Możliwość dofinansowania

Cyberbezpieczeństwo dla seniorów – bezpieczne korzystanie z telefonu, internetu i bankowości elektronicznej

Numer usługi 2026/03/17/186688/3411987

1 600,00 PLN brutto
1 600,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
196,00 PLN cena rynkowa

MI6 Michał Pisańczuk

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
20.04.2026 do 21.04.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Osoby w wieku 40+, które korzystają lub zamierzają korzystać z telefonu komórkowego, internetu, poczty elektronicznej, bankowości elektronicznej, komunikatorów oraz serwisów społecznościowych i chcą zwiększyć bezpieczeństwo swoich działań w środowisku cyfrowym. Szkolenie jest skierowane do osób, które chcą nauczyć się rozpoznawać typowe zagrożenia cyberbezpieczeństwa oraz właściwie reagować w sytuacji próby oszustwa lub utraty danych.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	17-04-2026
Forma prowadzenia usługi	zdalna 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 usługi jest przygotowanie uczestników do bezpiecznego korzystania z telefonu, internetu, bankowości elektronicznej i mediów społecznościowych poprzez rozpoznawanie typowych cyberzagrożeń, ocenę ryzyka w

codziennych sytuacjach online, stosowanie podstawowych zasad ochrony danych i środków finansowych oraz podejmowanie właściwych działań w przypadku podejrzenia oszustwa lub incydentu bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje typowe mechanizmy cyberoszustw kierowanych do osób starszych.	identyfikuje cechy oszustw telefonicznych, SMS-owych i internetowych	Test teoretyczny
	odróżnia legalny kontakt od próby wyłudzenia	Test teoretyczny
	wskazuje sygnały ostrzegawcze w przykładowych komunikatach	Test teoretyczny
Ocenia wiarygodność wiadomości, linków, stron internetowych i ofert internetowych.	sprawdza podstawowe elementy wiarygodności strony lub wiadomości	Test teoretyczny
	wskazuje błędy, nietypowe adresy, presję czasu i próby wyłudzenia danych	Test teoretyczny
	odróżnia bezpieczną ofertę od podejrzanej	Test teoretyczny
Stosuje zasady bezpiecznego korzystania z bankowości elektronicznej, BLIK i zakupów online.	dobiera właściwy sposób postępowania przy płatności internetowej	Test teoretyczny
	wskazuje zasady ochrony kodu BLIK i danych bankowych	Test teoretyczny
	rozpoznaje niebezpieczne zachowania podczas zakupów i sprzedaży online	Test teoretyczny
Stosuje podstawowe zasady ochrony kont, urządzeń i danych osobowych.	wykorzystuje zasady tworzenia bezpiecznego hasła	Test teoretyczny
	wskazuje działania zwiększające bezpieczeństwo urządzenia	Test teoretyczny
	rozróżnia dane, których nie należy udostępniać	Test teoretyczny
	dobiera właściwe ustawienia i nawyki zwiększające prywatność	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Podejmuje właściwe działania po stwierdzeniu lub podejrzeniu incydentu bezpieczeństwa.	wskazuje kolejność działań po oszustwie lub utracie danych	Test teoretyczny
	dobiera instytucję właściwą do zgłoszenia incydentu	Test teoretyczny
	przygotowuje plan reakcji w sytuacji zagrożenia	Test teoretyczny

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

Dzień 1. Rozpoznawanie zagrożeń

1. Wprowadzenie do tematu cyberbezpieczeństwa seniorów
2. Najczęstsze mechanizmy oszustw telefonicznych i SMS-owych
3. Rozpoznawanie phishingu, smishingu i vishingu
4. Identyfikowanie fałszywych stron internetowych
5. Bezpieczne zakupy online i korzystanie z platform ogłoszeniowych
6. Ćwiczenia praktyczne z analizy komunikatów, wiadomości i scenariuszy oszustw

Dzień 2. Ochrona siebie i swoich środków

1. Rozpoznawanie oszustw inwestycyjnych i fałszywych zbiórek
2. Bezpieczne korzystanie z BLIK, bankowości online i mediów społecznościowych
3. Tworzenie i stosowanie bezpiecznych haseł
4. Podstawowe zasady ochrony urządzeń i prywatności
5. Postępowanie po incydencie bezpieczeństwa
6. Ćwiczenia praktyczne, analiza przypadków i podsumowanie szkolenia

