

**Cyberbezpieczeństwo – praktyczny kurs pracy w sieci Internet**

Numer usługi 2025/05/16/165415/2752555

5 025,00 PLN brutto

5 025,00 PLN netto

89,73 PLN brutto/h

89,73 PLN netto/h

"LIWONA" SPÓŁKA
Z OGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ



📍 zdalna w czasie rzeczywistym

🎓 Usługa szkoleniowa

🕒 56 h

📅 16.06.2025 do 04.07.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Małopolski Pociąg do kariery
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	Grupą docelową są osoby mieszkające, bądź pracujące w województwie Małopolskim, chcące podnieść swoje kwalifikacje w zakresie cyberbezpieczeństwa. Usługa również adresowana dla uczestników projektu Małopolski pociąg do kariery. Szkolenie kierowane do osób niepełnosprawnych.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	15-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	56
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa "Cyberbezpieczeństwo - praktyczny kurs pracy w sieci Internet" przygotowuje do samodzielnego i bezpiecznego korzystania z sieci Internet, zabezpieczenia swoich danych, weryfikowania informacji, sprawnego posługiwania się najpotrzebniejszymi portalami internetowymi i aplikacjami mobilnymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Podopieczny konfiguruje skrzynkę pocztową, ustawia filtry, wysyła załączniki i korzysta z różnych ustawień wiadomości. Rozpoznaje podejrzan e-maile i unika klikania w nieznane linki.	Uczestnik bezproblemowo posługuje się skrzynką e-mail, dostosowuje ustawienia do swoich preferencji oraz zachowuje swoją prywatność.	Obserwacja w warunkach rzeczywistych
	Podopieczny identyfikuje podejrzan elementy w wiadomościach (np. niezgodność domeny nadawcy, błędy w treści, podejrzan linki).	Obserwacja w warunkach rzeczywistych
Uczeń rozpoznaje wiarygodne źródła informacji, efektywnie wyszukiuje potrzebne informacje i rozróżnia, które informacje są zgodne z faktami.	Uczeń rozróżnia cechy fałszywej lub niewiarygodnej informacji (np. strony bez wskazanego autora, brak wiarygodnych odnośników).	Obserwacja w warunkach rzeczywistych
Uczestnik chroni swoje konta, w tym ustawienia prywatności, zabezpieczenia haseł, ograniczenia dostępu do swoich danych i treści dla obcych osób. Rozpoznaje, jakie informacje można bezpiecznie publikować w serwisach społecznościowych, a jakie dane (tj. adresy, zdjęcia rodzinne) powinny być chronione.	Uczeń przechodzi przez proces ustawiania konta w serwisie społecznościowym, ustawiając odpowiednie opcje prywatności i ograniczenia dostępu do swoich danych.	Obserwacja w warunkach rzeczywistych
	Uczeń wymienia i opisuje potencjalne zagrożenia związane z udostępnianiem danych osobowych w Internecie (np. kradzież tożsamości, oszustwa finansowe, stalking, naruszenie prywatności, cyberbullying).	Obserwacja w warunkach rzeczywistych
Rozpoznaje próby wyłudzenia danych (phishing, smishing, vishing) oraz odpowiednio zgłasza incydenty związane z próbą wyłudzenia danych.	Uczeń charakteryzuje przykładowe wiadomości phishingowe i pokazuje, jakie elementy wskazują na próbę wyłudzenia danych (np. fałszywe linki, błędy gramatyczne, niezgodności w adresach e-mail).	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Dokument potwierdzający uzyskanie kompetencji 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?

Dokument potwierdza, że walidacja została przeprowadzona 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?

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Jedna grupa max. 20 osobowa.

Usługa realizowana w godzinach dydaktycznych. Przerwy są wliczone w czas usługi rozwojowej.

