



ADVERT Edyta  
Stąpór-Rynk

★★★★★ 4,8 / 5

189 ocen

## Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie.

Numer usługi 2025/08/14/174663/2941153

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 16 h

📅 12.11.2025 do 13.11.2025

2 650,00 PLN brutto

2 650,00 PLN netto

165,63 PLN brutto/h

165,63 PLN netto/h

## Informacje podstawowe

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kategoria</b>                       | Informatyka i telekomunikacja / Bezpieczeństwo IT                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Grupa docelowa usługi</b>           | <p>Szkolenie przeznaczone dla przedsiębiorców i ich pracowników, którzy chcą poznać zasady ochrony przed cyberprzestępczością, oraz z uwagi na fakt zarządzania danymi osobowymi, ochrony tych danych przed atakami hakerów. Szkolenie dedykowane dla kadry zarządzającej, menagerów, księgowych, kancelarii prawnych.</p> <p>Szkolenie jest dostępne dla wszystkich zainteresowanych - bez względu na poziom doświadczenia w danej dziedzinie. Wierzymy, że każdy uczestnik będzie miał okazję pogłębić swoją wiedzę.</p> |
| <b>Minimalna liczba uczestników</b>    | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Maksymalna liczba uczestników</b>   | 25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Data zakończenia rekrutacji</b>     | 11-11-2025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Forma prowadzenia usługi</b>        | zdalna w czasie rzeczywistym                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Liczba godzin usługi</b>            | 16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Podstawa uzyskania wpisu do BUR</b> | Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Cel

### Cel edukacyjny

Usługa „ Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie.”

Przygotowuje uczestników do nabycia wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami

cyberprzestępców, wirusami, złośliwym oprogramowaniem.

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

| Efekty uczenia się                                                                                                                                       | Kryteria weryfikacji                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Metoda walidacji                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <p><b>W ZAKRESIE WIEDZY:</b><br/>Posiada wiedzę z zakresu zagrożeń cyberbezpieczeństwa i metod ochrony danych osobistych.</p>                            | <ul style="list-style-type: none"><li>• rozróżnia rodzaje zagrożeń w cyberprzestrzeni (np. phishing, malware, ransomware, spyware),</li><li>• charakteryzuje sposoby ataków na systemy operacyjne i sieci komputerowe,</li><li>• omawia zasady bezpiecznego korzystania z Internetu, poczty e-mail, chmury i mediów społecznościowych,</li><li>• wskazuje narzędzia i technologie stosowane do ochrony danych (np. firewalle, programy antywirusowe, VPN),</li><li>• opisuje zasady działania metod socjotechnicznych i ich wpływ na bezpieczeństwo informacji.</li></ul> | Test teoretyczny                     |
| <p><b>W ZAKRESIE UMIEJĘTNOŚCI</b><br/>Monitoruje i stosuje zasady bezpiecznego korzystania z zasobów sieciowych oraz chroni dane osobowe w praktyce.</p> | <ul style="list-style-type: none"><li>• konfiguruje przeglądarkę w trybie prywatnym/incognito i usuwa ślady aktywności w sieci,</li><li>• tworzy i przywraca kopie zapasowe danych,</li><li>• identyfikuje sytuacje zwiększonego ryzyka wycieku danych osobowych,</li><li>• stosuje metody bezpiecznego logowania i uwierzytelniania użytkowników,</li><li>• posługuje się narzędziami do szyfrowania i zabezpieczania plików oraz folderów.</li></ul>                                                                                                                    | Obserwacja w warunkach rzeczywistych |
| <p><b>W ZAKRESIE KOMPETENCJI SPOŁECZNYCH :</b><br/>Stosuje zasady odpowiedzialnego i świadomego zachowania w środowisku cyfrowym.</p>                    | <ul style="list-style-type: none"><li>• rozpoznaje próby wyłudzenia danych i fałszywe komunikaty (np. fałszywe e-maile, linki, aplikacje),</li><li>• odróżnia legalne działania od nieetycznych praktyk w sieci,</li><li>• definiuje i omawia pojęcia związane z cyberbezpieczeństwem (np. VPN, trojan, malware, szyfrowanie, incydent bezpieczeństwa),</li><li>• wykazuje postawę odpowiedzialności za ochronę danych w środowisku pracy,</li><li>• komunikuje zagrożenia cyfrowe współpracownikom i wspiera ich w stosowaniu zasad bezpieczeństwa.</li></ul>            | Obserwacja w warunkach rzeczywistych |

# 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 – Część teoretyczna:

- Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.
- Zarządzanie i ochrona danych w przedsiębiorstwie e- szyfrowanie danych – kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków -incydenty bezpieczeństwa.

### 2 – Część praktyczna:

- Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.
- Zarządzanie i ochrona danych w przedsiębiorstwie e- szyfrowanie danych – kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków -incydenty bezpieczeństwa.
- Walidacja

Szkolenie kierowane jest : dla wszystkich zainteresowanych - bez względu na poziom doświadczenia w danej dziedzinie. Wierzymy, że każdy uczestnik będzie miał okazję pogłębić swoją wiedzę.

