



AKADEMIA
PRZEDSIĘBIORCY
WEC SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,6 / 5

5 ocen

Cyberbezpieczeństwo- bezpieczny użytkownik w sieci

Numer usługi 2025/08/06/174043/2925261

📍 zdalna w czasie rzeczywistym

🎓 Usługa szkoleniowa

🕒 4 h

📅 20.08.2025 do 20.08.2025

799,50 PLN brutto

650,00 PLN netto

199,88 PLN brutto/h

162,50 PLN netto/h

Informacje podstawowe

Kategoria	Inne / Edukacja
Identyfikatory projektów	Kierunek - Rozwój, Małopolski Pociąg do kariery
Grupa docelowa usługi	Szkolenie jest skierowane do osób korzystających z internetu i narzędzi cyfrowych w codziennej pracy lub życiu prywatnym, które chcą zwiększyć swoje bezpieczeństwo w sieci. Nie jest wymagana specjalistyczna wiedza techniczna, jednak podstawowa znajomość obsługi komputera i internetu będzie przydatna. Usługa również adresowana dla Uczestników Projektu MP i/lub dla Uczestników Projektu NSE. Usługa adresowana również dla Uczestników Projektu Kierunek-Rozwój.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	14-08-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	4
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest rozwinięcie umiejętności ochrony danych i prywatności w Internecie, zabezpieczania kont i urządzeń, unikania zagrożeń online, korzystania z legalnych źródeł zasobów cyfrowych, ochrony wizerunku w sieci, bezpiecznych zakupów oraz komunikacji, a także stosowania praktycznych narzędzi i dobrych praktyk w zakresie bezpieczeństwa cyfrowego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA • Znajomość podstawowych zasad prawnych związanych z pobieraniem i wykorzystywaniem zasobów cyfrowych, w tym praw autorskich, RODO oraz ochrony danych osobowych. • Zrozumienie zagrożeń internetowych, takich jak oszustwa, phishing, wirusy, oraz sposobów zabezpieczania się przed nimi. • Wiedza na temat bezpiecznej wymiany informacji i danych w internecie, w tym szyfrowania, hasłowania plików oraz dwuskładnikowego uwierzytelniania. • Świadomość zagrożeń związanych z korzystaniem z urządzeń IoT (np. lodówki, drukarki) oraz ich zabezpieczania. • Zrozumienie narzędzi do komunikacji online i ich roli w bezpiecznej pracy zespołowej.	Efekty uczenia się w zakresie wiedzy zostaną uznane za osiągnięte, jeśli uczestnik testu: Poprawne wskazanie zasad prawa cyfrowego, ochrony danych, metod zabezpieczeń i narzędzi online w pytaniach testowych. Weryfikacja: pytania testowe sprawdzające znajomość pojęć, funkcjonalności oraz zasad etycznych i organizacyjnych korzystania z AI.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
UMIEJĘTNOŚCI • Umiejętność korzystania z legalnych zasobów (grafik, plików, multimediiów) dostępnych do użytku komercyjnego oraz instytucjonalnego. • Umiejętność zabezpieczania kont internetowych za pomocą menadżerów haseł, uwierzytelniania dwuskładnikowego oraz innych nowoczesnych metod ochrony. • Praktyczne stosowanie narzędzi do sprawdzania dostępności i poprawności zasobów cyfrowych oraz ich ochrony przed wirusami. • Umiejętność realizowania bezpiecznych transakcji online i korzystania z mechanizmów chroniących kupujących, takich jak chargeback. • Efektywne zarządzanie przechowywaniem danych na nośnikach zewnętrznych oraz w chmurze.	Efekty uczenia się w zakresie wiedzy zostaną uznane za osiągnięte, jeśli uczestnik testu: Wybór właściwych działań i narzędzi ochrony danych, kont, transakcji i zasobów cyfrowych w różnych sytuacjach. Sposób weryfikacji: test jednokrotnego wyboru sprawdzający umiejętność doboru poprawnych rozwiązań w opisanych przypadkach.	Test teoretyczny z wynikiem generowanym automatycznie
KOMPETENCJE • Zdolność do świadomego i bezpiecznego korzystania z zasobów internetu, z zachowaniem zasad ochrony danych osobowych oraz wizerunku w sieci. • Umiejętność korzystania z bezpiecznych narzędzi do komunikacji online, które zapewniają ochronę prywatności i danych w pracy zespołowej. • Kompetencje w zakresie zabezpieczania urządzeń i systemów przed zagrożeniami wynikającymi z ich połączenia z internetem. • Wiedza i praktyczne umiejętności dotyczące ochrony swoich finansów oraz danych osobowych podczas zakupów online.	Efekty uczenia się w zakresie wiedzy zostaną uznane za osiągnięte, jeśli uczestnik testu: Prawidłowe decyzje i strategie bezpiecznego korzystania z internetu, komunikacji online i urządzeń. Sposób weryfikacji: test jednokrotnego wyboru sprawdzający zdolność podejmowania właściwych decyzji w scenariuszach sytuacyjnych.	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

