Możliwość dofinansowania

Growth Advisors
Jacek Piątkowski

★★★★½

Cyberbezpieczeństwo w miejscu pracy - Ochrona przed zagrożeniami

Numer usługi 2025/02/21/41113/2575125

zdalna w czasie rzeczywistym
Usługa szkoleniowa
11 h
24.04.2025 do 24.04.2025

1 405,89 PLN brutto
1 143,00 PLN netto
127,81 PLN brutto/h
103,91 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Firmy z sektora MŚP, które chcą zwiększyć swoje bezpieczeństwo w sieci oraz poznać aktualne zagrożenia, • Kierownicy i managerowie, odpowiedzialni za zarządzanie zespołami i projektami, które powinny być świadome zagrożeń i metod ochrony, • Pracownicy wszystkich szczebli w celu podniesienia ogólnej świadomości dotyczącej cyberzagrożeń, • Osoby pracujące zdalnie w kontekście nauki bezpiecznego korzystania z technologii i ochrony danych osobowych w pracy zdalnej, • Instytucje publiczne, które muszą przestrzegać norm bezpieczeństwa danych, • Osoby poszukujące pracy w IT, które chcą zdobyć wiedzę w zakresie cyberbezpieczeństwa, jako elementy swojej kariery zawodowej.
Minimalna liczba uczestników	7
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	22-04-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	11
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie z cyberbezpieczeństwa ma na celu przede wszystkim zwiększenie świadomości uczestników na temat zagrożeń w sieci oraz metod ochrony przed nimi. Uczestnicy uczą się rozpoznawać potencjalne ataki, takie jak phishing czy malware, co pozwala im lepiej chronić swoje dane osobowe i firmowe. Dodatkowo, szkolenie może pomóc w rozwinięciu umiejętności praktycznych takich jak zarządzanie hasłami czy korzystanie z narzędzi zabezpieczających. Wreszcie, zdobycie wiedzy z zakresu cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zrozumie podstawowe zagadnienia związane z bezpieczeństwem online	Uczestnik potrafi zdefiniować pojęcie bezpieczeństwa w sieci oraz wymienić przykłady zagrożeń i ataków	Test teoretyczny
	Uczestnik potrafi wymienić podstawowe terminy związane z bezpieczeństwem w sieci	Test teoretyczny
Uczestnik rozumie konieczność korzystania z silnych haseł i potrafi je tworzyć	Uczestnik rozumie, dlaczego powinien tworzyć silne hasła w sieci i zna ryzyko związane z posiadaniem słabych haseł	Test teoretyczny
	Uczestnik umie stworzyć silne hasło	Test teoretyczny
Uczestnik zna zasady ochrony konputerów i sieci internetowej	Uczestnik potrafi opisać znaczenie wdrożenia podstawowych środków ochrony, takich jak aktualizacje oprogramowania oraz zabezpieczenie sieci wifi	Test teoretyczny
Uczestnik potrafi rozpoznawać zagrożenia online	Uczestnik potrafi wymienić rodzaje oprogramowania antywirusowego	Test teoretyczny
	Uczestnik wie po czym rozpoznawać podejrzane wiadomości email, sms i połączenia telefoniczne	Test teoretyczny
	Uczestnik zna podstawowe zasady bezpieczeństwa związane z ochroną poczty email, mediami społecznościowymi i zakupami online	Test teoretyczny
Uczestnik rozumie znaczenie ochrony urządzeń mobilnych	Uczestnik potrafi skonfigurować zabezpieczenia na urządzeniach mobilnych	Test teoretyczny
	Uczestnik potrafi opisać znaczenie aktualizacji oprogramowania	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozumie znaczenie bezpieczeństwa danych osobowych w sieci	Uczestnik zna zasady ochrony danych osobowych	Test teoretyczny
	Uczestnik wie jak chronić swoje dane osobowe, oraz dane z którymi pracuje, przed kradzieżą	Test teoretyczny
	Uczestnik potrafi sprawdzić czy jego dane osobowe nie wyciekły do sieci	Test teoretyczny
Uczestnik rozumie zagrożena dotyczące cyberbezpieczeństwa wynikające z pracy zdalnej	Uczestnik wie z jakimi typami ataków może się spotkać podczas pracy zdalnej	Test teoretyczny
	Uczestnik zna zasady pracy zdalnej z danymi wrażliwymi i wie jak unikać potencjalnych zagrożeń	Test teoretyczny
KOMPETENCJE SPOŁECZNE: Uczestnik potrafi rozpoznawać zagrożenia związane z poznawaniem nowych osób online	Uczestnik zna podstawowe zasady cyberhigieny	Test teoretyczny
	Uczestnik wie jak rozpoznać podejrzane kontakty ze strony osób trzecich, na przykład w mediach społecznościowych	Test teoretyczny
	Uczestnik wie co to jest SCAM	Test teoretyczny
	Uczestnik rozumie ryzyko związane z otrzymywaniem widomości i linków z nieznanych źródeł	Test teoretyczny

