Możliwość dofinansowania

Bezpieczne korzystanie z narzędzi cyfrowych i ochrona informacji w pracy online

Numer usługi 2026/03/09/157622/3391042

935,00 PLN brutto
935,00 PLN netto
187,00 PLN brutto/h
187,00 PLN netto/h
196,00 PLN cena rynkowa

Grupa WW GovTech sp. z o.o.

★★★★★ 5,0 / 5

40 ocen

Nisko / stacjonarna
Usługa szkoleniowa
5 h
25.05.2026 do 25.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	## Grupa docelowa • pracownicy organizacji korzystający z poczty e-mail, internetu, aplikacji i kont online, • osoby pracujące z danymi i dokumentami w środowisku cyfrowym, • pracownicy działów administracyjnych, HR, sprzedaży, obsługi klienta i komunikacji, • osoby wykonujące zadania w modelu zdalnym lub hybrydowym, • osoby odpowiedzialne za bezpieczne korzystanie z kont i komunikacji online w codziennej pracy.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	22-05-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	5
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 przygotowanie uczestników do bezpiecznego korzystania z narzędzi cyfrowych w codziennej pracy poprzez rozpoznawanie zagrożeń online, stosowanie zasad cyberhigieny, zabezpieczanie kont i danych, ocenę wiarygodności wiadomości, linków i źródeł informacji oraz ograniczanie ryzyk zakłócających cyfrowe procesy pracy w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wskazuje podstawowe zagrożenia występujące podczas korzystania z narzędzi cyfrowych i rozróżnia ich wpływ na użytkownika oraz organizację.	Rozróżnia rodzaje zagrożeń cyfrowych oraz przyporządkowuje ich skutki do sytuacji zawodowych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozróżnia phishing, vishing, smishing, malware i ransomware oraz wskazuje charakterystyczne cechy tych zagrożeń.	Przyporządkowuje cechy i kanały ataku do właściwego rodzaju zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje zasady cyberhigieny oraz rozróżnia rozwiązania służące ochronie kont i dostępu do danych.	Dobiera poprawne zasady haseł, rozróżnia zastosowanie 2FA/MFA oraz wskazuje rolę menedżera haseł.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozróżnia podejrzane linki, wiadomości, załączniki i strony internetowe oraz wskazuje działania ograniczające ryzyko.	Identyfikuje sygnały ostrzegawcze i dobiera bezpieczne działania użytkownika.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje sposoby sprawdzania wycieków danych i rozróżnia działania podejmowane po wykryciu naruszenia lub przejęcia konta.	Dobiera działanie do rodzaju naruszenia i wskazuje właściwą kolejność podstawowych czynności zabezpieczających.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje narzędzia i kryteria oceny wiarygodności informacji oraz rozróżnia źródła bardziej i mniej wiarygodne.	Dobiera kryterium oceny do przykładowej informacji i rozróżnia źródła pod względem wiarygodności.	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

Zakres usługi / ramowy program

1. **Cyberbezpieczeństwo w pracy online – podstawowe pojęcia i ryzyka:** Rola użytkownika w ochronie informacji i ciągłości pracy z wykorzystaniem narzędzi cyfrowych.
2. **Najczęstsze zagrożenia w środowisku cyfrowym:** Phishing, vishing, smishing, malware, ransomware – charakterystyka i skutki dla użytkownika oraz organizacji.
3. **Techniki ataków i sygnały ostrzegawcze:** Socjotechnika, presja czasu, podszywanie się, fałszywe domeny, podejrzane linki i załączniki.
4. **Cyberhigiena i ochrona kont:** Zasady tworzenia i sprawdzania haseł, 2FA/MFA, menedżery haseł, zabezpieczanie poczty, kont społecznościowych i kont zakupowych.
5. **Bezpieczna praca z informacją i danymi w środowisku cyfrowym:** Rozpoznawanie podejrzanych wiadomości, stron i załączników; działania ograniczające ryzyko ujawnienia danych.
6. **Weryfikacja wycieków danych i reagowanie na incydenty użytkownika:** Jak sprawdzić, czy dane wyciekły, jakie działania podjąć po wykryciu naruszenia lub przejęcia konta.
7. **Ocena wiarygodności informacji i źródeł online:** Narzędzia i kryteria oceny źródeł, weryfikacja treści i komunikatów otrzymywanych online.
8. **Podsumowanie + Q&A**
9. **Walidacja** – test teoretyczny z wynikiem generowanym automatycznie.

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Cyberbezpieczeństwo w pracy online: podstawowe pojęcia i ryzyka	-	25-05-2026	09:00	09:30	00:30
2 z 9 Najczęstsze zagrożenia: phishing, vishing, smishing, malware, ransomware	-	25-05-2026	09:30	10:15	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 9 Techniki ataków i sygnały ostrzegawcze: linki, domeny, załączniki, wiadomości	-	25-05-2026	10:15	11:00	00:45
4 z 9 Przerwa	-	25-05-2026	11:00	11:15	00:15
5 z 9 Cyberhigiena i ochrona kont: hasła, 2FA/MFA, menedżery haseł, zabezpieczenia kont	-	25-05-2026	11:15	12:00	00:45
6 z 9 Bezpieczna praca z informacją i danymi: wiadomości, strony, załączniki, działania ochronne	-	25-05-2026	12:00	12:45	00:45
7 z 9 Weryfikacja wycieków danych i reagowanie na incydenty użytkownika	-	25-05-2026	12:45	13:30	00:45
8 z 9 Ocena wiarygodności informacji i źródeł online + podsumowanie i Q&A	-	25-05-2026	13:30	13:45	00:15
9 z 9 Walidacja: test teoretyczny (wynik generowany automatycznie)	-	25-05-2026	13:45	14:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	935,00 PLN
Koszt przypadający na 1 uczestnika netto	935,00 PLN
Koszt osobogodziny brutto	187,00 PLN
Koszt osobogodziny netto	187,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzyma prezentację ze szkolenia oraz zaświadczenie.

Informacje dodatkowe

Podstawa zwolnienia z VAT:

1. art. 43 ust. 1 pkt 29 lit. c ustawy o VAT – dofinansowanie 100%,
2. § 3 ust. 1 pkt 14 rozporządzenia MF – dofinansowanie min. 70%,
3. przy dofinansowaniu poniżej 70% do ceny doliczany jest VAT 23%.

Adres

ul. Sandomierska Boczna 2
37-400 Nisko
woj. podkarpackie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Wojciech Polar

E-mail w.polar@grupaww.pl
Telefon (+48) 784 405 838