-

<u>Dzień 1: Wprowadzenie i bezpieczeństwo e-maili</u>		
1.	Wprowadzenie do kursu: cele, plan, certyfikacja	9:00 - 10:00 (15 min przerwy)
2.	Czym jest cyberbezpieczeństwo – podstawowe pojęcia	
3.	Cyber zagrożenia – klasyfikacja: techniczne, socjaltechniczne, fizyczne	
4.	Najczęstsze wektory ataków – skrzynka e-mail, przeglądarka, telefon	

5.	Zakładanie konta e-mail (Gmail, WP, Outlook)	10:00 - 13:00 (30 min przerwy + 15 min przerwy)
6.	Bezpieczne hasło: • Co to jest silne hasło? • Przykłady dobrych i złych haseł • Tworzenie zapamiętywalnych, silnych haseł	
7.	Menadżery haseł – Bitwarden, KeePass, 1Password	
8.	Uwierzytelnianie dwuskładnikowe (2FA) – omówienie, konfiguracja	
9.	Ćwiczenia: • Ustawienie 2FA • Konfiguracja podpisu i stopki • Weryfikacja nadawców i linków • Zgłaszanie spamu i phishingu	13:00 - 14:00 (15 min przerwy)
<u>Dzień 2: E-usługi i aplikacje urzędowe</u>		
1.	EPUAP – struktura, dostęp, funkcje	9:00 - 10:00 (15 min przerwy)
2.	Profil zaufany – do czego służy, jak założyć	
3.	Wysyłka pism urzędowych online	
4.	PUE ZUS – przegląd danych o ubezpieczeniu, świadczeniach	10:00 - 13:00 (30 min przerwy + 15 min przerwy)
5.	Aplikacja mObywatel: • Instalacja, logowania, odzyskiwanie dostępu • Przegląd usług (mTożsamość, mPrawo Jazdy) • Zastrzeżenie numeru PESEL	
6.	IKP – dostęp do danych medycznych, recept, historii leczenia	
7.	Aplikacje dodatkowe: • mZUS, mBank, Duolingo, EmpikGO	13:00 - 14:00 (15 min przerwy)
8.	Ćwiczenia: • Logowanie do ePUAP, PUE, IKP	

Dzień 3: Zakupy online i media społecznościowe

1.	Rodzaje sklepów internetowych – co warto wiedzieć	9:00 - 10:00 (15 min przerwy)
2.	Bezpieczne zakupy: • Na co zwracać uwagę (certyfikaty SSL, opinie) • Jak sprawdzić firmę • Jak płacić bezpiecznie (blik, karta, płatności odroczone)	
3.	Oszustwa zakupowe – scenariusze i analiza przypadków	
4.	OLX i Allegro – na co uważać, jak nie dać się naciągnąć	10:00 - 13:00 (30 min przerwy + 15 min przerwy)
5.	Media społecznościowe: • Facebook, Instagram, TikTok – konfiguracja prywatności • LinkedIn i wizerunek zawodowy • Rozpoznawanie fałszywych profili	
6.	Dark Patterns – jak portale manipulują użytkownikami?	
7.	Warsztaty: • Zakup symulowany z analizą • Ustawienie prywatności konta na Facebooku	13:00 - 14:00 (15 min przerwy)

Dzień 4: Telefon jako centrum danych

1.	Zabezpieczenia urządzeń mobilnych: • PIN, wzór, odcisk palca, FaceID • Automatyczne blokady i szyfrowanie pamięci	9:00 - 10:00 (15 min przerwy)
2.	Usługi lokalizacyjne – jak znaleźć zagubiony telefon	
3.	Google Find My Device i Apple Find My iPhone	10:00 - 13:00 (30 min przerwy + 15 min przerwy)
4.	Funkcje ratunkowe: ICE, karta medyczna	
5.	Bezpieczne instalowanie aplikacji	
6.	Phishing i malware w aplikacjach (np. WhatsApp, Messenger, SMS)	

