



CENTRUM
INNOWACYJNYCH
ROZWIĄZAŃ
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,9 / 5

26 ocen

Szkolenie: Aktywni i Bezpieczni w Sieci – cyberbezpieczeństwo z uwzględnieniem kompetencji cyfrowych i zielonych kompetencji

Numer usługi 2026/07/28/201147/3714139

📍 Gliwice

🏢 Usługa szkoleniowa

📅 stacjonarna

👥 Zajęcia grupowe

🕒 08:00 h

📅 07.10.2026 do 14.10.2026

1 906,50 PLN brutto

1 550,00 PLN netto

238,31 PLN brutto/h

193,75 PLN netto/h

233,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Internet

Grupa docelowa usługi

Usługa skierowana jest do osób dorosłych, które z własnej inicjatywy chcą nabyć lub podnieść kwalifikacje w zakresie bezpiecznego korzystania z Internetu, rozwijając jednocześnie kompetencje cyfrowe oraz zielone kompetencje związane z odpowiedzialnym wykorzystywaniem technologii cyfrowych.

W szczególności usługa przeznaczona jest dla:

- osób korzystających z Internetu w życiu prywatnym i zawodowym,
- pracowników administracji, biur, edukacji, organizacji i przedsiębiorstw,
- osób pracujących lub planujących pracę zdalną, hybrydową lub biurową,
- seniorów oraz osób o podstawowych kompetencjach cyfrowych,
- osób chcących skutecznie rozpoznawać zagrożenia online, chronić swoje dane i urządzenia oraz rozwijać bezpieczne nawyki cyfrowe zgodne z zasadami odpowiedzialnego korzystania z zasobów cyfrowych.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji

