



IQ CONSULTING
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ



Podstawy bezpieczeństwa w Internecie – kurs dla seniora

Numer usługi 2025/05/14/120895/2744810

📍 Opole / stacjonarna

👤 Usługa szkoleniowa

🕒 32 h

📅 25.07.2025 do 27.07.2025

5 500,00 PLN brutto

5 500,00 PLN netto

171,88 PLN brutto/h

171,88 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Grupą docelową kursu „ Podstawy bezpieczeństwa w Internecie – kurs dla seniora ” są osoby starsze, które chcą bezpiecznie korzystać z Internetu, ale nie czują się pewnie w świecie cyfrowym. Uczestnikami kursu będą seniorzy o niskim lub średnim poziomie kompetencji cyfrowych, którzy korzystają z komputera, smartfona lub tabletu do codziennych czynności, takich jak kontakt z rodziną, przeglądanie wiadomości czy bankowość internetowa. Kurs jest skierowany do osób, które chcą zwiększyć swoją wiedzę na temat zagrożeń w sieci oraz nauczyć się, jak chronić swoje dane i bezpiecznie poruszać się w Internecie.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	24-07-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	32

Cel

Cel edukacyjny

Celem szkolenia jest zwiększenie świadomości i kompetencji cyfrowych uczestników w zakresie bezpiecznego korzystania z Internetu. Uczestnicy zdobędą podstawową wiedzę na temat zagrożeń online (takich jak oszustwa, wirusy, phishing) oraz nauczą się praktycznych umiejętności chronienia swoich danych osobowych, haseł i urządzeń. Szkolenie ma na celu nie tylko podnieść poziom bezpieczeństwa cyfrowego seniorów, ale także zwiększyć ich pewność.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia podstawowe zagrożenia internetowe, takie jak phishing, wirusy czy oszustwa.	Prawidłowo identyfikuje co najmniej trzy typy zagrożeń (np. phishing, wirusy, fałszywe strony).	Wywiad swobodny
Definiuje zasady tworzenia silnych i bezpiecznych haseł.	Podaje minimum trzy cechy silnego hasła (np. długość, znaki specjalne, brak danych osobowych).	Obserwacja w warunkach rzeczywistych
Charakteryzuje bezpieczne zachowania podczas korzystania z poczty elektronicznej i mediów społecznościowych.	Opisuje przynajmniej trzy sposoby bezpiecznego korzystania z e-maila i mediów społecznościowych.	Wywiad swobodny
Uzasadnia potrzebę ochrony danych osobowych w Internecie.	Wyjaśnia, dlaczego ochrona danych osobowych jest ważna, podając co najmniej jeden przykład możliwych konsekwencji ich utraty.	Wywiad swobodny
Kontroluje ustawienia bezpieczeństwa na swoich urządzeniach i w przeglądarce internetowej.	Samodzielnie sprawdza lub modyfikuje co najmniej jedno ustawienie bezpieczeństwa w systemie lub przeglądarce.	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, dokument potwierdza uzyskanie kompetencji i zawiera opis efektów uczenia się.

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

Tak, dokument potwierdza, że walidacja przeprowadzona jest w w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji

Program

Szkolenie trwa 32 godziny dydaktyczne (24 godzin zegarowych). Jedna godzina dydaktyczna trwa 45 minut. Każdego dnia przewidziana jest przerwa 30 minutowa o godz.12:00

Dzień 1

Moduł 1: Wprowadzenie do Internetu i zagrożeń cyfrowych

- Powitanie uczestników, omówienie celów i zasad szkolenia
- Podstawowe pojęcia: Internet, przeglądarka, strony internetowe
- Rodzaje zagrożeń w sieci: wirusy, phishing, fałszywe wiadomości
- Rozpoznawanie podejrzanych wiadomości i stron internetowych
- Ćwiczenia praktyczne: analiza przykładowych zagrożeń
- Dyskusja i pytania

Moduł 2: Hasła i logowanie – ochrona tożsamości w sieci

- Jak tworzyć silne hasła
- Czego unikać przy tworzeniu haseł
- Zarządzanie hasłami: notowanie vs menedżery haseł
- Logowanie dwuetapowe (2FA) – podstawy i przykłady
- Ćwiczenia praktyczne: tworzenie haseł, ocena siły hasła

Dzień 2

Moduł 3: Ochrona prywatności i danych osobowych

- Co to są dane osobowe i jak można je stracić
- Jakie dane można udostępniać w Internecie, a jakie nie
- Ochrona prywatności w mediach społecznościowych
- Ustawienia prywatności w przeglądarkach
- Ćwiczenia praktyczne: przegląd ustawień prywatności

Moduł 4: Bezpieczne korzystanie z e-maila i komunikatorów

- Rozpoznawanie podejrzanych e-maili i linków
- Jak działa phishing i jak się przed nim bronić
- Bezpieczne przesyłanie informacji
- Ćwiczenia praktyczne: analiza fałszywych e-maili, bezpieczne odpowiedzi

Dzień 3

Moduł 5: Zakupy online i bankowość internetowa – bezpieczne transakcje

- Jak rozpoznać bezpieczne sklepy internetowe
- Szyfrowanie strony i certyfikat SSL – jak je sprawdzić
- Zasady bezpiecznych płatności online
- Bankowość elektroniczna – jak korzystać, by się nie narazić
- Ćwiczenia praktyczne: analiza stron zakupowych, symulacja bezpiecznego zakupu