7.	Aplikacje bankowe – jak korzystać odpowiedzialnie	13:00 - 14:00
8.	Portfele mobilne – Google Pay, Apple Pay	(15 min przerwy)
<u>Dzień 5: Socjotechnika i manipulacje</u>		
1.	Czym jest socjotechnika – metody wpływu	9:00 - 10:00 (15 min przerwy)
2.	Scenariusze ataków emocjonalnych: • Fałszywy wnuczek • Prokurator/pulicjant • Oszust na blik	
3.	Spoofing – podszywanie się pod numer	10:00 - 13:00
4.	Telemarketing – jak się zabezpieczać i zgłaszać nękanie	(30 min przerwy + 15 min przerwy)
5.	Deepfake i voice spoofing – zagrożenia AI	
6.	Warsztaty: • Symulacja oszustwa telefonicznego	13:00 - 14:00 (15 min przerwy)
<u>Dzień 6: Dane osobowe i ochrona RODO</u>		
1.	RODO – podstawowe założenia	9:00 - 10:00
2.	Co to są dane osobowe, wrażliwe i szczególne	(15 min przerwy)
3.	Prawo do bycia zapomnianym – jak żądać usunięcia danych	10:00 - 13:00
4.	Ochrona wizerunku w Internecie	(30 min przerwy + 15 min przerwy)
5.	Jak świadomie publikować zdjęcia i dane	
6.	Retencja danych – jak długo mogą trzymać twoje dane?	13:00 - 14:00 (15 min przerwy)
7.	Przykłady naruszeń RODO i ich skutki	
<u>Dzień 7: Incydenty bezpieczeństwa i wyciek danych</u>		

1.	Jak dochodzi do wycieków danych	9:00 - 10:00
2.	Skąd wiadomo, że moje dane wyciekły? (HaveIBeenPwned, LeakCheck)	(15 min przerwy)
3.	Wyciek bazy haseł, PESEL, numeru dowodu – skutki prawne i finansowe	10:00 - 13:00
4.	Zgłoszenia do UODO, banku, CERT	(30 min przerwy +
5.	Mapowanie zagrożeń – analiza ryzyk domowych	15 min przerwy)
6.	Warsztaty: • Sprawdzanie własnych kont pod kątem wycieku • Tworzenie planu reakcji na incydent	13:00 - 14:00 (15 min przerwy)

Dzień 8: Sieci komputerowe i routery

1.	Jak działa sieć domowa (router, modem, IP)	9:00 - 10:00 (15 min przerwy)
2.	Jak zabezpieczyć router: • Zmiana hasła • Ukrycie SSID • Ustawienia zapory	
3.	Publiczne WiFi – najczęstsze zagrożenia	10:00 - 13:00
4.	VPN – co to jest, jak działa, darmowe vs płatne	(30 min przerwy +
5.	Wyszukiwanie ukrytych sieci – wardriving	15 min przerwy)
6.	Warsztaty: • Zmiana ustawień routera	13:00 - 14:00 (15 min przerwy)

Dzień 9: Nośniki danych, backup i metadane

1.	Bezpieczne korzystanie z pendrive'ów i kart SD	9:00 - 10:00 (15 min przerwy)
2.	Szyfrowanie nośników – BitLocker, VeraCrypt	10:00 - 13:00
3.	Kopia zapasowa – co i jak często kupować?	(30 min przerwy +
4.	Backup telefonu, chmura vs fizyczna kopia	15 min przerwy)

5.	Metadane – czym są i jak je usunąć	13:00 - 14:00
6.	Przykłady: metadane w zdjęciach i Wordzie	(15 min przerwy)
<u>Dzień 10: Symulacje ataków i testy phishingowe</u>		
1.	Phishing e-mailowy – przykłady, jak rozpoznać	9:00 - 10:00 (15 min przerwy)
2.	SMS phishing (smishing) - charakterystyka	10:00 - 13:00
3.	Fałszywe strony logowania – jak są generowane	(30 min przerwy + 15 min przerwy)
4.	Analiza nagłówków e-maili	
5.	Test phishingowy dla uczestników	13:00 - 14:00 (15 min przerwy)
<u>Dzień 11: Podsumowanie, test końcowy i certyfikacja</u>		
1.	Powtórka najważniejszych zagadnień	9:00 - 10:00 (15 min przerwy)
2.	Lista „10 Zasad Cyberbezpieczeństwa”	10:00 - 13:00
3.	Test wiedzy (pytania + zadania scenariuszowe)	(30 min przerwy + 15 min przerwy)
4.	Podsumowanie osiągnięć	13:00 - 14:00 (15 min przerwy)
5.	Walidacja szkolenia – Piotr Roszak 04.07.2025	09:00 - 10:00

