



Keystone Consulting
Sp. z o.o.

★★★★★ 4,9 / 5

153 oceny

Bezpieczny senior w sieci – mądrość, spokój i odwaga w cyfrowym świecie.

Numer usługi 2025/02/04/12632/2540849

📍 Katowice / stacjonarna

🏠 Usługa szkoleniowa

🕒 8 h

📅 20.09.2025 do 21.09.2025

2 500,00 PLN brutto

2 500,00 PLN netto

312,50 PLN brutto/h

312,50 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie jest skierowane do osób starszych i seniorów, którzy:

1. Chcą korzystać z internetu, ale obawiają się zagrożeń związanych z technologią.
2. Chcą nauczyć się, jak chronić swoje dane osobowe i unikać oszustw.
3. Pragną lepiej rozumieć zasady działania internetu, aby wykorzystywać go w codziennym życiu.
4. Chcą czuć się pewniej i bezpieczniej podczas korzystania z komputera, telefonu czy innych urządzeń.

To szkolenie jest doskonałym wyborem zarówno dla osób początkujących w korzystaniu z internetu, jak i tych, które chcą uporządkować swoją wiedzę i zwiększyć swoje

bezpieczeństwo w sieci.

Minimalna liczba uczestników

15

Maksymalna liczba uczestników

30

Data zakończenia rekrutacji

15-09-2025

Forma prowadzenia usługi

stacjonarna

Liczba godzin usługi

8

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 szkolenia jest edukacja osób starszych w zakresie bezpiecznego i świadomego korzystania z internetu. Wyposaża uczestników w wiedzę i praktyczne umiejętności pozwalające unikać zagrożeń w sieci, takich jak oszustwa, wyłudzenia danych, czy manipulacje emocjonalne. Ponadto, program wspiera rozwijanie pewności siebie w świecie cyfrowym, umożliwiając korzystanie z internetu w sposób bezpieczny, świadomy i komfortowy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po ukończeniu szkolenia uczestnicy: 1.Zrozumieją znaczenie obecności w sieci oraz korzyści i zagrożenia z nią związane. 2.Będą świadomi wpływu postępu technologicznego na życie codzienne i sposoby adaptacji do zmian. 3.Rozpoznają zagrożenia związane z bezpieczeństwem w internecie i będą potrafili stosować podstawowe zasady ochrony danych. 4.Nauczą się identyfikować oraz reagować na zagrożenia takie jak spoofing, phishing, smishing i vishing. 5.Zdobędą umiejętność podejmowania świadomych decyzji i budowania schematów postępowania w sytuacjach zagrożenia. 6.Będą potrafili zarządzać emocjami w kontekście cyberzagrożeń i unikać działań pod wpływem paniki. 7.Poznają dostępne źródła informacji i pomocy w przypadku cyberataków lub oszustw internetowych. 8.Zwiększą swoją pewność siebie w korzystaniu z internetu, rozwijaniu kompetencji cyfrowych i komunikacji online.	1. Zrozumienie znaczenia obecności w sieci oraz korzyści i zagrożeń z nią związanych 2. Świadomość wpływu postępu technologicznego i sposobów adaptacji do zmian 3. Rozpoznawanie zagrożeń w sieci i stosowanie zasad ochrony danych 4. Identyfikacja oraz reakcja na zagrożenia (spoofing, phishing, smishing, vishing) 5. Tworzenie i stosowanie schematów postępowania w sytuacjach zagrożenia 6. Zarządzanie emocjami w sytuacjach cyberzagrożeń 7. Znajomość źródeł informacji i miejsc wsparcia w przypadku cyberzagrożeń	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

1. "Strach ma wielkie oczy" (Wprowadzenie do tematu)

1.1. Co nas popycha do obecności w sieci?

Omówienie korzyści z obecności w internecie.

Dyskusja: Jakie są Wasze główne powody korzystania z internetu?

1.2. Postęp technologiczny i ewolucja technologii – jak za tym nadążyć?

2. "Jak sobie pościelisz, tak się wyśpisz" (Świadomość i bezpieczeństwo w sieci)

2.1. Budowanie świadomości w sieci – walka dobra ze złem

2.2. Co to znaczy bezpieczeństwo w sieci i jak je sobie zapewnić?

3. "Gdyby kózka nie skakała, toby nóżki nie złamała" (O zagrożeniach w sieci)

3.1. Prawdziwe historie – przykłady osób dotkniętych oszustwami w sieci

Dyskusja: Jakie emocje budzą te historie? Czy uczestnicy mieli podobne doświadczenia?

