



## Bezpieczny Pracownik

Numer usługi 2024/06/24/166538/2194380

246,00 PLN brutto

200,00 PLN netto

82,00 PLN brutto/h

66,67 PLN netto/h

EXIMO PROJECT  
SPÓŁKA Z  
OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ

Brak ocen dla tego dostawcy

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 3 h

📅 03.09.2024 do 03.09.2024

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
<b>Grupa docelowa usługi</b>	<ul style="list-style-type: none"><li>Szkolenie jest skierowane do wszystkich, którzy chcą poszerzyć swoją wiedzę na temat bezpiecznego użytkowania Internetu.</li><li>Szkolenie realizujemy także w formie zamkniętej dla poszczególnych firm - wówczas program możemy rozszerzyć o testy phishingowe, które pomogą w identyfikacji słabych punktów i zbudowaniu świadomości pracowników. Cenę ustalamy wówczas indywidualnie, biorąc pod uwagę liczebność grupy. Napisz na: <a href="mailto:szkolenia@eximoproject.pl">szkolenia@eximoproject.pl</a></li></ul>
<b>Minimalna liczba uczestników</b>	30
<b>Maksymalna liczba uczestników</b>	50
<b>Data zakończenia rekrutacji</b>	29-08-2024
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	3
<b>Podstawa uzyskania wpisu do BUR</b>	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

# Cel

## Cel edukacyjny

Celem szkolenia jest wyposażenie uczestników w niezbędną wiedzę, umiejętności i postawy niezbędne do skutecznego radzenia sobie z cyberzagrożeniami oraz rozwój bezpieczeństwa w środowisku online.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zrozumie podstawowe pojęcia związane z cyberzagrożeniami, takie jak: phishing, scam, ransomware.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik pozyska wiedzę na temat statystyk oraz przykładów znaczących incydentów cybernetycznych.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik będzie potrafił rozpoznawać podstawowe zagrożenia cybernetyczne.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Uczestnik zdobędzie praktyczne umiejętności w obszarze bezpieczeństwa poczty elektronicznej, zabezpieczania urządzeń mobilnych, korzystania z publicznych sieci bezprzewodowych i tworzenia bezpiecznych haseł.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
• Uczestnik będzie gotów do stałego podnoszenia świadomości w zakresie cyberbezpieczeństwa.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
• Uczestnik kształtuje postawę gotowości do skutecznego reagowania w sytuacjach kryzysowych, posiadając opanowane podstawowe kroki w przypadku ataku lub naruszenia bezpieczeństwa.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych

## Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

tak

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

tak

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

tak

## Program

1. Przywitanie, cel szkolenia.
2. Przedstawienie statystyk oraz przykładów ataków na firmy i pracowników. Wskazanie motywów hakerów.
3. Wskazanie technik socjotechnicznych wraz z rzeczywistymi przykładami:
  - phishing,
  - scam,
  - ransomware.
4. Przedstawienie dobrych praktyk aby wzmocnić ochronę przed zagrożeniami cybernetycznymi:
5. Bezpieczeństwo w obsłudze poczty elektronicznej:
  - zabezpieczenie urządzeń mobilnych,
  - korzystanie z publicznych sieci bezprzewodowych,
  - jak stosować bezpieczne hasła.
6. Podsumowanie i schemat działania dla sytuacji kryzysowych

## Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	246,00 PLN
Koszt przypadający na 1 uczestnika netto	200,00 PLN

---

**Koszt osobogodziny brutto**

82,00 PLN

---

**Koszt osobogodziny netto**

66,67 PLN

---

## Prowadzący

Liczba prowadzących: 2

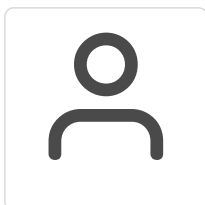


1 z 2

### MARCIN CHLEBOWSKI

Marcin Chlebowski - Współzałożyciel i CEO Eximo Project, firmie specjalizującej się w integracji systemów informatycznych oraz projektującej rozwiązania z zakresu bezpieczeństwa informatycznego.

Specjalista z zakresu bezpieczeństwa IT (CCIE #21714 Security) i technologii sieciowych. Prowadzi szkolenia z zakresu cyberbezpieczeństwa od siedmiu lat. Zrealizował kilkadziesiąt projektów szkoleniowych, a spod jego skrzydeł wyszło kilka tysięcy uczestników szkoleń.



2 z 2

### Damian Wierzyński

Damian Wierzyński – ma za sobą 10 lat doświadczenia w oswojaniu pracowników nietechnicznych z tajnikami technologii.

Potrafi opowiedzieć o tych skomplikowanych sprawach w taki sposób, że nikt nie wyjdzie ze szkolenia bez większej wiedzy. Jego specjalnością jest cyberbezpieczeństwo, infrastruktura sieciowa, systemy zabezpieczeń i rozwiązania Microsoftu.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (dostęp do materiałów autorskich, przygotowanych przez trenera, przesłane na adres e-mail uczestnika)

### Informacje dodatkowe

- Jedna godzina szkoleniowa to 45 minut.
- Szkolenie prowadzone jest w języku polskim, materiały przekazane do doskonalenia wiedzy także są opracowane w tym języku.
- Szkolenie będzie prowadzone w formie wykładu z analizą studiów przypadku. Elementem wykładu będą dyskusje z uczestnikami.
- Prowadzący będzie korzystał z materiałów dydaktycznych takich jak: prezentacja multimedialna.
- Zleceniodawca ma prawo zgłosić reklamację z tytułu niewykonania lub nienależytego wykonania usługi szkoleniowej. Termin składania reklamacji wynosi 14 dni roboczych, licząc od dnia, w którym usługa została zakończona lub miała zostać zakończona.
- Zleceniobiorca ma 14 dni roboczych na rozpatrzenie reklamacji; w przypadkach wymagających dodatkowych czynności wyjaśniających, czas rozpatrywania reklamacji może ulec wydłużeniu maksymalnie do 30 dni roboczych.
- Reklamacja powinna zostać przekazana mailowo na adres: support@eximoproject.pl.

# Warunki techniczne

**Komunikator:** Usługa będzie prowadzona za pośrednictwem platformy Microsoft Teams.

**Sprzęt:** Uczestnik potrzebuje komputera z aktualnym systemem operacyjnym Microsoft Windows lub macOS.

**Łącze internetowe:** Uczestnik powinien dysponować łączem internetowym o przepustowości minimum 10Mbit.

**Informacje organizacyjne:** Uczestnik na tydzień przed planowanym szkoleniem otrzyma maila organizacyjnego, zawierającego szczegółową instrukcję dołączenia do sesji szkoleniowej na platformie MS Teams.

## Kontakt



**Marika Ptak**

**E-mail** [eximo@eximoproject.pl](mailto:eximo@eximoproject.pl)

**Telefon** (+48) 52 5684 420