Harmonogram

Liczba przedmiotów/zajęć: 89

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 89 Wprowadzenie do kursu: cele, plan, certyfikacja. Czym jest cyberbezpieczeństwo - podstawowe pojęcia. Cyber zagrożenia, najczęstsze wektory zagrożenia	Grzegorz Chlebus	16-06-2025	09:00	09:45	00:45
2 z 89 Przerwa	Grzegorz Chlebus	16-06-2025	09:45	10:00	00:15
3 z 89 Zakładanie konta e-mail (Gmail, WP, Outlook). Bezpieczne hasło - pojęcie, przykłady i tworzenie haseł	Grzegorz Chlebus	16-06-2025	10:00	11:15	01:15
4 z 89 Przerwa obiadowa	Grzegorz Chlebus	16-06-2025	11:15	11:45	00:30
5 z 89 Menadżery haseł, uwierzytelnianie dwuskładnikowe	Grzegorz Chlebus	16-06-2025	11:45	12:45	01:00
6 z 89 Przerwa	Grzegorz Chlebus	16-06-2025	12:45	13:00	00:15
7 z 89 Ćwiczenia	Grzegorz Chlebus	16-06-2025	13:00	13:45	00:45
8 z 89 Przerwa	Grzegorz Chlebus	16-06-2025	13:45	14:00	00:15
9 z 89 EPUAP; Profil zaufany: Wysyłka pism urzędowych	Grzegorz Chlebus	17-06-2025	09:00	09:45	00:45
10 z 89 Przerwa	Grzegorz Chlebus	17-06-2025	09:45	10:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 89 PUE ZUS; Aplikacja mObywatel - Instalacja, logowania, odzyskiwanie dostępu, przegląd usług	Grzegorz Chlebus	17-06-2025	10:00	11:15	01:15
12 z 89 Przerwa obiadowa	Grzegorz Chlebus	17-06-2025	11:15	11:45	00:30
13 z 89 Aplikacja mObywatel: Zastrzerzenie numeru PESEL. IKP - dostęp do danych medycznych, recept, historii leczenia	Grzegorz Chlebus	17-06-2025	11:45	12:45	01:00
14 z 89 Przerwa	Grzegorz Chlebus	17-06-2025	12:45	13:00	00:15
15 z 89 Aplikacje dodatkowe (mZUS, mBank, Duolingo, EmpikGO). Ćwiczenia	Grzegorz Chlebus	17-06-2025	13:00	13:45	00:45
16 z 89 Przerwa	Grzegorz Chlebus	17-06-2025	13:45	14:00	00:15
17 z 89 Rodzaje sklepów internetowych. Bezpieczne zakupy	Grzegorz Chlebus	19-06-2025	09:00	09:45	00:45
18 z 89 Przerwa	Grzegorz Chlebus	19-06-2025	09:45	10:00	00:15
19 z 89 Oszustwa zakupowe. OLX i Allegro - na co uważać	Grzegorz Chlebus	19-06-2025	10:00	11:15	01:15
20 z 89 Przerwa obiadowa	Grzegorz Chlebus	19-06-2025	11:15	11:45	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 89 Media społecznościowe : Facebook, Instagram, TikTok, LinkedIn, rozpoznawanie fałszywych profili. Dark Patterns.	Grzegorz Chlebus	19-06-2025	11:45	12:45	01:00
22 z 89 Przerwa	Grzegorz Chlebus	19-06-2025	12:45	13:00	00:15
23 z 89 Warsztaty: Zakup symulowany z analizą, ustawienie prywatności konta na Facebooku	Grzegorz Chlebus	19-06-2025	13:00	13:45	00:45
24 z 89 Przerwa	Grzegorz Chlebus	19-06-2025	13:45	14:00	00:15
25 z 89 Zabezpieczenia urządzeń mobilnych, usługi lokalizacyjne	Grzegorz Chlebus	23-06-2025	09:00	09:45	00:45
26 z 89 Przerwa	Grzegorz Chlebus	23-06-2025	09:45	10:00	00:15
27 z 89 Google Find My Device i Apple Find My iPhone; Funkcje ratunkowe: ICE, karta medyczna	Grzegorz Chlebus	23-06-2025	10:00	11:15	01:15
28 z 89 Przerwa obiadowa	Grzegorz Chlebus	23-06-2025	11:15	11:45	00:30