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

MODUŁ I. Wprowadzenie do bezpieczeństwa i ochrony online

- Wprowadzenie do tematu
- Statystyki: dane dotyczące wzrostu zagrożeń online
- Definicja bezpieczeństwa w sieci z przykładami ataków z życia codziennego
- Przegląd podstawowych terminów i definicji związanych z bezpieczeństwem online
- Zagrożenia związane z korzystaniem z telefonów i komputerów
- Demonstracja programów do tworzenia fałszywej tożsamości online oraz case study

MODUŁ II. Hasła

- Dlaczego mocne hasła są kluczowe?
- Ryzyka związane z używaniem słabych i łatwo odgadnianych haseł
- Sposoby i narzędzia do tworzenia silnych haseł
- Ciekawostki: najdziwniejsze hasła używane przez ludzi
- Praktyczna prezentacja łamania popularnych haseł
- Ćwiczenia zarządzania hasłami

MODUŁ III. Ochrona komputerów i sieci

- Wprowadzenie do antywirusów i oprogramowania zabezpieczającego
- Znaczenie aktualizacji systemów i aplikacji w zapewnianiu bezpieczeństwa
- Praktyczne wskazówki dotyczące aktualizacji
- Bezpieczne korzystanie z poczty elektronicznej i unikanie zagrożeń
- Zabezpieczanie sieci Wi-Fi i ustawienia routera
- Zasady korzystania z bezpiecznych sieci

MODUŁ IV. Rozpoznawanie i unikanie zagrożeń online

- Jak rozpoznawać podejrzane wiadomości e-mail, SMS-y i połączenia telefoniczne
- Demonstracja faktycznej rozmowy z oszustem
- Bezpieczne surfowanie w internecie i unikanie podejrzanych witryn
- Symulacja kontrolowanego ataku na wymyślone konto
- Ochrona skrzynki e-mail
- Zagrożenia związane z social mediami
- Bezpieczne zakupy online i ochrona przed oszustwami

MODUŁ V. Ochrona urządzeń mobilnych (telefony komórkowe)

- Zabezpieczanie ekranu blokady i hasła
- Aktualizacje systemowe i oprogramowania
- Bezpieczne korzystanie z aplikacji mobilnych
- Ostrzeżenia dotyczące nieznanych wiadomości i linków
- Ćwiczenia: Ustawianie prywatności i zarządzanie uprawnieniami aplikacji

MODUŁ VI. Bezpieczeństwo danych osobowych

- Jak chronić dane osobowe przed kradzieżą
- Zasady pracy z danymi wrażliwymi
- Sprawdzanie, czy dane osobowe uczestników nie wyciekły
- Uświadomienie uczestnikom, dlaczego cyberbezpieczeństwo i RODO stanowią nieodłączną parę w dzisiejszym świecie biznesu. Obie te dziedziny ściśle się ze sobą wiążą, a brak należytej ochrony danych osobowych może prowadzić do poważnych konsekwencji, zarówno finansowych, jak i reputacyjnych dla firmy.
- Co oznacza RODO dla cyberbezpieczeństwa?
- Wymagania prawne i regulacyjne dotyczące ochrony danych, takie jak RODO

MODUŁ VII. Bezpieczeństwo pracy zdalnej/ hybrydowej w kontekście RODO/Cyberbezpieczeństwa

- Typowe ataki na osoby pracujące zdalnie

- Na co zwrócić uwagę podczas pracy zdalnej
- Najlepsze praktyki dotyczące ochrony danych w pracy zdalnej
- Jak rozpoznawać i unikać potencjalnych zagrożeń związanych z ochroną danych osobowych w swojej pracy
- Jak właściwie postępować z danymi klientów i współpracowników, aby nie naruszać przepisów RODO
- Bezpieczeństwo w chmurze: zagrożenia i najlepsze praktyki związane z usługami chmurowymi
- Wykształcenie właściwych nawyków cyberhigieny, które są kluczowe w codziennej pracy (w tym pracy zdalnej), aby skutecznie chronić dane osobowe

MODUŁ VIII. Podsumowanie szkolenia

- Podsumowanie kluczowych punktów
- Zachęta do implementacji nowych nawyków online
- Sesja pytań i odpowiedzi

