



PHRS SPÓŁKA Z  
OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ

★★★★★ 5,0 / 5

680 ocen

## Szkolenie - Cyberbezpieczeństwo w sieci - moduł rozszerzony

Numer usługi 2026/04/30/135866/3524798

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

2 800,00 PLN brutto  
2 800,00 PLN netto  
175,00 PLN brutto/h  
175,00 PLN netto/h  
261,33 PLN cena rynkowa ⓘ

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Grupa docelowa usługi</b>	Grupę docelową usługi stanowią seniorzy chcący zgłębić wiedzę w obszarze cyberbezpieczeństwa.
<b>Minimalna liczba uczestników</b>	3
<b>Maksymalna liczba uczestników</b>	30
<b>Data zakończenia rekrutacji</b>	24-05-2026
<b>Forma prowadzenia usługi</b>	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
<b>Liczba godzin usługi</b>	16
<b>Podstawa uzyskania wpisu do BUR</b>	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
<p><b>Wiedza:</b> Uczestnik charakteryzuje zaawansowane metody oszustw internetowych (np. spoofing, phishing ukierunkowany).</p>	<p>- wskazuje różnice pomiędzy co najmniej 2 typami oszustw, poprawnie -identyfikuje minimum 4 z 6 przykładów.</p>	Test teoretyczny z wynikiem generowanym automatycznie
		Wywiad swobodny
<p><b>Wiedza:</b> Uczestnik wyjaśnia mechanizmy działania zabezpieczeń cyfrowych (np. 2FA, szyfrowanie, aktualizacje).</p> <p><b>Umiejętności:</b> Uczestnik analizuje komunikaty i sytuacje pod kątem ryzyka cyberzagrożeń.</p> <p><b>Umiejętności:</b> Uczestnik konfiguruje podstawowe zabezpieczenia na urządzeniu (np. ustawienia prywatności, aktualizacje).</p> <p><b>Umiejętności:</b> Uczestnik stosuje zasady bezpiecznego korzystania z bankowości i usług online w sytuacjach podwyższonego ryzyka.</p> <p><b>Umiejętności:</b> Uczestnik reaguje na incydenty bezpieczeństwa (np. wyciek danych, próba oszustwa).</p> <p><b>Kompetencje Społeczne:</b> Uczestnik stosuje zasady ograniczonego zaufania w środowisku cyfrowym.</p>	<p>- opisuje działanie minimum 2 mechanizmów zabezpieczeń, - przyporządkowuje zabezpieczenia do właściwych zastosowań.</p> <p>-identyfikuje zagrożenia w minimum 3 z 4 scenariuszy, - wskazuje co najmniej 2 elementy ryzyka w każdej sytuacji</p> <p>- poprawnie wykonuje minimum 2 działania konfiguracyjne, stosuje właściwe ustawienia bezpieczeństwa.</p> <p>- wykonuje poprawnie zadanie symulacyjne, wskazuje minimum 3 zasady bezpieczeństwa w danej sytuacji.</p> <p>- wskazuje właściwe działania w minimum 2 z 3 przypadków, określa kolejność działań (np. blokada konta, zgłoszenie).</p> <p>- w ćwiczeniach unika ryzykownych zachowań, wskazuje minimum 2 sytuacje wymagające ostrożności.</p>	Wywiad swobodny
		Test teoretyczny z wynikiem generowanym automatycznie
		Wywiad swobodny
		Test teoretyczny z wynikiem generowanym automatycznie
		Wywiad swobodny
		Test teoretyczny z wynikiem generowanym automatycznie
		Wywiad swobodny
		Test teoretyczny z wynikiem generowanym automatycznie
		Wywiad swobodny
		Test teoretyczny z wynikiem generowanym automatycznie
<p><b>Kompetencje społeczne:</b> Uczestnik upowszechnia zasady cyberbezpieczeństwa w swoim otoczeniu.</p>	<p>- formułuje minimum 2 zasady do przekazania innym, przedstawia przykład sytuacji wymagającej edukacji innych.</p>	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 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 – 5,25 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: 11

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<b>1 z 11</b> Dzień I - Nowe metody oszustw internetowych	Łukasz Falba	25-05-2026	13:30	15:30	02:00	Tak
<b>2 z 11</b> Dzień I - Przerwa kawowa	Łukasz Falba	25-05-2026	15:30	15:45	00:15	Tak
<b>3 z 11</b> Dzień I - Praktyczne scenariusze zagrożeń	Łukasz Falba	25-05-2026	15:45	17:45	02:00	Tak
<b>4 z 11</b> Dzień II- Bezpieczeńst wo urzędzeń	Łukasz Falba	26-05-2026	09:00	10:30	01:30	Tak
<b>5 z 11</b> Dzień II- Przerwa kawowa	Łukasz Falba	26-05-2026	10:30	10:45	00:15	Tak
<b>6 z 11</b> 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
<b>7 z 11</b> Dzień II-Przerwa obiadowa	Łukasz Falba	26-05-2026	12:15	12:45	00:30	Tak
<b>8 z 11</b> Dzień II-Bezpieczna bankowość i zakupy – poziom zaawansowany	Łukasz Falba	26-05-2026	12:45	14:15	01:30	Tak
<b>9 z 11</b> Dzień II-Przerwa kawowa	Łukasz Falba	26-05-2026	14:15	14:30	00:15	Tak
<b>10 z 11</b> Dzień II - Reagowanie na incydent	Łukasz Falba	26-05-2026	14:30	16:00	01:30	Tak
<b>11 z 11</b> Dzień II - walidacja w formie zdalnej na zoom	-	26-05-2026	16:00	16:45	00:45	Nie

## Cennik

### Cennik

Rodzaj ceny	Cena
<b>Koszt przypadający na 1 uczestnika brutto</b>	2 800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
<b>Koszt przypadający na 1 uczestnika netto</b>	2 800,00 PLN
<b>Koszt osobogodziny brutto</b>	175,00 PLN
<b>Koszt osobogodziny netto</b>	175,00 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 wszystkich warunków uczestnictwa w projekcie 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 wszystkich uczestników oraz zastosowanego 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 OS wersja 10.13; przeglądarka internetowa Google Chrome, Mozilla Firefox lub Safari; stałe łącze internetowe o prędkości 1,5 Mbps; kamera, mikrofon, głośniki lub słuchawki (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 - do zakończenia 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](mailto:marcin@phrs.pl)

**Telefon** (+48) 785 258 696