29 z 89 Bezpieczne instalowanie aplikacji, phishing i malware w aplikacjach	Grzegorz Chlebus	23-06-2025	11:45	12:45	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
30 z 89 Przerwa	Grzegorz Chlebus	23-06-2025	12:45	13:00	00:15
31 z 89 Aplikacje bankowe, portfele mobilne	Grzegorz Chlebus	23-06-2025	13:00	13:45	00:45
32 z 89 Przerwa	Grzegorz Chlebus	23-06-2025	13:45	14:00	00:15
33 z 89 Czym jest socjotechnika, scenariusze ataków emocjonalnych	Grzegorz Chlebus	24-06-2025	09:00	09:45	00:45
34 z 89 Przerwa	Grzegorz Chlebus	24-06-2025	09:45	10:00	00:15
35 z 89 Scenariusze ataków emocjonalnych cd.; spoofing	Grzegorz Chlebus	24-06-2025	10:00	11:15	01:15
36 z 89 Przerwa obiadowa	Grzegorz Chlebus	24-06-2025	11:15	11:45	00:30
37 z 89 Telemarketing, deepfake i voice spoofing	Grzegorz Chlebus	24-06-2025	11:45	12:45	01:00
38 z 89 Przerwa	Grzegorz Chlebus	24-06-2025	12:45	13:00	00:15
39 z 89 Warsztaty: Symulacja oszustwa telefonicznego	Grzegorz Chlebus	24-06-2025	13:00	13:45	00:45
40 z 89 Przerwa	Grzegorz Chlebus	24-06-2025	13:45	14:00	00:15
41 z 89 RODO - podstawowe założenia, co to są dane osobowe, wrażliwe i szczególne	Grzegorz Chlebus	25-06-2025	09:00	09:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
42 z 89 Przerwa	Grzegorz Chlebus	25-06-2025	09:45	10:00	00:15
43 z 89 Prawo do bycia zapomnianym, ochrona wizerunku w Internecie	Grzegorz Chlebus	25-06-2025	10:00	11:15	01:15
44 z 89 Przerwa obiadowa	Grzegorz Chlebus	25-06-2025	11:15	11:45	00:30
45 z 89 Ochrona wizerunku w Internecie cd., jak świadomie publikować zdjęcia i dane	Grzegorz Chlebus	25-06-2025	11:45	12:45	01:00
46 z 89 Przerwa	Grzegorz Chlebus	25-06-2025	12:45	13:00	00:15
47 z 89 Retencja danych; przykłady naruszeń RODO i ich skutki	Grzegorz Chlebus	25-06-2025	13:00	13:45	00:45
48 z 89 Przerwa	Grzegorz Chlebus	25-06-2025	13:45	14:00	00:15
49 z 89 Jak dochodzi do wycieków danych. Skąd wiadomo, że moje dane wyciekły?	Grzegorz Chlebus	26-06-2025	09:00	09:45	00:45
50 z 89 Przerwa	Grzegorz Chlebus	26-06-2025	09:45	10:00	00:15
51 z 89 Wyciek bazy haseł, PESEL, numeru dowodu. Zgłoszenia do UODO, banku, CERT.	Grzegorz Chlebus	26-06-2025	10:00	11:15	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
52 z 89 Przerwa obiadowa	Grzegorz Chlebus	26-06-2025	11:15	11:45	00:30
53 z 89 Zgłoszenia do UODO, banku, CERT cd. Mapowanie zagrożeń – analiza ryzyk domowych	Grzegorz Chlebus	26-06-2025	11:45	12:45	01:00
54 z 89 Przerwa	Grzegorz Chlebus	26-06-2025	12:45	13:00	00:15
55 z 89 Warsztaty: sprawdzanie własnych kont pod kątem wycieku, tworzenie planu reakcji na incydent	Grzegorz Chlebus	26-06-2025	13:00	13:45	00:45
56 z 89 Przerwa	Grzegorz Chlebus	26-06-2025	13:45	14:00	00:15
57 z 89 Jak działa sieć domowa? Jak zabezpieczyć router?	Grzegorz Chlebus	30-06-2025	09:00	09:45	00:45
58 z 89 Przerwa	Grzegorz Chlebus	30-06-2025	09:45	10:00	00:15