05-10-2026

Forma prowadzenia usługi

stacjonarna

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do bezpiecznego i świadomego korzystania z Internetu oraz technologii cyfrowych. Rozwija kompetencje cyfrowe w zakresie rozpoznawania zagrożeń online, ochrony danych, bezpiecznego korzystania z poczty elektronicznej, bankowości internetowej i aplikacji cyfrowych. Kształtuje zielone kompetencje zgodne z klasyfikacją ESCO poprzez odpowiedzialne korzystanie z technologii cyfrowych oraz racjonalne wykorzystywanie zasobów cyfrowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe zagrożenia cyberbezpieczeństwa oraz wyjaśnia zasady bezpiecznego i odpowiedzialnego korzystania z technologii cyfrowych z uwzględnieniem zielonych kompetencji. Rozpoznaje próby oszustw internetowych, telefonicznych i SMS oraz stosuje zasady ograniczonego zaufania podczas korzystania z usług cyfrowych.	rozróżnia najczęściej występujące zagrożenia w Internecie (m.in. phishing, smishing, vishing);	Test teoretyczny
	wyjaśnia znaczenie kompetencji cyfrowych i zielonych kompetencji;	Test teoretyczny
	wskazuje wpływ korzystania z technologii cyfrowych na środowisko oraz sposoby ograniczania śladu cyfrowego.	Test teoretyczny
	identyfikuje cechy charakterystyczne fałszywych wiadomości i prób wyłudzenia danych;	Test teoretyczny
	wskazuje właściwy sposób postępowania po otrzymaniu podejrzanego wiadomości lub telefonu;	Test teoretyczny
	rozpoznaje przykłady manipulacji wykorzystywanych przez cyberprzestępców.	Test teoretyczny
Stosuje zasady bezpiecznego korzystania z poczty elektronicznej, stron internetowych oraz chroni dane osobowe podczas korzystania z usług cyfrowych.	rozpoznaje podejrzaną wiadomości, linki i strony internetowe;	Analiza dowodów i deklaracji
	wskazuje zasady bezpiecznego korzystania z poczty elektronicznej;	Analiza dowodów i deklaracji
	opracowuje zasady ochrony danych osobowych i bezpiecznego korzystania z Internetu.	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Tworzy bezpieczne hasła, stosuje podstawowe zasady ochrony prywatności oraz świadomie korzysta z mediów społecznościowych.	tworzy przykłady silnych haseł zgodnych z zasadami bezpieczeństwa;	Analiza dowodów i deklaracji
	wskazuje informacje, których nie należy publikować w Internecie;	Analiza dowodów i deklaracji
	proponuje działania zwiększające poziom prywatności kont internetowych.	Analiza dowodów i deklaracji
Stosuje zasady bezpiecznego korzystania z bankowości elektronicznej, zakupów online oraz odpowiedzialnego użytkowania urządzeń cyfrowych zgodnie z zasadami zrównoważonego rozwoju. Podejmuje właściwe działania po wystąpieniu zagrożenia cyberbezpieczeństwa oraz stosuje zasady bezpiecznego usuwania danych i przygotowania urządzeń do ponownego wykorzystania lub recyklingu.	wskazuje zasady bezpiecznych płatności internetowych;	Test teoretyczny
	rozpoznaje cechy wiarygodnego sklepu internetowego;	Test teoretyczny
	wymienia działania wydłużające okres użytkowania urządzeń oraz ograniczające ilość elektroodpadów.	Test teoretyczny
	wskazuje właściwe działania po ujawnieniu danych lub kliknięciu w podejrzany link;	Analiza dowodów i deklaracji
	opracowuje indywidualny plan bezpiecznego i odpowiedzialnego korzystania z technologii;	Analiza dowodów i deklaracji
	przedstawia zasady bezpiecznego usuwania danych przed przekazaniem urządzenia do ponownego użycia lub recyklingu.	Analiza dowodów i deklaracji
Odpowiedzialnie korzysta z technologii cyfrowych z uwzględnieniem zasad cyberbezpieczeństwa oraz zrównoważonego wykorzystania zasobów cyfrowych Współpracuje z innymi użytkownikami technologii cyfrowych, dzieli się wiedzą na temat bezpiecznego korzystania z Internetu oraz wspiera osoby z najbliższego otoczenia w rozpoznawaniu zagrożeń cyfrowych.	deklaruje stosowanie dobrych praktyk w zakresie cyberbezpieczeństwa i ochrony środowiska;	Analiza dowodów i deklaracji
	wskazuje działania, które będzie wdrażał w życiu codziennym i przekazywał innym użytkownikom;	Analiza dowodów i deklaracji
	wykazuje gotowość do rozwijania kompetencji cyfrowych i zielonych.	Analiza dowodów i deklaracji
	deklaruje gotowość przekazywania dobrych praktyk dotyczących cyberbezpieczeństwa,	Analiza dowodów i deklaracji
	wskazuje sposoby wspierania innych użytkowników w bezpiecznym korzystaniu z technologii.	Analiza dowodów i deklaracji

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

10:00–10:45 Moduł I. Bezpieczny i zielony świat cyfrowy – świadome korzystanie z technologii

Zakres tematyczny

- czym jest cyberbezpieczeństwo i dlaczego dotyczy każdego użytkownika Internetu,
- najczęstsze zagrożenia dla osób starszych korzystających z Internetu,
- kompetencje cyfrowe potrzebne do bezpiecznego funkcjonowania w społeczeństwie,
- czym są zielone kompetencje według ESCO,
- wpływ korzystania z Internetu, telefonów komórkowych, komputerów oraz usług cyfrowych na środowisko,
- ślad cyfrowy i ślad węglowy usług internetowych,
- energia wykorzystywana przez urządzenia elektroniczne oraz centra danych,
- odpowiedzialne korzystanie z urządzeń elektronicznych,
- zasada „Napraw – Zabezpiecz – Korzystaj dłużej – Oddaj do recyklingu”.

Ćwiczenie praktyczne

Analiza codziennych zachowań użytkownika Internetu – uczestnicy wskazują działania sprzyjające bezpieczeństwu cyfrowemu oraz ochronie środowiska.

