



Ernabo Adrian Flak

★★★★★ 4,6 / 5

861 ocen

Szkolenie: Twoje bezpieczeństwo w cyfrowym świecie

Numer usługi 2026/04/27/22948/3516444

📍 Poraj

🏢 Usługa szkoleniowa

📄 stacjonarna

🕒 21:00 h

📅 04.07.2026 do 25.07.2026

4 200,00 PLN brutto

4 200,00 PLN netto

200,00 PLN brutto/h

200,00 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Osoby dorosłe w tym: Uczniowie, Seniorzy, Pracownicy firm i instytucji publicznych. Wszyscy, którzy korzystają z komputerów, internetu i poczty elektronicznej w pracy.

Osoby odpowiedzialne za przetwarzanie danych firmowych lub wrażliwych.

Każdy, kto chce zwiększyć świadomość zagrożeń w sieci i nauczyć się podstawowych metod ochrony danych.

- Szkolenie przeznaczone jest również dla uczestników projektu **Kierunek Rozwój** realizowany przez WUP w Toruniu.
- Usługa również adresowana dla Uczestników Projektu **Małopolski Pociąg do Kariery sezon 1**
- Usługa skierowana również dla uczestników projektu "**Zachodniopomorskie bony szkoleniowe**"
- Oraz dla uczestników projektów dofinansowanych **w całej Polsce**
- Szkolenie skierowane jest zarówno do **osób indywidualnych, jak i pracodawców i ich pracowników.**

Minimalna liczba uczestników

3

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

03-07-2026

Forma prowadzenia usługi

stacjonarna

Liczba godzin usługi

21

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do rozpoznawania zagrożeń w sieci i stosowania praktycznych metod ochrony danych oraz systemów w codziennej pracy. Uczestnicy nauczą się bezpiecznego korzystania z komputerów, poczty elektronicznej i urządzeń mobilnych oraz reagowania na potencjalne incydenty cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje kluczowe zagrożenia w sieci oraz mechanizmy manipulacji stosowane przez cyberprzestępców.	Definiuje cyberbezpieczeństwo jako proces ochrony danych i urządzeń przed nieuprawnionym dostępem.	Test teoretyczny z wynikiem generowanym automatycznie
	Wymienia co najmniej 3 kanały, którymi może zostać zaatakowany (telefon, e-mail, strony WWW).	Test teoretyczny z wynikiem generowanym automatycznie
	Odróżnia autentyczną wiadomość od próby phishingu na podstawie typowych cech (błędy językowe, ponaglanie, podejrzany link).	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik samodzielnie zabezpiecza swoje urządzenia oraz tworzy bezpieczne poświadczenia dostępu.	Wyjaśnia, na czym polega socjotechnika w metodach „na wnuczka” czy „na policjanta”.	Test teoretyczny z wynikiem generowanym automatycznie
	Tworzy silne hasło (minimum 12 znaków, duże/małe litery, cyfry, znaki specjalne) i wyjaśnia, dlaczego nie należy go powielać w różnych serwisach.	Obserwacja w warunkach symulowanych
	Wskazuje w ustawieniach telefonu miejsce sprawdzania aktualizacji systemu.	Test teoretyczny
	Demonstruje sposób blokowania ekranu (PIN, wzór lub biometria).	Test teoretyczny
	Wyjaśnia ryzyko związane z instalowaniem aplikacji spoza oficjalnych sklepów (Google Play / App Store).	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik bezpiecznie porusza się po stronach internetowych i realizuje transakcje płatnicze.	Weryfikuje tożsamość strony bankowej poprzez sprawdzenie protokołu https oraz symbolu kłódki.	Test teoretyczny
	Wymienia zasady bezpiecznych zakupów (sprawdzanie opinii o sklepie, unikanie podejrzanie niskich cen).	Test teoretyczny
	Charakteryzuje bezpieczne metody płatności (np. jednorazowy kod BLIK vs. podawanie pełnych danych karty).	Test teoretyczny
	Wyjaśnia, dlaczego nie należy logować się do bankowości elektronicznej w publicznych sieciach Wi-Fi.	Test teoretyczny
Uczestnik świadomie zarządza swoimi danymi osobowymi i chroni swoją prywatność w mediach społecznościowych.	Wymienia dane wrażliwe, których nigdy nie podaje osobom postronnym (PESEL, numer dowodu, kody CVV/CVC, hasła).	Obserwacja w warunkach symulowanych
	Identyfikuje informacje, których nie należy publikować publicznie na portalach typu Facebook (np. zdjęcia biletów, informacja o nieobecności w domu).	Obserwacja w warunkach symulowanych
Uczestnik opisuje, jak zminimalizować skutki ataku i gdzie szukać pomocy.	Opisuje procedurę postępowania po kliknięciu w fałszywy link (odłączenie od sieci, zmiana haseł, kontakt z bankiem).	Test teoretyczny
	Wskazuje numer alarmowy do banku w celu zastrzeżenia karty/konta.	Obserwacja w warunkach symulowanych
	Wskazuje sposób zgłaszania podejrzanych wiadomości SMS do CERT Polska (numer 8080).	Obserwacja w warunkach symulowanych
	Stosuje zasadę „ograniczonego zaufania” i przerywa podejrzaną rozmowę telefoniczną.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://icdl.pl/>