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Powitanie i „cyfrowy świat seniora" + Quiz wstępny	Trener	20-04-2026	08:00	10:00	02:00
2 z 15 Przerwa 1	Trener	20-04-2026	10:00	10:30	00:30
3 z 15 Oszustwa telefoniczne i SMS – przekręt na wnuczka, na policjanta/bank, smishing, vishing	Trener	20-04-2026	10:30	12:30	02:00
4 z 15 Przerwa 2	Trener	20-04-2026	12:30	13:00	00:30
5 z 15 cd.: Ćwiczenia warsztatowe – odgrywanie ról, analiza SMS-ów	Trener	20-04-2026	13:00	14:30	01:30
6 z 15 Przerwa 3	Trener	20-04-2026	14:30	15:00	00:30
7 z 15 Phishing i fałszywe strony internetowe | Zakupy online (Allegro, OLX) + Quiz podsumowujący Dzień 1 + zadanie domowe	Trener	20-04-2026	15:00	16:00	01:00
8 z 15 Omówienie zadania domowego + Przekręty inwestycyjne i finansowe + Fałszywe zbiórki charytatywne	Trener	21-04-2026	08:00	10:00	02:00
9 z 15 Przerwa 1	Trener	21-04-2026	10:00	10:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 15 BLIK i przekręt na BLIK | Bankowość online | Facebook, WhatsApp i media społecznościowe	Trener	21-04-2026	10:30	12:30	02:00
11 z 15 Przerwa 2	Trener	21-04-2026	12:30	13:00	00:30
12 z 15 Bezpieczne hasła, urządzenia i prywatność w sieci	Trener	21-04-2026	13:00	14:00	01:00
13 z 15 Przerwa 3	Trener	21-04-2026	14:00	14:30	00:30
14 z 15 Co zrobić gdy zostałem ofiarą? Pomoc i kontakty.	Trener	21-04-2026	14:30	15:30	01:00
15 z 15 Walidacja efektów uczenia się	-	21-04-2026	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 600,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	1 600,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Trener

Trener

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują materiały szkoleniowe wspierające utrwalenie wiedzy i stosowanie zasad bezpieczeństwa w codziennym korzystaniu z internetu, w tym:

- prezentację szkoleniową omawianą podczas zajęć,
- checklistę „Jak rozpoznać podejrzaną wiadomość lub próbę oszustwa”,
- zestaw podstawowych zasad bezpiecznego korzystania z internetu i urządzeń cyfrowych,
- krótkie materiały podsumowujące najważniejsze dobre praktyki bezpieczeństwa.

Materiały przekazywane są w formie elektronicznej lub drukowanej.

Warunki uczestnictwa

Warunkiem otrzymania zaświadczenia/dyplomu jest udział w minimum 80% zajęć w ramach usługi rozwojowej oraz podejscie do walidacji

Informacje dodatkowe

W trakcie każdego dnia szkoleniowego, zgodnie z obowiązującymi wytycznymi, przewidziane są przerwy ujęte w harmonogramie zajęć iwliczone w cenę usługi rozwojowej. Zajęcia realizowane są w godzinach zegarowych. Po zakończeniu udziału w usłudze rozwojowejuczestnik otrzymuje zaświadczenie/certyfikat potwierdzający jej ukończenie oraz dokonuje oceny usługi w Bazie Usług Rozwojowych.

Warunki techniczne

Platforma realizacji szkolenia: Zoom

Wymagania techniczne dotyczące udziału w szkoleniu na platformie Zoom:

1. **Sprzęt komputerowy:**
   - Uczestnik powinien dysponować komputerem stacjonarnym lub laptopem (PC lub Mac) z dostępem do sieci internet.Rekomendowane jest posiadanie kamery internetowej oraz mikrofonu w celu aktywnego udziału w zajęciach.
2. **Przeglądarka internetowa:**
   - Zalecane jest korzystanie z aktualnych wersji przeglądarek internetowych, takich jak Google Chrome, Mozilla Firefox lub Safari, w celuzapewnienia prawidłowego działania platformy.
3. **Połączenie interneto**we:
   - Wymagane jest stabilne połączenie internetowe o minimalnej przepustowości 2 Mbps umożliwiające udział w sesjach wideo. Dlazwiększenia stabilności połączenia rekomendowane jest korzystanie z łącza przewodowego.
4. **Platforma Zoom:**

- - - - Przed rozpoczęciem szkolenia konieczne jest pobranie i zainstalowanie aktualnej wersji aplikacji Zoom oraz posiadanie aktywnegokonta użytkownika (z możliwością założenia bezpłatnego konta).

5. **System operacyjny:**
   - Szkolenie jest kompatybilne z systemami operacyjnymi Windows oraz macOS.

6. **Oprogramowanie dodatkowe:**
   - Rekomendowane jest korzystanie z aktualnych wersji niezbędnego oprogramowania systemowego oraz przeglądarkowego w celuzapewnienia prawidłowej pracy środowiska szkoleniowego.

7. **Dźwięk:**
   - Zaleca się korzystanie ze słuchawek z mikrofonem w celu poprawy jakości dźwięku oraz wcześniejsze sprawdzenie poprawnościdziałania sprzętu audio.

Przygotowanie do szkolenia:

- Uczestnik powinien przed rozpoczęciem zajęć przetestować sprzęt oraz połączenie internetowe oraz zapewnić sobie ciche ikomfortowe miejsce pracy.

Wsparcie techniczne:

- W trakcie realizacji szkolenia zapewniony jest kontakt z pomocą techniczną na wypadek wystąpienia problemów technicznych.

Spełnienie powyższych wymagań technicznych umożliwia sprawną realizację szkolenia, minimalizuje ryzyko zakłóceń oraz zapewniaefektywną komunikację pomiędzy prowadzącym a uczestnikami.

Kontakt

MICHAŁ PISAŃCZUK

E-mail szkolenia@pisanczuk.com
Telefon (+48) 504 382 739