10:45–11:45 Moduł II. Oszustwa internetowe, telefoniczne i SMS – jak nie dać się oszukać

- fałszywe wiadomości dotyczące przesyłek, dopłat, rachunków, mandatów, wygranych oraz zwrotów pieniędzy,
- najczęściej spotykane metody oszustw: „na pracownika banku”, „na policjanta”, „na wnuczkę”, „na inwestycję” oraz „na BLIK”,
- rozpoznawanie prób wyludzania danych osobowych, haseł oraz kodów autoryzacyjnych,
- mechanizmy manipulacji wykorzystywane przez cyberprzestępców: presja czasu, wzbudzanie strachu, poczucie obowiązku lub chęci szybkiego zysku,
- wykorzystanie sztucznej inteligencji do tworzenia fałszywych wiadomości, zdjęć i nagrań głosowych,
- zasada ograniczonego zaufania podczas korzystania z Internetu i telefonu,
- sposoby sprawdzania wiarygodności nadawcy wiadomości oraz numerów telefonów,
- właściwe postępowanie po otrzymaniu podejrzanego wiadomości lub telefonu.

Ćwiczenie praktyczne:

„Prawdziwa czy fałszywa wiadomość?” – analiza autentycznych przykładów SMS-ów, wiadomości e-mail i komunikatów internetowych.

11:45–12:15 Przerwa

12:15–13:00 Moduł III. Bezpieczna poczta elektroniczna, strony internetowe i ochrona danych

- czym jest phishing i w jaki sposób cyberprzestępcy próbują wyłudzić dane,
- rozpoznawanie podejrzanych wiadomości e-mail, SMS oraz komunikatów internetowych,
- sprawdzanie adresu nadawcy, domeny internetowej oraz certyfikatu bezpieczeństwa strony,
- bezpieczne otwieranie wiadomości, linków i załączników,
- rozpoznawanie fałszywych komunikatów o wirusach, blokadzie urządzenia lub konieczności natychmiastowej płatności,
- zasady bezpiecznego korzystania z poczty elektronicznej,
- usuwanie spamu, niepotrzebnych newsletterów oraz zbędnych wiadomości,
- porządkowanie skrzynki pocztowej jako element cyfrowej higieny oraz ograniczania ilości przechowywanych danych.

Ćwiczenie praktyczne:

Analiza przykładowych wiadomości e-mail i SMS oraz ocena bezpieczeństwa wybranych stron internetowych.

13:00–13:45 Moduł IV. Bezpieczne korzystanie z mediów społecznościowych i usług cyfrowych

- tworzenie silnych i łatwych do zapamiętania haseł,
- dlaczego nie należy stosować jednego hasła do wielu kont,
- uwierzytelnianie dwuskładnikowe i jego znaczenie dla bezpieczeństwa,
- bezpieczne przechowywanie danych do logowania,
- jakie informacje stanowią dane osobowe i wymagają szczególnej ochrony,
- jakie informacje warto, a jakich nie należy publikować w mediach społecznościowych,
- zarządzanie ustawieniami prywatności kont internetowych,
- usuwanie nieużywanych kont, aplikacji i danych jako element zwiększania bezpieczeństwa oraz ograniczania śladu cyfrowego.

Ćwiczenie praktyczne:

Ocena przykładowych haseł oraz konfiguracja ustawień prywatności na przykładzie serwisu społecznościowego.

13:45–14:15 Przerwa

14:15–15:15 Moduł V. Bezpieczna bankowość internetowa, zakupy online oraz zielone korzystanie z urządzeń

- bezpieczne logowanie do bankowości elektronicznej i aplikacji mobilnych,
- zasady korzystania z kodów SMS, PIN oraz płatności BLIK,
- rozpoznawanie fałszywych sklepów internetowych i ofert sprzedaży,
- sprawdzanie wiarygodności sprzedawcy, opinii oraz danych kontaktowych,
- bezpieczne płatności internetowe i ochrona danych finansowych,
- odpowiedzialne zakupy internetowe – wybór produktów trwałych, energooszczędnych i naprawialnych,
- dokumenty elektroniczne jako sposób ograniczania zużycia papieru,
- aktualizowanie systemów operacyjnych i aplikacji,
- instalowanie programów wyłącznie z zaufanych źródeł,
- bezpieczne korzystanie z publicznych sieci Wi-Fi,
- wydłużanie okresu użytkowania telefonu i komputera poprzez właściwą eksploatację, konserwację oraz oszczędzanie energii,
- prawidłowe przygotowanie urządzenia do sprzedaży, przekazania lub recyklingu poprzez bezpieczne usunięcie danych.