Warunki organizacyjne: każdy uczestnik pracuje indywidualnie przy samodzielnym stanowisku komputerowym.

W harmonogramie uwzględniono godziny zegarowe, natomiast kurs opiera się na 45-minutowych godzinach lekcyjnych- stąd rozbieżność pomiędzy liczbą godzin w harmonogramie a ogólną liczbą godzin kursu.

1 godzina= 45 minut (godzina szkoleniowa)

Szkolenie obejmuje łącznie 16 godzin dydaktycznych, co przekłada się na 12 godzin zegarowych. Szkolenie obejmuje 1:30 przerwy. 12 godzin dydaktycznych to część teoretyczna zaś 4 godziny dydaktyczne obejmuje część praktyczna. Podczas ostatnich 30 minut szkolenia zostanie przeprowadzona walidacja.

Przerwy nie są wliczane w czas szkolenia.

Szkolenie będzie realizowane w formie zdalnej za pomocą platformy ClickMeeting.

Całość nagrania zostanie zarchiwizowana i umieszczona na dysku zewnętrznym w celu kontroli i audytu.

1. Prezentacja powerpoint celem utrwalenia informacji przekazanych w trakcie szkolenia drogą mailową.

2. E-materiały w formacie PDF.

Szkolenie w formie zdalnej będzie odbywało się w czasie rzeczywistym. W zależności od czasu potrzeb będą wykorzystywane różne elementy: ćwiczenia, testy, ankiety, udostępnianie ekranu i inne. Całe szkolenie jest rejestrowane w celach kontroli/audytu. Wykorzystanie nagrania w innym celu niż kontrola/audyt wymaga zgody Trenera i Uczestników

# Harmonogram

Liczba przedmiotów/zajęć: 15

| Przedmiot / temat zajęć                                                                                                                                                                                              | Prowadzący        | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------|---------------------|---------------------|---------------|
| <div>1 z 15</div> Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich. | Rafał Tomaszewski | 12-11-2025            | 09:00               | 10:30               | 01:30         |
| <div>2 z 15</div> przerwa                                                                                                                                                                                            | Rafał Tomaszewski | 12-11-2025            | 10:30               | 10:45               | 00:15         |
| <div>3 z 15</div> Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich. | Rafał Tomaszewski | 12-11-2025            | 10:45               | 12:15               | 01:30         |
| <div>4 z 15</div> przerwa                                                                                                                                                                                            | Rafał Tomaszewski | 12-11-2025            | 12:15               | 12:30               | 00:15         |

| Przedmiot / temat zajęć                                                                                                                                                                                   | Prowadzący        | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------|---------------------|---------------------|---------------|
| 5 z 15 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich. | Rafał Tomaszewski | 12-11-2025            | 12:30               | 14:00               | 01:30         |
| 6 z 15 przerwa                                                                                                                                                                                            | Rafał Tomaszewski | 12-11-2025            | 14:00               | 14:15               | 00:15         |
| 7 z 15 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich. | Rafał Tomaszewski | 12-11-2025            | 14:15               | 15:45               | 01:30         |
| 8 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie - szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa        | Rafał Tomaszewski | 13-11-2025            | 09:00               | 10:30               | 01:30         |
| 9 z 15 przerwa                                                                                                                                                                                            | Rafał Tomaszewski | 13-11-2025            | 10:30               | 10:45               | 00:15         |

| Przedmiot / temat zajęć                                                                                                                                                                                        | Prowadzący        | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------|---------------------|---------------------|---------------|
| <div>10 z 15</div> Zarządzanie i ochrona danych w przedsiębiorstwie - szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa | Rafał Tomaszewski | 13-11-2025            | 10:45               | 12:15               | 01:30         |
| <div>11 z 15</div> przerwa                                                                                                                                                                                     | Rafał Tomaszewski | 13-11-2025            | 12:15               | 12:30               | 00:15         |
| <div>12 z 15</div> Zarządzanie i ochrona danych w przedsiębiorstwie - szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa | Rafał Tomaszewski | 13-11-2025            | 12:30               | 14:00               | 01:30         |
| <div>13 z 15</div> przerwa                                                                                                                                                                                     | Rafał Tomaszewski | 13-11-2025            | 14:00               | 14:15               | 00:15         |
| <div>14 z 15</div> Zarządzanie i ochrona danych w przedsiębiorstwie - szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa | Rafał Tomaszewski | 13-11-2025            | 14:15               | 15:15               | 01:00         |
| <div>15 z 15</div> Walidacja                                                                                                                                                                                   | -                 | 13-11-2025            | 15:15               | 15:45               | 00:30         |

# Cennik

## Cennik

| Rodzaj ceny                               | Cena         |
|-------------------------------------------|--------------|
| Koszt przypadający na 1 uczestnika brutto | 2 650,00 PLN |
| Koszt przypadający na 1 uczestnika netto  | 2 650,00 PLN |
| Koszt osobogodziny brutto                 | 165,63 PLN   |
| Koszt osobogodziny netto                  | 165,63 PLN   |

