



FUNDACJA
ROZWOJU
KOMPETENCJI I
PRZEDSIĘBIORCZO
ŚCI PROAKTYWNI



Bezpieczeństwo cyfrowe - zapobieganie i reagowanie na zagrożenia

Numer usługi 2024/09/30/137673/2336008

📍 zdalna w czasie rzeczywistym
🏠 Usługa szkoleniowa
🕒 24 h
📅 10.09.2025 do 10.10.2025

2 160,00 PLN brutto
2 160,00 PLN netto
90,00 PLN brutto/h
90,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Do udziału w szkoleniu zapraszamy wszystkie osoby zainteresowane bezpiecznym korzystaniem z Internetu – zarówno w życiu prywatnym, jak i zawodowym, m.in.: - pracowników firm – szczególnie działów IT i administracji, - specjalistów ds. bezpieczeństwa i/lub ochrony danych osobowych, - menadżerów, kierowników, przedsiębiorców, - rodziców, opiekunów, nauczycieli.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	03-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest zwiększenie świadomości uczestników na temat zagrożeń w cyberprzestrzeni oraz nauczenie ich praktycznych umiejętności i dobrych praktyk w zakresie ochrony danych i systemów informatycznych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik po udziale w szkoleniu: - definiuje podstawowe pojęcia związane z bezpieczeństwem cyfrowym, - wymienia i omawia rodzaje zagrożeń z uwzględnieniem obecnych trendów (phishing, scam), - charakteryzuje rodzaje złośliwego oprogramowania i metody ochrony przed infekcją, - zna zasady tworzenia silnych haseł i ich bezpiecznego przechowywania, - zna metody szyfrowania i zabezpieczania danych w chmurze.	Uczestnik prowadzi swobodną rozmowę na tematy związane z cyberbezpieczeństwem.	Test teoretyczny z wynikiem generowanym automatycznie
UMIEJĘTNOŚCI: Uczestnik po udziale w szkoleniu: - korzysta z narzędzi do zarządzania hasłami, - stosuje różnego rodzaju techniki uwierzytelniania, - zabezpiecza urządzenia cyfrowe przed złośliwym oprogramowaniem, - rozpoznaje zaufane strony i unika niebezpiecznych, - stosuje metody bezpiecznego zarządzania danymi osobowymi, - konfiguruje routery i zabezpiecza sieci wi-fi, - zabezpiecza urządzenia mobile tj. smartfon, tablet, - aktualizuje systemy operacyjne i aplikacje w celach bezpieczeństwa.	Uczestnik wykonuje samodzielnie zadania praktyczne w zakresie cyberbezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
KOMPETENCJE SPOŁECZNE: Uczestnik po udziale w szkoleniu: - jest świadomy zagrożeń związanych z cyberprzestrzenią, - korzysta z narzędzi cyfrowych w sposób świadomy i odpowiedzialny, - współpracuje z innymi w celu zabezpieczenia wspólnego dobra np. danych osobowych i plików firmowych, - promuje zasady bezpiecznego korzystania z technologii.	Uczestnik rozwiązuje case study przy współpracy z innymi kursantami, poprzez analizę danego przypadku i zaproponowanie rozwiązania.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak - Dokument zawiera opis efektów uczenia.

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

Tak - Walidacja zostanie przeprowadzona w oparciu o zdefiniowane wcześniej kryteria weryfikacji.

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

Tak - Walidację przeprowadza osoba, która nie prowadziła zajęć.

Program

- 1. Podstawowe pojęcia związane z bezpieczeństwem cyfrowym
- 2. Rodzaje zagrożeń z uwzględnieniem obecnych trendów (phishing, scam)
- 3. Rodzaje złośliwego oprogramowania i metody ochrony przed infekcją
- 4. Zasady tworzenia silnych haseł i ich bezpiecznego przechowywania
- 5. Metody szyfrowania i zabezpieczania danych w chmurze
- 6. Narzędzia do zarządzania hasłami i techniki uwierzytelniania
- 7. Zabezpieczanie urządzeń cyfrowych przed złośliwym oprogramowaniem
- 8. Rozpoznawania stron zaufanych i niebezpiecznych
- 9. Metody bezpiecznego zarządzania danymi osobowymi
- 10. Konfiguracja routerów i zabezpieczanie sieci wi-fi
- 11. Zabezpieczanie urządzeń mobilnych tj. smartfon, tablet
- 12. Aktualizacja systemów operacyjnych i aplikacji

Harmonogram

Liczba przedmiotów/zajęć: 0

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

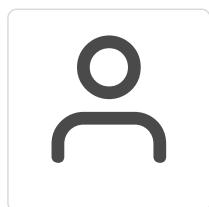
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 160,00 PLN
Koszt przypadający na 1 uczestnika netto	2 160,00 PLN
Koszt osobogodziny brutto	90,00 PLN
Koszt osobogodziny netto	90,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Grzegorz Foltak

opis zostanie zamieszczony wkrótce

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały elektroniczne opracowane przez prowadzącego szkolenie.

Informacje dodatkowe

Terminy szkoleń zostaną ustalone wspólnie po zebraniu się grupy i skonsultowaniu potrzeb poszczególnych uczestników. Harmonogram zostanie umieszczony co najmniej 5 dni przed rozpoczęciem szkolenia.

W szkoleniu mogą wziąć udział osoby z projektu Małopolski Pociąg do Kariery, Marr Bony Nowa Perspektywa, Kierunek-Rozwój oraz osoby spoza projektu. Prosimy o kontakt w sprawie szczegółów.

Warunki techniczne

Komputer/urządzenie mobilne z dostępem do Internetu i kamery.

Kontakt



Fundacja Proaktywni



E-mail poczta@fundacjaproaktywni.pl

Telefon (+48) 533 442 199