Możliwość dofinansowania

PHRS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

680 ocen

Szkolenie - Cyberbezpieczeństwo w sieci - moduł rozszerzony

Numer usługi 2026/04/16/135866/3491741

2 800,00 PLN brutto
2 800,00 PLN netto
175,00 PLN brutto/h
175,00 PLN netto/h
250,00 PLN cena rynkowa

Ruska Wieś
Usługa szkoleniowa
mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
16:00 h
25.05.2026 do 26.05.2026

Informacje podstawowe

Kategoria	Biznes / Marketing
Grupa docelowa usługi	Grupę docelową usługi stanowią seniorzy chcący zgłębić wiedzę w obszarze cyberbezpieczeństwa.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	30
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	16
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 praktycznych kompetencji uczestników w zakresie zaawansowanego rozpoznawania zagrożeń cyfrowych, świadomego zarządzania bezpieczeństwem swoich urządzeń i danych oraz podejmowania właściwych działań w sytuacjach incydentów bezpieczeństwa w środowisku cyfrowym. 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 zaawansowane metody oszustw internetowych (np. spoofing, phishing ukierunkowany).	- wskazuje różnice pomiędzy co najmniej 2 typami oszustw, poprawnie -identyfikuje minimum 4 z 6 przykładów.	Test teoretyczny z wynikiem generowanym automatycznie Wywiad swobodny
Wiedza: Uczestnik wyjaśnia mechanizmy działania zabezpieczeń cyfrowych (np. 2FA, szyfrowanie, aktualizacje).	- opisuje działanie minimum 2 mechanizmów zabezpieczeń, - przyporządkowuje zabezpieczenia do właściwych zastosowań.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik analizuje komunikaty i sytuacje pod kątem ryzyka cyberzagrożeń.	-identyfikuje zagrożenia w minimum 3 z 4 scenariuszy, - wskazuje co najmniej 2 elementy ryzyka w każdej sytua	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik konfiguruje podstawowe zabezpieczenia na urządzeniu (np. ustawienia prywatności, aktualizacje).	- poprawnie wykonuje minimum 2 działania konfiguracyjne, stosuje właściwe ustawienia bezpieczeństwa.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik stosuje zasady bezpiecznego korzystania z bankowości i usług online w sytuacjach podwyższonego ryzyka.	- wykonuje poprawnie zadanie symulacyjne, wskazuje minimum 3 zasady bezpieczeństwa w danej sytuacji.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik reaguje na incydenty bezpieczeństwa (np. wyciek danych, próba oszustwa).	- wskazuje właściwe działania w minimum 2 z 3 przypadków, określa kolejność działań (np. blokada konta, zgłoszenie).	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje Społeczne: Uczestnik stosuje zasady ograniczonego zaufania w środowisku cyfrowym.	- w ćwiczeniach unika ryzykownych zachowań, wskazuje minimum 2 sytuacje wymagające ostrożności.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Uczestnik upowszechnia zasady cyberbezpieczeństwa w swoim otoczeniu.	- formułuje minimum 2 zasady do przekazania innym, przedstawia przykład sytuacji wymagającej edukacji innych.	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 ochrona danych w praktyce”

Czas: 5,4 godzin dydaktycznych (z przerwami)

Cel dnia: Celem pierwszego dnia szkolenia jest rozwinięcie zdolności uczestników do rozpoznawania bardziej złożonych zagrożeń cyfrowych oraz świadomego zarządzania bezpieczeństwem swoich urządzeń i danych poprzez analizę rzeczywistych scenariuszy, poznanie mechanizmów działania zabezpieczeń oraz praktyczne zastosowanie ustawień prywatności i ochrony informacji w środowisku internetowym.