Ćwiczenie praktyczne:

Ocena wiarygodności przykładowego sklepu internetowego oraz wykonanie podstawowego przeglądu ustawień bezpieczeństwa i oszczędzania energii telefonu.

15:15–16:00 Moduł VI. Reagowanie na zagrożenia oraz dobre praktyki bezpiecznego i zielonego korzystania z technologii

- postępowanie po kliknięciu w podejrzany link lub otwarciu niebezpiecznego załącznika,
- działania po ujawnieniu danych osobowych lub przekazaniu kodu autoryzacyjnego,
- kontakt z bankiem, blokowanie karty płatniczej oraz zabezpieczenie kont internetowych,
- zmiana haseł i odzyskiwanie dostępu do kont,
- zgłaszanie podejrzanych wiadomości oraz prób oszustwa odpowiednim instytucjom,
- postępowanie w przypadku utraty lub kradzieży telefonu,
- bezpieczne usuwanie danych ze starego sprzętu,
- odpowiedzialne przekazywanie urządzeń do ponownego wykorzystania lub recyklingu,
- opracowanie własnych zasad bezpiecznego i odpowiedzialnego korzystania z technologii w życiu codziennym.

Ćwiczenie praktyczne:

Opracowanie indywidualnej listy „10 zasad Bezpiecznego i Zielonego Seniora w Sieci”.

16:00–18:00 Walidacja efektów uczenia się

Osoba prowadząca walidację nie uczestniczy w prowadzeniu usługi szkoleniowej, co zapewnia rozdzielenie procesu kształcenia od procesu walidacji zgodnie z wymaganiami BUR

Program wpisuje się w założenia Regionalnej Strategii Innowacji Województwa Śląskiego 2030 poprzez rozwijanie kompetencji cyfrowych, cyberbezpieczeństwa oraz zielonych kompetencji wspierających transformację cyfrową, podnoszenie odporności cyfrowej społeczeństwa oraz zrównoważone wykorzystanie technologii.

Usługa wspiera realizację celów Programu Rozwoju Technologii Województwa Śląskiego na lata 2019–2030 poprzez rozwijanie kompetencji niezbędnych do bezpiecznego korzystania z technologii cyfrowych, odpowiedzialnego zarządzania zasobami cyfrowymi oraz wspierania transformacji cyfrowej i zielonej gospodarki.

Harmonogram

Liczba pozycji harmonogramu: 9

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Moduł I. Bezpieczny i zielony świat cyfrowy – świadome korzystanie z technologii	Zajęcia	Monika Wądrzyk	07-10-2026	10:00	10:45	00:45
2 z 9 Moduł II. Oszustwa internetowe, telefoniczne i SMS – jak nie dać się oszukać	Zajęcia	Monika Wądrzyk	07-10-2026	10:45	11:45	01:00
3 z 9 -	Przerwa	-	07-10-2026	11:45	12:15	00:30
4 z 9 Moduł III. Bezpieczna poczta elektroniczna, strony internetowe i ochrona danych	Zajęcia	Monika Wądrzyk	07-10-2026	12:15	13:00	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 9 Moduł IV. Bezpieczne korzystanie z mediów społecznościowych i usług cyfrowych	Zajęcia	Monika Wądrzyk	07-10-2026	13:00	13:45	00:45
6 z 9 -	Przerwa	-	07-10-2026	13:45	14:15	00:30
7 z 9 Moduł V. Bezpieczna bankowość internetowa, zakupy online oraz zielone korzystanie z urządzeń	Zajęcia	Monika Wądrzyk	07-10-2026	14:15	15:15	01:00
8 z 9 Moduł VI. Reagowanie na zagrożenia oraz dobre praktyki bezpiecznego i zielonego korzystania z technologii	Zajęcia	Monika Wądrzyk	07-10-2026	15:15	16:00	00:45
9 z 9 -	Walidacja	-	07-10-2026	16:00	18:00	02:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	05:00
w tym suma godzin walidacji	02:00
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeżeli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 906,50 PLN
Koszt przypadający na 1 uczestnika netto	1 550,00 PLN
Koszt osobogodziny brutto	238,31 PLN
Koszt osobogodziny netto	193,75 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Monika Wądrzyk