MODUŁ IX. Walidacja

- Test wiedzy

Harmonogram

Liczba przedmiotów/zajęć: 12

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Wprowadzenie do bezpieczeństwa i ochrony online	Grzegorz Małek	24-04-2025	08:00	09:00	01:00
2 z 12 Hasła	Grzegorz Małek	24-04-2025	09:00	10:00	01:00
3 z 12 PRZERWA	Grzegorz Małek	24-04-2025	10:00	10:15	00:15
4 z 12 Ochrona komputerów i sieci	Grzegorz Małek	24-04-2025	10:15	11:15	01:00
5 z 12 Rozpoznawanie i unikanie zagrożeń online	Grzegorz Małek	24-04-2025	11:15	12:15	01:00
6 z 12 PRZERWA	Grzegorz Małek	24-04-2025	12:15	12:30	00:15
7 z 12 Ochrona urządzeń mobilnych (telefony komórkowe)	Grzegorz Małek	24-04-2025	12:30	13:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 12 Bezpieczeństwo danych osobowych	Grzegorz Małek	24-04-2025	13:30	14:30	01:00
9 z 12 PRZERWA	Grzegorz Małek	24-04-2025	14:30	14:45	00:15
10 z 12 Bezpieczeństwo pracy zdalnej/ hybrydowej w kontekście RODO/Cyberbezpieczeństwa i podsumowanie szkolenia	Grzegorz Małek	24-04-2025	14:45	16:00	01:15
11 z 12 Podsumowanie	Grzegorz Małek	24-04-2025	16:00	16:30	00:30
12 z 12 Walidacja	-	24-04-2025	16:30	17:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 405,89 PLN
Koszt przypadający na 1 uczestnika netto	1 143,00 PLN
Koszt osobogodziny brutto	127,81 PLN
Koszt osobogodziny netto	103,91 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Grzegorz Małek

Trener z zakresu cyberbezpieczeństwa i programowania, posiadający bogate doświadczenie edukacyjne oraz zawodowe. Ukończył studia z zakresu informatyki śledczej na Wyższej Szkole

Przedsiębiorczości i Administracji w Lublinie oraz inżynierię oprogramowania na Wyższej Szkole Informatyki i Zarządzania w Rzeszowie. Dodatkowo, zdobył wiedzę na podyplomowych studiach z fizyki na Uniwersytecie Marii Curie-Skłodowskiej oraz w zakresie administracji infrastruktury informacyjnej. Jako trener programowania, prowadził kursy w językach takich jak Java, Python i JavaScript w renomowanych firmach w Polsce. Wykłada przedmioty związane z programowaniem i systemami zarządzania treścią na Dolnośląskiej Szkole Wyższej we Wrocławiu. Jego doświadczenie obejmuje także prowadzenie szkoleń z zakresu cyberbezpieczeństwa, testów penetracyjnych oraz systemów kontroli wersji GIT. Właściciel własnej firmy w dziedzinie technologii informatycznych, a także nauczyciel zawodu Technik Informatyk i Programista. Posiada liczne certyfikaty, w tym CyberOps Associate oraz Microsoft Certified Trainer, co potwierdza jego kompetencje w obszarze bezpieczeństwa IT. Jego umiejętności obejmują nie tylko programowanie, ale również diagnostykę sprzętu komputerowego, konfigurację systemów operacyjnych oraz zarządzanie bazami danych. Trener z pasją do wdrażania innowacji w obszarze programowania i cyberbezpieczeństwa, angażujący się w edukację młodzieży oraz dorosłych w zakresie bezpiecznego korzystania z technologii.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1 godzina szkolenia to godzina dydaktyczna (45 min).

Uczestnik otrzyma:

- materiały szkoleniowe i dydaktyczne
- zaświadczenie o ukończeniu szkolenia.

Informacje dodatkowe

1. Oferujemy kompleksowe wsparcie w **pozyskaniu dofinansowania** na wszystkie oferowane usługi.
2. Realizujemy szkolenia również w **formie zamkniętej, dla konkretnych organizacji**, oddziałów firm, z możliwością **dopasowania usługi do konkretnych potrzeb** organizacji.
3. Przed zgłoszeniem na usługę **prosimy o kontakt** w celu potwierdzenia dostępności wolnych miejsc/gwarancji terminu.

Warunki techniczne

Szkolenie będzie prowadzone na platformie MS Teams. Uczestnik otrzyma link oraz niezbędne login i hasło do zalogowania się.

Wymagany jest dostęp do komputera lub laptopa z kamerą, mikrofonem i głośnikami, sieci wifi lub internetu przewodowego.

Kontakt

Marta Kozłowska

E-mail marta.kozlowska@growthadvisors.pl
Telefon (+48) 882 214 768