasz Falba	29-05-2026	09:00	11:00	02:00	Tak

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
16 z 18 Dzień III - Przerwa kawowa	Łukasz Falba	29-05-2026	11:00	11:15	00:15	Tak
17 z 18 Dzień III - Podsumowanie i plan działania	Łukasz Falba	29-05-2026	11:15	13:15	02:00	Tak
18 z 18 Dzień III - Walidacja w formie zdalnej na zoom	-	29-05-2026	13:15	14:00	00:45	Nie

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 450,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	5 450,00 PLN
Koszt osobogodziny brutto	181,67 PLN
Koszt osobogodziny netto	181,67 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Łukasz Falba

Trener i praktyk z doświadczeniem w obszarze marketingu cyfrowego, komunikacji internetowej oraz bezpieczeństwa użytkowników w środowisku online. Specjalizuje się w zagadnieniach związanych z funkcjonowaniem mediów społecznościowych, analizą zagrożeń w sieci oraz świadomym i bezpiecznym korzystaniem z narzędzi cyfrowych.
Współzałożyciel agencji marketingowej 4WebZones, w ramach której realizował projekty dla firm i organizacji, m.in. Hoist Polska, Sweco Consulting, mySafety oraz Pomorski Związek Żeglarski. Odpowiadał za planowanie i realizację kampanii internetowych oraz analizę zachowań

użytkowników w sieci.
Posiada doświadczenie w prowadzeniu szkoleń dla pracowników działów marketingu i sprzedaży, ze szczególnym uwzględnieniem praktycznego wykorzystania narzędzi cyfrowych oraz identyfikacji zagrożeń w środowisku online.
W ciągu ostatnich 24 miesięcy przeprowadził co najmniej 120 godzin szkoleń w obszarze kompetencji cyfrowych i bezpiecznego korzystania z internetu. Adres internetowy trenera: info@phrs.pl

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały własne trenera w postaci autorskiej prezentacji multimedialnej. Zostaną wysłane drogą mailową po zakończonym szkoleniu.

Szkolenie realizowane jest w grupie od 3 do 30 osób.

Podczas zajęć:

- uczestnicy pracują indywidualnie,
- realizowane są ćwiczenia w małych grupach 3–5 osób,
- każdy uczestnik ma zapewnione stanowisko umożliwiające realizację ćwiczeń.

Stanowisko obejmuje:

- miejsce siedzące,
- dostęp do internetu,
- dostęp do energii elektrycznej,
- możliwość korzystania z komputera lub urządzenia mobilnego.

W części zdalnej uczestnik korzysta z własnego sprzętu.

Warunki uczestnictwa

1. zarejestrowanie i założenie konta w Bazie Usług Rozwojowych

2. zapisanie się na szkolenie za pośrednictwem Bazy i przypisanego ID wsparcia oraz spełnienie wszystkichwarunkówuczestnictwawprojekcie określonych przez Operatora

3. Podstawowa wiedza z zakresu funkcjonowania internetu

Warunkiem ukończenia szkolenia jest:

- udział w minimum **80% zajęć**,
- udział w procesie walidacji,
- wykonanie ćwiczeń praktycznych.

Frekwencja potwierdzana jest poprzez:

- listy obecności (część stacjonarna),
- raporty logowań (część zdalna)

Informacje dodatkowe

Usługa zwolniona z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.

Warunki techniczne

Podstawą do rozliczenia usługi jest wygenerowanie z systemu Zoom raportu, umożliwiającego identyfikację wszystkichuczestnikóworazzastosowanego narzędzia

Do udziału w szkoleniu online niezbędne jest:

stabilne połączenie z Internetem

oraz jedno z poniższych urządzeń:

komputer stacjonarny

laptop

tablet

telefon z przeglądarką internetową

Minimalne wymagania techniczne:

procesor 2-rdzeniowy 2 GHz; 2 GB pamięci RAM; system operacyjny Windows 8 lub nowszy, MAC OSwersja10.13;przeglądarkainternetowa Google Chrome, Mozilla Firefox lub Safari; stałe łącze internetowe o prędkości 1,5 Mbps; kamera,mikrofonigłośniki lubsłuchawki (Teams lub Zoom współpracuje ze wszystkimi kamerami wbudowanymi w laptopy).

Nie jest wymagana instalacja oprogramowania ani umiejętności informatyczne, aby dołączyć do szkolenia.

Dołączenie następuje poprzez kliknięcie w indywidualny link wysłany mailem do uczestnika przed szkoleniem. Ważność linku - dozakończenia szkolenia wg harmonogramu szkolenia.

Adres

Ruska Wieś 5b
11-600 Ruska Wieś
woj. warmińsko-mazurskie

Villa Sielanka

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

MARCIN RATAJCZYK

E-mail marcin@phrs.pl
Telefon (+48) 785 258 696