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Rafał Tomaszewski

Rafał Tomaszewski to doświadczony trener, który od lat specjalizuje się w wspieraniu przedsiębiorców w prowadzeniu działalności gospodarczej. Jego wszechstronne wykształcenie oraz bogate doświadczenie zawodowe stanowią solidną podstawę dla oferowanych przez niego usług. Posiadając wykształcenie wyższe ekonomiczne, ze specjalnością w rachunkowości, Rafał Tomaszewski rozpoczął swoją karierę zawodową w 2010 roku. Od tego czasu aktywnie wykorzystuje swoją wiedzę i umiejętności w obszarze zarządzania finansami oraz prowadzenia rachunkowości w firmach. Aktualnie, jest certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001, co świadczy o jego zaawansowanych umiejętnościach w zakresie zarządzania ryzykiem i ochrony informacji w firmach. Ponadto, jest absolwentem studiów podyplomowych z zakresu Zarządzania Cyberbezpieczeństwem, co dodatkowo podkreśla jego specjalizację w obszarze bezpieczeństwa IT. Rafał Tomaszewski wyróżnia się profesjonalizmem, zaangażowaniem oraz umiejętnością dostosowywania się do zmieniających się warunków rynkowych i technologicznych. Jego głównym celem jest pomaganie przedsiębiorcom w osiągnięciu sukcesu poprzez efektywne zarządzanie finansami, procesami oraz bezpieczeństwem informacji.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają nagranie ze szkolenia oraz prezentację Power Point przygotowane przez Trenera wysłane na adres e-mail.

### Warunki uczestnictwa

Warunkiem uczestnictwa jest zarejestrowanie się i założenie konta w Bazie Usług Rozwojowych, zapisanie się na szkolenie za pośrednictwem Bazy oraz spełnienie wszystkich warunków określonych przez Operatora, do którego składają Państwo dokumenty o dofinansowanie.

Przed podpisaniem umowy o dofinansowanie szkolenia z Operatorem, skontaktuj się z nami w celu potwierdzenia terminu szkolenia i dostępności wolnych miejsc. Informujemy, że w trakcie szkolenia możliwa jest wizytacja z udziałem PARP, Operatora lub innej jednostki wyznaczonej w celu sprawdzenia poprawności realizacji usługi.

Szkolenie w formie zdalnej będzie odbywało się w czasie rzeczywistym. W zależności od czasu potrzeb będą wykorzystywane różne elementy: ćwiczenia, testy, ankiety, udostępnianie ekranu i inne.

## Informacje dodatkowe

Uwaga:

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Całe szkolenie jest rejestrowane w celach kontroli/audytu. Wykorzystanie nagrania w innym celu niż kontrola/audyt wymaga zgody Trenera i Uczestników.

Uczestnicy otrzymają zaświadczenie, potwierdzające że ukończyli szkolenie.

Forma świadczenia usługi :

Zdalna w czasie rzeczywistym - prowadzona na żywo.

## Warunki techniczne

Wymagania, które muszą zostać spełnione, aby uczestniczyć w szkoleniu na ClickMeeting.:

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);
- 2GB pamięci RAM (zalecane 4GB lub więcej);
- System operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS.

Ponieważ ClickMeeting jest platformą opartą na przeglądarce, wymagane jest korzystanie z najaktualniejszych oficjalnych wersji Google Chrome, Mozilla Firefox, Safari, Edge lub Opera.

ClickMeeting współpracuje z wszystkimi wbudowanymi w laptopy kamerami oraz większością kamer internetowych. Bardziej zaawansowana lub profesjonalna kamera może wymagać instalacji dodatkowego oprogramowania lub sprzętu.

Aby móc korzystać z usługi na niektórych urządzeniach mobilnych, konieczne może być pobranie odpowiedniej aplikacji w iTunes App Store lub Google Play Store. Do korzystania z usługi w pełnym zakresie dźwięku i obrazu podczas konferencji, konieczne jest posiadanie zestawu słuchawkowego, lub głośników podłączonych do urządzenia i rozpoznanych przez Państwa urządzenie i nie powinny być one jednocześnie używane przez żadną inną aplikację.

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Metody pracy podczas szkolenia on-line:

- wygodna forma szkolenia - wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki
- szkolenie realizowane jest w nowoczesnej formie w wirtualnym pokoju konferencyjnym i kameralnej grupie uczestników
- bierzesz udział w pełnowartościowym szkoleniu - Trener prowadzi zajęcia "na żywo" - widzisz go i słyszysz
- pokaz prezentacji, ankiet i ćwiczeń widzisz na ekranie swojego komputera w czasie rzeczywistym.

# Kontakt



**Aleksandra Kozak**

**E-mail** [a.jonca@fpd.pl](mailto:a.jonca@fpd.pl)

**Telefon** (+48) 574 157 925