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. Legalność pobieranych zasobów.

- Prawa autorskie, majątkowe, skąd pobierać treści, weryfikacja ich poprawności oraz informacje o źródle i sposobie wykorzystania, sprawdzanie plików pod względem zainfekowania wirusami, zasoby darmowe do wykorzystania komercyjnego, bezpłatne zasoby na użytek instytucji, darmowe aplikacje wspomagające pracę (grafiki, multimedia, pliki itp.),
- bezpieczeństwo wymiany informacji i danych między użytkownikami, RODO, ochrona danych osobowych, hasłowanie plików i szyfrowanie treści.

1. Ochrona dostępu do kont, skrzynek e-mailowych, jak zmniejszyć ryzyko ataku.

- Hasła, forma ich przechowywania, uwierzytelnianie dwuskładnikowe, menadżery haseł, czytniki biometryczne i inne zabezpieczenia np. klucz U2F
- Weryfikacja kont pod względem wycieku danych i bezpieczeństwa logowania.

1. Zagrożenia oraz oszustwa pojawiające się w internecie

- Rodzaje oszust i zagrożeń, przykłady i przypadki, formy zabezpieczenia i przeciwdziałania oraz ochrony przed tego rodzaju działaniami. Jak trafiają do nas wirusy?
- Jak trafiają do nas wirusy, czyli dobre praktyki w bezpiecznym korzystaniu z narzędzi online.

1. Wizerunek w internecie. Ochrona danych osobowych.

- Ochrona danych w internecie, metadane udostępniane w plikach, ograniczenie widoczności profili, informacje ogólnodostępne – OSINT – biały wywiad – co wiemy, o nas na przykładzie danych publikowanych w sieci, publiczne rejestry, informacje, śledzenie w internecie, monitorowanie użytkowników i ruchu w internecie.

1. Analiza narzędzi do komunikacji. Internet jako przestrzeń bezpiecznej komunikacji.

- Bezpieczne komunikatory, szyfrowanie danych, praca zespołowa

1. Bezpieczne zakupy i finanse

- Weryfikacja sprzedającego, realizowanie bezpiecznych transakcji, usługi chargeback itd. chroniące kupującego po realizacji umowy, zasady i praktyki dotyczące bezpiecznych zakupów.

1. Ochrona urządzeń i sprzętu

- Czy lodówka, lub drukarka podłączona do sieci może mi zaszkodzić?

1. Jak bezpiecznie przechowywać pliki i dane

- Nośniki zewnętrzne
- W chmurze
- Duże pliki

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Legalność pobieranych zasobów	Paweł Bukowski	20-08-2025	08:30	09:00	00:30
2 z 9 Ochrona dostępu do kont, skrzynek e-mailowych, jak zmniejszyć ryzyko ataku	Paweł Bukowski	20-08-2025	09:00	09:25	00:25
3 z 9 Zagrożenia oraz oszustwa pojawiające się w internecie	Paweł Bukowski	20-08-2025	09:25	09:50	00:25
4 z 9 Wizerunek w internecie. Ochrona danych osobowych	Paweł Bukowski	20-08-2025	09:50	10:15	00:25
5 z 9 Analiza narzędzi do komunikacji. Internet jako przestrzeń bezpiecznej komunikacji	Paweł Bukowski	20-08-2025	10:15	10:35	00:20
6 z 9 Bezpieczne zakupy i finanse	Paweł Bukowski	20-08-2025	10:35	10:55	00:20
7 z 9 Ochrona urządzenie i sprzętu	Paweł Bukowski	20-08-2025	10:55	11:15	00:20
8 z 9 Jak bezpiecznie przechowywać pliki i dane	Paweł Bukowski	20-08-2025	11:15	11:40	00:25
9 z 9 Test wiedzy i podsumowanie	Paweł Bukowski	20-08-2025	11:40	12:30	00:50