Strona internetowa Instytucji Walidującej: <https://centrum.kiss.pl/>

Informacje

Nazwa Podmiotu prowadzącego walidację	Śląskie Centrum Szkoleniowo-Egzaminacyjne KISS
Nazwa Podmiotu certyfikującego	Polskie Biuro ECDL / Polskie Towarzystwo Informatyczne

Program

Program szkolenia jest dostosowany do potrzeb uczestników usługi oraz głównego celu usługi i jej charakteru oraz obejmuje zakres tematyczny usługi. Uczestnik nie musi spełniać dodatkowych wymagań dot. poziomu zaawansowania.

Usługa prowadzona jest w godzinach dydaktycznych. Przerwy nie są wliczone w ogólny czas usługi rozwojowej. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazują nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Szkolenie będzie realizowane **w formie stacjonarnej**, co umożliwi aktywny udział uczestników w warsztatach i ćwiczeniach grupowych. Szkolenie ma charakter teoretyczno-praktyczny. Szkolenie zostanie przeprowadzone w formie pozwalającej uczestnikowi na efektywny udział tj. w formie: wykładów interaktywnych, warsztatów praktycznych, „analizy przypadków, ćwiczeń indywidualnych.

Podział szkolenia:

- 8h dydaktycznych teoretycznych,
- 12 h dydaktycznych praktycznych,
- 1 h dydaktyczna walidacji

Usługa szkoleniowa realizowana stacjonarnie w sali szkoleniowej zapewniającej odpowiednie warunki do pracy dydaktycznej – zgodnie z obowiązującymi przepisami BHP oraz wytycznymi organizatora.

Każdy uczestnik pracuje indywidualnie na komputerze z bieżącym wsparciem trenera.

Przed dokonaniem zapisu i złożeniem karty uczestnictwa do Operatora, zachęcamy do **kontaktowania się z nami telefonicznie, SMS-em lub e-mailem** pod adresem/numerem wskazanym w zakładce „**Kontakt**”.

Pozwoli to **potwierdzić dostępność miejsca** w grupie szkoleniowej oraz rozwiązać ewentualne wątpliwości.

Program szkolenia:

Moduł 1: Wprowadzenie – gdzie czyhają zagrożenia?

- czym jest cyberbezpieczeństwo (prosto i praktycznie)
- gdzie najczęściej spotykamy zagrożenia:
 - telefon (połączenia, SMS-y)
 - internet (strony, zakupy)
 - e-mail
- dlaczego seniorzy są częstym celem oszustów

Moduł 2: Najczęstsze oszustwa – jak działają przestępcy?

- metoda „na wnuczka”, „na policjanta”, „na pracownika banku”
- fałszywe SMS-y (np. dopłata do paczki, bank, InPost)

- phishing – fałszywe strony banków
- przykłady prawdziwych scenariuszy (case study)

Ćwiczenie: rozpoznawanie podejrzanej wiadomości

Moduł 3: Zasady cyberhigieny na co dzień

- silne hasła – jak je tworzyć i zapamiętać
- dlaczego nie używać jednego hasła wszędzie
- aktualizacje telefonu i komputera
- instalowanie aplikacji (tylko oficjalne sklepy)
- blokada telefonu (PIN, odcisk palca)

Moduł 4: Bezpieczne korzystanie z internetu i zakupów

- jak rozpoznać bezpieczną stronę (https, kłódka)
- zakupy online – na co uważać
- bezpieczne płatności (BLIK, karta, przelew)
- publiczne Wi-Fi – zagrożenia

Moduł 5: Prywatność i dane osobowe

- jakie dane są wrażliwe (PESEL, hasła, dane karty)
- czego NIE udostępniać przez telefon i internet
- ostrożność w mediach społecznościowych

Moduł 6: Co zrobić w sytuacji zagrożenia?

- podejrzany telefon – jak reagować
- kliknięcie w fałszywy link – co dalej
- gdzie zgłosić oszustwo:
 - bank
 - policja
 - CERT Polska

Moduł 7: Podsumowanie – 10 zasad bezpiecznego seniora

- nie podawaj danych przez telefon
- nie klikaj w podejrzane linki
- sprawdzaj nadawcę
- używaj silnych haseł
- zachowaj spokój – nie działaj pod presją

Metody dydaktyczne

- proste prezentacje (język bez technicznego żargonu)
- przykłady z życia
- ćwiczenia praktyczne
- dyskusja i pytania

EGZAMIN (PODMIOT ZEWNĘTRZNY)

do kwalifikacji: ECDL STANDARD S3 – IT SECURITY

Okres oczekiwania na wydanie wyniku przeprowadzonej walidacji: Czas oczekiwania na wydanie wyniku przeprowadzonej walidacji wynosi do 7 dni, licząc od kolejnego dnia po jej przeprowadzeniu.

