Możliwość dofinansowania

PHRS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

680 ocen

Szkolenie - Cyberbezpieczeństwo w sieci - moduł podstawowy

Numer usługi 2026/04/16/135866/3491587

Ruska Wieś

Usługa szkoleniowa

mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

16:00 h

24.05.2026 do 25.05.2026

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

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
Data zakończenia rekrutacji	23-05-2026
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 podniesienie poziomu bezpieczeństwa cyfrowego uczestników poprzez rozwinięcie praktycznych umiejętności rozpoznawania zagrożeń w internecie, ochrony danych osobowych oraz bezpiecznego korzystania z podstawowych usług online, takich jak poczta elektroniczna, bankowość internetowa czy media społecznościowe. 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: - Identyfikuje podstawowe zagrożenia występujące w internecie, w tym phishing, złośliwe oprogramowanie oraz próby wyłudzenia danych.	- wskazuje poprawnie minimum 4 z 6 przedstawionych zagrożeń, - przyporządkowuje zagrożenia do właściwych kategorii (np. phishing, malware).	Test teoretyczny z wynikiem generowanym automatycznie Wywiad swobodny
Wiedza: Uczestnik rozróżnia bezpieczne i niebezpieczne komunikaty oraz strony internetowe.	- dokonuje poprawnej oceny minimum 3 z 4 przykładów, - wskazuje co najmniej 2 elementy świadczące o wiarygodności lub zagrożeniu.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Wiedza: - Uczestnik wyjaśnia podstawowe zasady ochrony danych osobowych w internecie.	- wskazuje minimum 3 zasady ochrony danych, - poprawnie odpowiada na minimum 70% pytań testowych.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik rozpoznaje podejrzane wiadomości i próby oszustwa internetowego.	- identyfikuje minimum 3 z 4 niebezpiecznych komunikatów, - wskazuje element ryzyka w każdej analizowanej sytuacji.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik tworzy i stosuje bezpieczne hasła oraz podstawowe zabezpieczenia.	- tworzy hasło spełniające minimum 3 kryteria bezpieczeństwa, - wskazuje minimum 2 zasady ich bezpiecznego stosowania.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik stosuje zasady bezpiecznego korzystania z usług internetowych.	- wykonuje poprawnie zadanie symulacyjne (np. zakup online / logowanie), - wskazuje minimum 2 działania zwiększające bezpieczeństwo.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Uczestnik reaguje adekwatnie w sytuacji zagrożenia cyfrowego.	- wskazuje właściwe działanie w minimum 2 z 3 scenariuszy, określa sposób - zgłoszenia incydentu.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje Społeczne: Uczestnik zachowuje ostrożność podczas korzystania z internetu.	- w trakcie ćwiczeń stosuje zasady bezpieczeństwa, - wskazuje minimum 2 ryzyka związane z udostępnianiem danych.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Uczestnik podejmuje świadome decyzje dotyczące bezpieczeństwa cyfrowego.	- dokonuje poprawnego wyboru w minimum 2 z 3 analizowanych sytuacji, - uzasadnia decyzję w oparciu o poznane zasady.	Wywiad swobodny Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Kompetencje Społeczne: Uczestnik uzasadnia znaczenie stosowania zasad cyberbezpieczeństwa w codziennym życiu.	- wskazuje minimum 2 argumenty potwierdzające znaczenie bezpieczeństwa, - odnosi zasady do własnych doświadczeń.	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: „Podstawy cyberbezpieczeństwa i ochrona przed zagrożeniami w sieci”

Czas: 10,6 godzin dydaktycznych (z przerwami)

Cel dnia: Celem pierwszego dnia szkolenia jest zbudowanie podstawowej świadomości uczestników w zakresie zagrożeń występujących w internecie oraz rozwinięcie umiejętności identyfikowania potencjalnych niebezpieczeństw, w szczególności oszustw internetowych, a także nabycie praktycznych kompetencji związanych z bezpiecznym korzystaniem z sieci, tworzeniem i zarządzaniem hasłami oraz ochroną danych osobowych.

Plan dnia:

1. **Godzina** 08:00 – 10:30**:** Wprowadzenie do cyberbezpieczeństwa
2. **Godzina** 10:30 – 10:45**:** Przerwa kawowa
3. **Godzina 10**:45 – 12:15**:** Bezpieczne korzystanie z internetu
4. **Godzina** 12:15 – 12:45**:** Przerwa Obiadowa
5. **Godzina** 12:45 – 14:15**:** Hasła i ochrona danych
6. **Godzina** 14:15 – 14:30**:** Przerwa kawowa
7. **Godzina** 14:30 – 16:00: Oszustwa internetowe

Dzień 2: „Bezpieczne korzystanie z usług internetowych i komunikacji online”

Czas: 5,4 godzin dydaktycznych (z przerwami)

Cel dnia: Celem drugiego dnia szkolenia jest utrwalenie i rozwinięcie praktycznych umiejętności bezpiecznego korzystania z narzędzi komunikacji internetowej, mediów społecznościowych oraz usług online, w tym zakupów i bankowości elektronicznej, a także przygotowanie uczestników do świadomego reagowania w sytuacjach zagrożenia i podejmowania bezpiecznych decyzji w środowisku cyfrowym.

Plan dnia:

1. **Godzina** 09:00 – 10:30**:** Bezpieczna komunikacja i media społecznościowe
2. **Godzina** 10:30 – 10:45**:** Przerwa kawowa
3. **Godzina** 10:45 – 12:15**:** Bezpieczne zakupy i bankowość internetowa
4. **Godzina** 12:15 - 13:00 - 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 - Wprowadzenie do cyberbezpieczeństwa	Łukasz Falba	24-05-2026	08:00	10:30	02:30	Tak
2 z 11 Dzień I - przerwa kawowa	Łukasz Falba	24-05-2026	10:30	10:45	00:15	Tak

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
3 z 11 Dzień I - Bezpieczne korzystanie z internetu	Łukasz Falba	24-05-2026	10:45	12:15	01:30	Tak
4 z 11 Dzień I - Przerwa Obiadowa	Łukasz Falba	24-05-2026	12:15	12:45	00:30	Tak
5 z 11 Dzień I - Hasła i ochrona danych	Łukasz Falba	24-05-2026	12:45	14:15	01:30	Tak
6 z 11 Dzień I - Przerwa kawowa	Łukasz Falba	24-05-2026	14:15	14:30	00:15	Tak
7 z 11 Dzień I - Oszustwa internetowe	Łukasz Falba	24-05-2026	14:30	16:00	01:30	Tak
8 z 11 Dzień II - Bezpieczna komunikacja i media społecznościowe	Łukasz Falba	25-05-2026	09:00	10:30	01:30	Tak
9 z 11 Dzień II - Przerwa kawowa	Łukasz Falba	25-05-2026	10:30	10:45	00:15	Tak
10 z 11 Dzień II - Bezpieczne zakupy i bankowość internetowa	Łukasz Falba	25-05-2026	10:45	12:15	01:30	Tak
11 z 11 Dzień II - Walidacja w formie zdalnej na zoom	-	25-05-2026	12:15	13:00	00:45	Nie

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