59 z 89 Jak zabezpieczyć router cd. Publiczne WiFi	Grzegorz Chlebus	30-06-2025	10:00	11:15	01:15
60 z 89 Przerwa obiadowa	Grzegorz Chlebus	30-06-2025	11:15	11:45	00:30
61 z 89 VPN, wyszukiwanie ukrytych sieci	Grzegorz Chlebus	30-06-2025	11:45	12:45	01:00
62 z 89 Przerwa	Grzegorz Chlebus	30-06-2025	12:45	13:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
63 z 89 Warsztaty: zmiana ustawień routera	Grzegorz Chlebus	30-06-2025	13:00	13:45	00:45
64 z 89 Przerwa	Grzegorz Chlebus	30-06-2025	13:45	14:00	00:15
65 z 89 Bezpieczne korzystanie z pendrive'ów i kart SD	Grzegorz Chlebus	01-07-2025	09:00	09:45	00:45
66 z 89 Przerwa	Grzegorz Chlebus	01-07-2025	09:45	10:00	00:15
67 z 89 Szyfrowanie nośników, kopia zapasowa	Grzegorz Chlebus	01-07-2025	10:00	11:15	01:15
68 z 89 Przerwa obiadowa	Grzegorz Chlebus	01-07-2025	11:15	11:45	00:30
69 z 89 Kopia zapasowa cd., backup telefonu, chmura vs fizyczna kopia	Grzegorz Chlebus	01-07-2025	11:45	12:45	01:00
70 z 89 Przerwa	Grzegorz Chlebus	01-07-2025	12:45	13:00	00:15
71 z 89 Metadane - czym są i jak je usunąć? Przykłady	Grzegorz Chlebus	01-07-2025	13:00	13:45	00:45
72 z 89 Przerwa	Grzegorz Chlebus	01-07-2025	13:45	14:00	00:15
73 z 89 Phishing e-mailowy - przykłady, jak rozpoznać	Grzegorz Chlebus	02-07-2025	09:00	09:45	00:45
74 z 89 Przerwa	Grzegorz Chlebus	02-07-2025	09:45	10:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
75 z 89 SMS phishing (smishing). Falszywe strony logowania – jak są generowane.	Grzegorz Chlebus	02-07-2025	10:00	11:15	01:15
76 z 89 Przerwa obiadowa	Grzegorz Chlebus	02-07-2025	11:15	11:45	00:30
77 z 89 Falszywe strony logowania – jak są generowane cd. Analiza nagłówków e-maili.	Grzegorz Chlebus	02-07-2025	11:45	12:45	01:00
78 z 89 Przerwa	Grzegorz Chlebus	02-07-2025	12:45	13:00	00:15
79 z 89 Test phishingowy dla uczestników	Grzegorz Chlebus	02-07-2025	13:00	13:45	00:45
80 z 89 Przerwa	Grzegorz Chlebus	02-07-2025	13:45	14:00	00:15
81 z 89 Powtórka najważniejszych zagadnień	Grzegorz Chlebus	03-07-2025	09:00	09:45	00:45
82 z 89 Przerwa	Grzegorz Chlebus	03-07-2025	09:45	10:00	00:15
83 z 89 Lista "10 Zasad Cyberbezpieczeństwa"	Grzegorz Chlebus	03-07-2025	10:00	11:15	01:15
84 z 89 Przerwa obiadowa	Grzegorz Chlebus	03-07-2025	11:15	11:45	00:30
85 z 89 Test wiedzy	Grzegorz Chlebus	03-07-2025	11:45	12:45	01:00
86 z 89 Przerwa	Grzegorz Chlebus	03-07-2025	12:45	13:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
87 z 89 Podsumowanie osiągnięć	Grzegorz Chlebus	03-07-2025	13:00	13:45	00:45
88 z 89 Przerwa	Grzegorz Chlebus	03-07-2025	13:45	14:00	00:15
89 z 89 Walidacja szkolenia	-	04-07-2025	10:00	11:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 025,00 PLN
Koszt przypadający na 1 uczestnika netto	5 025,00 PLN
Koszt osobogodziny brutto	89,73 PLN
Koszt osobogodziny netto	89,73 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Grzegorz Chlebus