Cennik

Cennik

Rodzaj ceny	Cena
-------------	------

Koszt przypadający na 1 uczestnika brutto	799,50 PLN
Koszt przypadający na 1 uczestnika netto	650,00 PLN
Koszt osobogodziny brutto	199,88 PLN
Koszt osobogodziny netto	162,50 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Paweł Bukowski

Absolwent Informatyki i wykładowca Społecznej Akademii Nauk w katedrze gospodarki elektronicznej. Od ponad 13 lat prowadzi szkolenia z zakresu IT, biznesu, nowoczesnych technologii, digital marketingu, kompetencji cyfrowych, obsługi Office i Google, wdrażania produktów i usług. Zrealizował ponad 7500 godzin szkoleniowych w ostatnich 5 latach. Współpracował m.in. z Volkswagenem, Autodesk, Kellogg's, Fundacją WZWR, Top Farms. Posiada certyfikaty Cisco CCNA, Cisco Wireless LAN, Adobe Photoshop, Franklin Covey („7 nawyków...”, „Focus”), Clarity4D (komunikacja i negocjacje), szkolenia z obsługi klienta i autoprezentacji. Stawia na praktyczne podejście i efektywne wykorzystanie zasobów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają materiały w postaci skryptu pdf.

Warunki uczestnictwa

Szkolenie jest skierowane do osób korzystających z internetu i narzędzi cyfrowych w codziennej pracy lub życiu prywatnym, które chcą zwiększyć swoje bezpieczeństwo w sieci. Nie jest wymagana specjalistyczna wiedza techniczna, jednak podstawowa znajomość obsługi komputera i internetu będzie przydatna.

Informacje dodatkowe

Szkolenie trwa od godziny 08:30-12:30 (4h).

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek-Rozwój.

Kompetencja związana z cyfrową transformacją.

Warunki techniczne

1. Platforma komunikacyjna

Szkolenie będzie prowadzone za pośrednictwem platformy **Microsoft Teams**. Jest to profesjonalne narzędzie do wideokonferencji, współpracy i wymiany plików, które umożliwia dostęp do prezentowanych treści, uczestnictwo w dyskusjach oraz współpracę na żywo.

2. Minimalne wymagania sprzętowe

Urządzenie uczestnika musi spełniać następujące wymagania:

- **Komputer/laptop:**
 - Procesor: **minimum 1.6 GHz** lub wyższy
 - Pamięć RAM: **minimum 4 GB**
 - Karta graficzna: zgodna z **DirectX 9** lub nowsza
 - System operacyjny: **Windows 10 lub nowszy / macOS X 10.11 El Capitan** lub nowszy
- **Tablet/smartfon:**
 - Android: wersja **6.0** lub nowsza
 - iOS: wersja **12.0** lub nowsza
 - Kamera internetowa i mikrofon (wbudowane lub zewnętrzne).

3. Minimalne wymagania dotyczące parametrów łącza sieciowego

- **Prędkość pobierania:** minimum **1.2 Mbps**
- **Prędkość wysyłania:** minimum **1.2 Mbps**
- **Stale i stabilne połączenie internetowe** (preferowane jest połączenie kablowe lub Wi-Fi o stabilnym sygnale).

4. Niezbędne oprogramowanie

- Aplikacja **Microsoft Teams**:
 - Użytkownicy komputerów mogą pobrać aplikację Teams z oficjalnej strony Microsoft lub korzystać z wersji przeglądarkowej (najlepiej w przeglądarce **Microsoft Edge, Google Chrome** lub **Safari**).
 - Użytkownicy urządzeń mobilnych powinni pobrać aplikację **Microsoft Teams** z odpowiednich sklepów (Google Play, App Store).
- **Przeglądarka internetowa:** jeśli szkolenie odbywa się przez przeglądarkę, rekomendowane są najnowsze wersje przeglądarek Microsoft Edge, Google Chrome, Mozilla Firefox lub Safari.

Kontakt



Anna Kieszek

E-mail anna.kieszek@wecfinanse.pl

Telefon (+48) 608 479 111