Trenerka i specjalistka ds. szkoleń z doświadczeniem w projektowaniu oraz realizacji szkoleń stacjonarnych i online. Specjalizuje się w tworzeniu programów edukacyjnych, zarządzaniu procesami szkoleniowymi oraz wdrażaniu narzędzi cyfrowych wspierających rozwój kompetencji. W ciągu ostatnich 5 lat prowadziła szkolenia i warsztaty z zakresu wykorzystania nowych technologii, sztucznej inteligencji (AI), automatyzacji pracy oraz efektywnego wykorzystania narzędzi cyfrowych w organizacjach. Posiada doświadczenie w projektowaniu materiałów szkoleniowych, treści edukacyjnych oraz komunikacji skierowanej do uczestników i klientów. Tworzyła materiały cyfrowe, prezentacje oraz treści wykorzystywane w procesach edukacyjnych i komunikacyjnych. W pracy wykorzystuje narzędzia generatywnej AI do przygotowywania tekstów, grafik, prezentacji i materiałów komunikacyjnych. Posiada praktyczną znajomość zasad tworzenia promptów,

weryfikacji treści generowanych przez AI oraz odpowiedzialnego wykorzystania technologii cyfrowych.

Zarządzała platformami e-learningowymi, m.in. Schoox oraz Campus AI, wspierając organizacje w wykorzystaniu technologii w procesach rozwojowych.

W ostatnich latach rozwijała kompetencje w obszarze AI, gospodarki obiegu zamkniętego (GOZ), cyberbezpieczeństwa oraz śladu węglowego organizacji. Doświadczenie zdobyte nie wcześniej niż 5 lat przed publikacją usługi w BUR.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe udostępniane są w wersji cyfrowej.

Uczestnik korzysta z własnego laptopa, komputera, tabletu lub smartfona z dostępem do Internetu. Minimalne wymagania sprzętowe:

- System operacyjny min. taki jak Windows 8 (zalecany Windows 11), Mac OS wersja 10.13-zalecana najnowsza wersja , Linux, Chrome OS, Aktualna wersja systemu Android/iOS-po aktualizacji.
- Przeglądarka: Chrome, Edge, Firefox lub Safari w aktualnej wersji
 - urządzenie z aktualnym systemem operacyjnym,
 - aktualna przeglądarka internetowa,
 - dostęp do Internetu,
 - możliwość otwierania plików PDF oraz dokumentów tekstowych,
 - aktywne konto e-mail.

Warunki uczestnictwa

- Warunkiem ukończenia usługi jest uczestnictwo w co najmniej 80% zajęć oraz przystąpienie do procesu walidacji. Warunkiem uzyskania certyfikatu potwierdzającego nabycie kompetencji jest pozytywny wynik walidacji przeprowadzonej przez niezależny podmiot walidujący.
- Karta usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych
- przed dokonaniem zapisu na usługę należy skontaktować się z usługodawcą celem weryfikacji dostępności miejsca

Uczestnik przyjmuje do wiadomości, że usługa może podlegać monitoringowi, kontroli lub dokumentowaniu zgodnie z zasadami realizacji projektów dofinansowanych ze środków publicznych. Ewentualne utrwalanie wizerunku odbywa się wyłącznie w zakresie niezbędnym do realiza

Informacje dodatkowe

Usługa zwolniona z VAT na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U.2013 poz. 1722 z późniejszymi zmianami)

Program rozwija kompetencje cyfrowe oraz zielone kompetencje zgodne z klasyfikacją ESCO i wspiera realizację założeń transformacji cyfrowej oraz gospodarki o obiegu zamkniętym (GOZ).

Szkolenie realizowane jest stacjonarnie w wymiarze **8 h zegarowych**, obejmujących zajęcia merytoryczne, ćwiczenia praktyczne, przerwy oraz walidację. Przerwy są wliczone w czas trwania usługi.

Adres

ul. Jagiellońska 22
44-100 Gliwice
woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



Żaneta Łaba

E-mail wsparcie@centrum-innowacji.pl

Telefon (+48) 517 283 451