Trener, przedsiębiorca i specjalista w zakresie zarządzania, audytów oraz energetyki odnawialnej. Od lat związany z biznesem jako wspólnik kilku firm wspierających działania marketingowe, a także przedsiębiorstwa zajmującego się pomocą osobom fizycznym i firmom w kryzysie finansowym. Posiada szeroką wiedzę z zakresu systemów zarządzania jakością – jest audytorem wewnętrznym systemu zarządzania jakością według normy PN-EN ISO 9001:2015. Ekspert w branży nieruchomości jako zarządca nieruchomości wielkopowierzchniowych oraz audytor energetyczny i remontowy budynków. Posiada tytuł technika urządzeń i systemów energetyki odnawialnej, co pozwala mu łączyć wiedzę techniczną z praktycznym podejściem do efektywności energetycznej. Jako certyfikowany trener VCC prowadzi szkolenia, dzieląc się swoją wiedzą i doświadczeniem. Jednocześnie kontynuuje swoją edukację jako student trzeciego roku prawa, co umożliwia mu lepsze zrozumienie aspektów prawnych związanych z prowadzoną działalnością. Dzięki połączeniu wiedzy z różnych dziedzin skutecznie doradza i wspiera firmy oraz osoby

prywatne w optymalizacji procesów, zarządzaniu nieruchomościami i rozwiązywaniu problemów finansowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Po ukończonym szkoleniu zakończonym testem, uczestnicy dostaną zaświadczenie o odbytych szkoleniu oraz certyfikat zdobytych kompetencji.

Informacje dodatkowe

Zaakceptowano Regulamin dla Instytucji Szkoleniowych.

Warunki techniczne

Minimalne parametry łącza wymaganego do komfortowego uczestnictwa w szkoleniu za pośrednictwem platformy Zoom: 5 Mb/s (przesyłanie) | 3,5 Mb/s (pobieranie)

Minimalne parametry sprzętu:

Procesor : Unisoc SC9832E (4x rdzenie o taktowaniu 1.40 GHz)

Układ graficzny: Mali T820 MP1

Pamięć RAM: 2 GB

Dysk twardy: 32GB

Przekątna i rozdzielczość wyświetlacza: 8.0" 1280x800

Łączność: WiFi i/lub LTE

System operacyjny: Android 13 GO

Kontakt



Natalia Papuga

E-mail natalia@liwona.pl

Telefon (+48) 500 101 118