Moduł 6: Podstawowe ustawienia bezpieczeństwa w urządzeniach i sieci

- Aktualizacje systemu i programów
- Oprogramowanie antywirusowe i zapora sieciowa
- Korzystanie z publicznych sieci Wi-Fi – co warto wiedzieć
- Ćwiczenia praktyczne: sprawdzanie ustawień na własnych urządzeniach

Harmonogram

Liczba przedmiotów/zajęć: 12

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Powitanie uczestników, omówienie celów i zasad szkolenia	Marek Wendreński	25-07-2025	08:00	10:00	02:00
2 z 12 Prezentowanie podstawowych pojęć: Internet, przeglądarka, strony internetowe	Marek Wendreński	25-07-2025	10:00	12:00	02:00
3 z 12 Prezentowanie rodzajów zagrożeń w sieci: wirusy, phishing, fałszywe wiadomości	Marek Wendreński	25-07-2025	12:30	14:30	02:00
4 z 12 Prezentowanie postępowania w przypadku podejrzanych wiadomości i stron internetowych	Marek Wendreński	25-07-2025	14:30	16:30	02:00
5 z 12 Jak tworzyć silne hasła oraz czego unikać przy tworzeniu haseł	Marek Wendreński	26-07-2025	08:00	10:00	02:00
6 z 12 Zarządzanie hasłami: notowanie vs menedżery haseł	Marek Wendreński	26-07-2025	10:00	12:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 12 Co to są dane osobowe i jak można je stracić oraz czego nie udostępniać	Marek Wendreński	26-07-2025	12:30	14:30	02:00
8 z 12 Ochrona prywatności w mediach społecznościowych oraz rozpoznawanie podejrzanych e-maili i linków	Marek Wendreński	26-07-2025	14:30	16:30	02:00
9 z 12 Zasady bezpiecznych płatności online oraz jak rozpoznać bezpieczne sklepy internetowe	Marek Wendreński	27-07-2025	08:00	10:00	02:00
10 z 12 Bankowość elektroniczna – jak korzystać, by się nie narazić	Marek Wendreński	27-07-2025	10:00	12:00	02:00
11 z 12 Aktualizacje systemu i programów oraz oprogramowanie antywirusowe i zapora sieciowa	Marek Wendreński	27-07-2025	12:30	14:30	02:00
12 z 12 Walidacja szkolenia	-	27-07-2025	14:00	16:00	02:00

Cennik

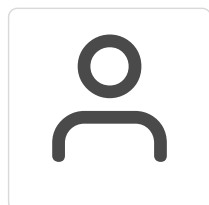
Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 500,00 PLN

Koszt przypadający na 1 uczestnika netto	5 500,00 PLN
Koszt osobogodziny brutto	171,88 PLN
Koszt osobogodziny netto	171,88 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Marek Wendreński

Zajmuje się tematyką social media od ponad 10 lat.

Dzięki social mediom zbudował rozpoznawalną markę osobistą, rozwinął biznesy, a teraz przekazuje wiedzę jak inni mogą duplikować najskuteczniejszą strategię działania.

Podczas szkolenia dzięki Markowi dowiesz się:

- Jak zbudować markę od 0
- Jak zwiększyć dwukrotnie ilość klientów w przeciągu 1 miesiąca po szkoleniu
- Jak rozwinąć biznes Beauty w czasie pandemii
- Jak zbudować strategię działania, której nie będzie w stanie skopiować konkurencja
- Jak podglądać konkurencję i wyprzedzić jej działania
- Jak tworzyć jedyne w swoim rodzaju treści oraz kanały przekazu
- Jak szybko się wybić na tle konkurencji
- Jak nawiązać nowe współprace
- Jak trafić do telewizji, radia oraz na 1 strony gazet
- Jak dzięki 1 skryptowi zbudujesz najlepsze oferty w internecie
- Jak zbudować konto na tik toku od 0 do 100 000 obserwujących w kilka miesięcy
- Jak tworzyć kampanie reklamowe wydając ułamek budżetu marketingowego

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały są przygotowane w formie elektronicznej.

Warunki uczestnictwa

Poziom frekwencji na szkoleniu pozwalający na wydanie zaświadczenia o ukończeniu szkolenia powinien wynosić 100%.

Informacje dodatkowe

Uczestnicy szkolenia otrzymają zaświadczenie o odbyciu szkolenia oraz certyfikat potwierdzający nabyte umiejętności, które stanowią potwierdzenie nabytych kompetencji podczas szkolenia.

W przypadku uczestnictwa w usłudze osoby z niepełnosprawnością dostawca usługi zapewni realizację usługi rozwojowej uwzględniając potrzeby osób z niepełnosprawnościami (w tym również dla osób ze szczególnymi potrzebami) zgodnie ze Standardami dostępności dla polityki spójności 2021-2027.

Adres

ul. Krakowska 32

45-075 Opole

woj. opolskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



Bartosz Grzywa

E-mail bartosz.grzywa@iq-consulting.pl

Telefon (+48) 723 552 443