Plan dnia:

1. **Godzina** 13:30 – 15:30**:** Nowe metody oszustw internetowych
2. **Godzina** 15:30 – 15:45**:** Przerwa kawowa
3. **Godzina** 15:45 – 17:45**:** Praktyczne scenariusze zagrożeń

Dzień 2: „Bezpieczeństwo danych i reagowanie na incydenty”

Czas: 10,6 godzin dydaktycznych (z przerwami)

Cel dnia: Celem drugiego dnia szkolenia jest przygotowanie uczestników do skutecznego reagowania na incydenty bezpieczeństwa w sieci oraz utrwalenie umiejętności bezpiecznego korzystania z usług finansowych i internetowych w sytuacjach podwyższonego ryzyka, z uwzględnieniem właściwych procedur postępowania i dostępnych form wsparcia.

Plan dnia:

1. **Godzina** 09:00 – 10:30 -Bezpieczeństwo urządzeń
2. **Godzina** 10:30 – 10:45 -Przerwa kawowa
3. **Godzina** 10:45 – 12:15 - Ochrona danych i prywatności
4. **Godzina** 12:15 - 12:45 - Przerwa obiadowa
5. **Godzina** 12:45 - 14:15 - Bezpieczna bankowość i zakupy – poziom zaawansowany
6. **Godzina** 14:15 - 14:30 - Przerwa kawowa
7. **Godzina** 14:30 - 16:00 - Reagowanie na incydenty
8. **Godzina** 16:00 - 16:45 - walidacja w formie zdalnej na zoom

Szkolenie realizowane jest w godzinach dydaktycznych (1 godzina dydaktyczna = 45 minut).Przerwy nie 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: 16 **godziny dydaktyczne**

W tym:

- zajęcia teoretyczne – 10 godzin
- zajęcia praktyczne – 6 godziny
- walidacja – 45 min
- 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: 11

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 11 Dzień I - Nowe metody oszustw internetowych	Łukasz Falba	25-05-2026	13:30	15:30	02:00	Tak
2 z 11 Dzień I - Przerwa kawowa	-	25-05-2026	15:30	15:45	00:15	Tak
3 z 11 Dzień I - Praktyczne scenariusze zagrożeń	Łukasz Falba	25-05-2026	15:45	17:45	02:00	Tak
4 z 11 Dzień II - Bezpieczeństwo urządzeń	Łukasz Falba	26-05-2026	09:00	10:30	01:30	Tak
5 z 11 Dzień II - Przerwa kawowa	Łukasz Falba	26-05-2026	10:30	10:45	00:15	Tak
6 z 11 Dzień II - Ochrona danych i prywatności	Łukasz Falba	26-05-2026	10:45	12:15	01:30	Tak

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
7 z 11 Dzień II - Przerwa obiadowa	Łukasz Falba	26-05-2026	12:15	12:45	00:30	Tak
8 z 11 Dzień II - Bezpieczna bankowość i zakupy – poziom zaawansowany	Łukasz Falba	26-05-2026	12:45	14:15	01:30	Tak
9 z 11 Dzień II - Przerwa kawowa	Łukasz Falba	26-05-2026	14:15	14:30	00:15	Tak
10 z 11 Dzień II - Reagowanie na incydenty	Łukasz Falba	26-05-2026	14:30	16:00	01:30	Tak
11 z 11 Dzień II - walidacja w formie zdalnej na zoom	-	26-05-2026	16:00	16:45	00:45	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN
Koszt osobogodziny brutto	175,00 PLN
Koszt osobogodziny netto	175,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Łukasz Falba

Praktyk i trener z zakresu digital marketingu, marketingu sprzedażowego w sieci, aszczególnieperformance marketingu w mediach społecznościowych. Jest współzałożycielemagencjimarketingowej 4WebZones, gdzie wraz z zespołem pomaga w marketingu internetowym fi rmomtakim jak: Hoist Polska, Zameh Marine, Sweco Consulting, mySafety, Żeglarski.info czyPomorskiZwiązek Żeglarski.Prowadził szkolenia dla działów marketingu i działów sprzedaży.Zarządzałkampaniami promocyjnymi w niemal wszystkich mediach społecznościowych i byłodpowiedzialnyza milionowe budżety swoich klientów. W ciągu ostatnich 24 miesięcy przeprowadziłco najmniej
120h z tej tematyki. 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