Z uwagi na to, data zakończenia usługi została wydłużona.

Harmonogram

Liczba pozycji harmonogramu: 12

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Moduł 1: Wprowadzenie – gdzie czyhają zagrożenia? cz.1	MARCIN RAŁ	04-07-2026	08:00	09:45	01:45
2 z 12 Moduł 1: Wprowadzenie – gdzie czyhają zagrożenia? cz.2	MARCIN RAŁ	07-07-2026	10:00	11:45	01:45
3 z 12 Przerwa	MARCIN RAŁ	07-07-2026	11:45	12:00	00:15
4 z 12 Moduł 2: Najczęstsze oszustwa – jak działają przestępcy?	MARCIN RAŁ	07-07-2026	12:00	15:30	03:30
5 z 12 Moduł 3: Zasady cyberhigieny na co dzień	MARCIN RAŁ	08-07-2026	10:00	11:45	01:45
6 z 12 Przerwa	MARCIN RAŁ	08-07-2026	11:45	12:00	00:15
7 z 12 Moduł 4: Bezpieczne korzystanie z internetu i zakupów	MARCIN RAŁ	08-07-2026	12:00	13:45	01:45
8 z 12 Moduł 5: Prywatność i dane osobowe	MARCIN RAŁ	08-07-2026	13:45	15:15	01:30
9 z 12 Moduł 6: Co zrobić w sytuacji zagrożenia?	MARCIN RAŁ	09-07-2026	10:00	11:30	01:30
10 z 12 Przerwa	MARCIN RAŁ	09-07-2026	11:30	11:45	00:15
11 z 12 Moduł 7: Podsumowanie – 10 zasad bezpiecznego seniora	MARCIN RAŁ	09-07-2026	11:45	14:00	02:15
12 z 12 Walidacja	-	09-07-2026	14:00	14:45	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 200,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	4 200,00 PLN
Koszt osobogodziny brutto	200,00 PLN
Koszt osobogodziny netto	200,00 PLN
W tym koszt walidacji brutto	95,00 PLN
W tym koszt walidacji netto	95,00 PLN
W tym koszt certyfikowania brutto	95,00 PLN
W tym koszt certyfikowania netto	95,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

MARCIN RAŁ

Praktyk i szkoleniowiec w zakresie technologii chmurowych oraz programowania. Uczy, jak skutecznie wykorzystać chmurę do optymalizacji procesów oraz efektywnego zarządzania infrastrukturą IT w sposób sprzyjający zrównoważonemu rozwojowi. Jako wykładowca na Uczelni Wyższej prowadzi zajęcia z programowania klienckiego, zarządzania usługami chmurowymi oraz baz danych dla aplikacji internetowych. Posiada ponad kilkunastoletnie doświadczenie w branży IT i zrealizował liczne kursy oraz warsztaty, skierowane zarówno do początkujących, jak i zaawansowanych.

W latach 2024-2026 zrealizował ponad 200 godzin szkoleniowych potwierdzonych rekomendacjami w ramach szkoleń z zakresu cyberbezpieczeństwa.

Jego szkolenia podkreślają, że technologie chmurowe odgrywają kluczową rolę w transformacji ekologicznej. Dzięki elastyczności i wydajności, jakie oferują chmury, organizacje mają możliwość zmniejszenia zużycia energii i zasobów, co ma pozytywny wpływ na ochronę środowiska.

W 2025 roku ukończył szkolenie "Cyberbezpieczeństwo".

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacje w formie PDF, pendrive, notatnik, długopis.

Warunki uczestnictwa

Wymagana jest obecność min 80% lub ze wskazaniami Operatora

Uczestnicy przyjmują do wiadomości, że usługa może być poddana monitoringowi z ramienia Operatora lub PARP i wyrażają na to zgodę. Uczestnik ma obowiązek zapisania się na usługę przez BUR co najmniej na 1 dzień roboczy przed rozpoczęciem realizacji usługi.

Przed zapisaniem się na usługę, w celu potwierdzenia dostępności miejsca w grupie szkoleniowej, prosimy o kontakt pod numerem telefonu

34 387 16 73

Informacje dodatkowe

Podstawa zwolnienia z VAT:

- 1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%
- 2) § 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 dofinansowania w co najmniej 70%
- 3) **W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT**

Adres

ul. Jasna 21
42-360 Poraj
woj. śląskie

Sala Konferencyjna UG PORAJ

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



NIKOL WATOŁA

E-mail kontakt@dofinansowanekursy.pl

Telefon (+48) 530 642 270