3.2. Warsztaty zachowań

Symulacje: co zrobić, gdy otrzymasz podejrzanego e-maila lub telefon?

3.3. Budowa schematów postępowania w sytuacjach podejrzanych

4. "Złość piękności szkodzi, a panika rozumowi" (Emocje i zagrożenia w sieci)

4.1. Emocje a działanie – jak nie stracić głowy?

4.2. Spoofing, phishing, smishing, vishing – „fishing”? Idziemy na ryby?

4.3. Warsztaty emocji

5. "Pod dobrą opieką nawet wilk nie straszny" (Gdzie szukać pomocy i informacji)

5.1. Jak samemu znaleźć informacje o zagrożeniach i ich zapobieganiu?

5.2. Gdzie i kiedy szukać pomocy w nagłych sytuacjach?

5.3. Ważne adresy i telefony

6. "Nie taki diabeł straszny, jak go malują" (Zakończenie z optymizmem)

6.1. Rozwój osobisty w sieci

6.2. Kontakt z innymi

6.3. Warsztat: Co nowego chcielibyście poznać w sieci, ale boicie się zacząć?

7. Podsumowanie

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	2 500,00 PLN
Koszt przypadający na 1 uczestnika netto	2 500,00 PLN
Koszt osobogodziny brutto	312,50 PLN
Koszt osobogodziny netto	312,50 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Anna Malinowska

Trenerka zarządzania projektami, ryzykiem i kryzysami. Absolwentka Politechniki Śląskiej oraz CEDEP, doświadczona menedżerka i trenerka z ponad 20-letnim doświadczeniem w zarządzaniu projektami, jakością, ryzykiem i kryzysami, głównie w branży motoryzacyjnej na poziomie korporacyjnym. Specjalizuje się w szkoleniach z zakresu zarządzania zmianą, problemami oraz ryzykiem, a także w kształtowaniu postaw przywódczych i doskonaleniu umiejętności zarządzania zespołami w sytuacjach kryzysowych. Prowadzi warsztaty i szkolenia dla menedżerów, liderów oraz specjalistów, przekazując wiedzę w sposób praktyczny, oparty na realnych przykładach oraz własnych doświadczeniach z zarządzania globalnymi projektami i wielomilionowymi budżetami. Dodatkowo specjalizuje się w tematyce cyberbezpieczeństwa, podkreślając znaczenie ochrony danych, bezpiecznych praktyk online i zarządzania ryzykiem związanym z cyfrowym środowiskiem pracy. Wspiera organizacje w budowaniu świadomości zagrożeń cybernetycznych oraz wprowadzaniu polityk bezpieczeństwa IT, minimalizując ryzyko ataków i naruszeń danych. W swoim dorobku trenerskim ma ponad 1000 godzin szkoleń przeprowadzonych w firmach, w których pracowała oraz dla przedstawicieli różnych branż – od przemysłu, przez finanse, po sektor usługowy. Jest również mentorką i certyfikowanym coachem, wspierającą rozwój kompetencji

liderskich i strategicznego podejścia do zarządzania.
Wyróżnia się zdolnością do przekazywania wiedzy w sposób inspirujący i angażujący.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały trenera, skrypt, wysłane w formie elektronicznej.

Warunki uczestnictwa

W przypadku szkoleń dofinansowanych warunkiem uczestnictwa w szkoleniach jest założenie przez Uczestnika konta w Bazie Usług Rozwojowych oraz spełnienie warunków, które są przedstawione przez danego Operatora, do którego składane są dokumenty o dofinansowanie do usługi rozwojowej.

Informacje dodatkowe

Podczas szkolenia przewidziane są przerwy.

Karta usługi zawiera stawkę VAT zw na podstawie §3. 1pkt 14 rozporządzenia Ministra Finansów z 20 grudnia 2013 roku w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. 2015, poz. 736, z późn. zm.) w związku z tym ta karta dotyczy podmiotów które mają dofinansowanie na poziomie pow. 70%. W innym przypadku prosimy o kontakt z realizatorem usługi.

Warunkiem otrzymania zaświadczenia jest 80% frekwencja.

Szkolenie realizowane jest w godzinach dydaktycznych 1 godzina = 45 minut

Uczestnik otrzymuje odpowiednie Zaświadczenie/Certyfikat informujące o ukończeniu szkolenia Bezpieczny senior w sieci – mądrość, spokój i odwaga w cyfrowym świecie.

Adres

ul. Kormoranów 1
40-521 Katowice
woj. śląskie

Kontakt



Anna Wiatrowska

E-mail anna.wiatrowska@keystone.com.pl

Telefon (+48) 663 992 525