Możliwość dofinansowania

Cyberprzestępczość - Podstawy Cyberbezpieczeństwa dla pracowników Administracyjno - Biurowych.

Numer usługi 2026/04/08/216002/3470893

504,00 PLN brutto
504,00 PLN netto
126,00 PLN brutto/h
126,00 PLN netto/h
261,33 PLN cena rynkowa

KORPORACJA "ROMANISZYN" PRZEDSIĘBIORSTWO PRODUKCYJNO-HANDLOWO-USŁUGOWE STANISŁAW ROMANISZYN

★★★★★ 5,0 / 5

1 ocena

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
04:00 h
30.06.2026 do 30.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób, które chcą zdobyć podstawową wiedzę z zakresu cyberbezpieczeństwa oraz nauczyć się rozpoznawać i unikać zagrożeń w środowisku cyfrowym. W szczególności dedykowane jest do pracowników biurowych i administracyjnych, którzy w codziennej pracy korzystają z komputerów, poczty elektronicznej, Internetu oraz systemów informatycznych. Przeznaczone jest dla osób nietechnicznych, pracujących z danymi osobowymi, finansowymi lub firmowymi, niezależnie od zajmowanego stanowiska. Szkolenie nie wymaga wcześniejszej wiedzy technicznej – jest wprowadzeniem do tematyki cyberbezpieczeństwa.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	23-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	4
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

Zwiększenie świadomości pracowników w zakresie cyberbezpieczeństwa oraz sposobów działania cyberprzestępców. Uczestnicy zdobędą wiedzę umożliwiającą rozpoznawanie najczęstszych zagrożeń, takich jak phishing, ataki socjotechniczne czy złośliwe oprogramowanie, oraz poznają skuteczne metody ochrony danych i systemów. Szkolenie kształtuje bezpieczne nawyki w codziennej pracy i uczy prawidłowego reagowania na incydenty cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe pojęcia związane z cyberprzestępczością i cyberbezpieczeństwem.	- definiuje pojęcia: cyberprzestępczość, phishing, malware, botnet, DDoS - wskazuje różnice między głównymi typami zagrożeń - omawia cele działania cyberprzestępców	Obserwacja w warunkach symulowanych
Identyfikuje współczesne zagrożenia w sieci oraz metody działania cyberprzestępców.	- opisuje działanie grup cyberprzestępczych - wyjaśnia mechanizm ataków DoS/DDoS oraz 0-day - rozpoznaje zastosowanie sztucznej inteligencji w cyberatakach	Obserwacja w warunkach rzeczywistych
Rozpoznaje najczęstsze techniki ataków skierowanych do użytkowników.	- wymienia i opisuje rodzaje phishingu i socjotechniki - wskazuje cechy charakterystyczne spamu i złośliwych wiadomości - omawia sposoby infekcji systemów (np. załączniki, nośniki danych)	Obserwacja w warunkach symulowanych
Wyjaśnia skutki cyberataków oraz zagrożenia związane z utratą danych.	- opisuje konsekwencje naruszenia bezpieczeństwa (finansowe, wizerunkowe, prawne) - wyjaśnia mechanizm kradzieży tożsamości - omawia znaczenie ochrony haseł i danych	Obserwacja w warunkach symulowanych
Identyfikuje potencjalne zagrożenia w codziennej pracy z wykorzystaniem komputera i internetu.	- analizuje przykładowe wiadomości e-mail i wskazuje zagrożenia - rozpoznaje podejrzane linki, załączniki i komunikaty - ocenia poziom ryzyka w przedstawionych sytuacjach	Obserwacja w warunkach rzeczywistych
Stosuje podstawowe zasady bezpieczeństwa w środowisku pracy.	- dobiera bezpieczne hasła zgodnie z zasadami bezpieczeństwa - wskazuje poprawne sposoby przechowywania i udostępniania danych - rozróżnia bezpieczne i niebezpieczne zachowania użytkownika	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Reaguje adekwatnie na potencjalne incydenty bezpieczeństwa.	- wskazuje właściwe działania w przypadku podejrzenia ataku - wybiera poprawne procedury zgłoszenia incydentu - unika działań zwiększających ryzyko (np. otwierania podejrzanych plików)	Obserwacja w warunkach symulowanych
Wdraża podstawowe działania prewencyjne zwiększające bezpieczeństwo.	- stosuje zasady bezpiecznego korzystania ze sprzętu firmowego i prywatnego - wskazuje metody zabezpieczenia stanowiska pracy - dobiera odpowiednie środki ochrony (np. aktualizacje, uwierzytelnianie)	Obserwacja w warunkach symulowanych
Jest świadomy zagrożeń związanych z cyberprzestępczością i ich wpływu na organizację.	- uzasadnia znaczenie przestrzegania zasad bezpieczeństwa - wskazuje konsekwencje nieodpowiedzialnych działań użytkownika	Obserwacja w warunkach symulowanych
Odpowiedzialnie stosuje zasady cyberbezpieczeństwa w pracy i życiu codziennym.	- deklaruje stosowanie dobrych praktyk bezpieczeństwa - wykazuje ostrożność w udostępnianiu danych	Obserwacja w warunkach symulowanych
Współpracuje w zakresie zapewnienia bezpieczeństwa informacji w organizacji.	- stosuje się do procedur obowiązujących w organizacji - komunikuje zagrożenia i incydenty odpowiednim osobom	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1) Podstawy cyberprzestępczości i zagrożeń w sieci :

1. Wprowadzenie do cyberprzestępczości – podstawy cyberbezpieczeństwa
2. Czy cyberprzestępcy naprawdę nam zagrażają?
3. Czy jestem atrakcyjnym klientem dla cyberprzestępcy?
4. Korzyści dla cyberprzestępców – co zyskują atakując twoje dane?
5. Czy cyberprzestępca jest zawsze anonimowy?

2) Cyberprzestępcy i nowoczesne formy ataków :

1. Zorganizowane grupy cyberprzestępcze – jak działają i dlaczego są groźne
2. Sieci botnet – jak cyberprzestępcy przejmują komputery
3. AI w rękach cyberprzestępców
4. Ataki DoS/DDoS – zagrożenia dla instytucji
5. Ataki 0-day – czy istnieje sposób obrony przed nimi?

3) Najczęstsze techniki ataków na użytkowników :

1. Rodzaje ataków na pracowników biurowych
2. Spam jako niegroźny sposób na groźne ataki
3. Phishing jako metoda okradania naszych kont bankowych
4. Ataki socjotechniczne, czyli niewinne wyłudzanie danych
5. Opłacona faktura jako sposób przemycenia wirusa do naszego systemu

4) Skutki cyberataków i kradzież danych :

1. Skutki udanego cyberataku
2. Kradzież tożsamości – co? jak? kiedy? gdzie?
3. Bezpieczeństwo haseł
4. Bezpieczne przekazywanie haseł współpracownikom
5. Znaleziony pendrive jako pozwolenie na atak cyberprzestępcy

5) Ochrona, prewencja i bezpieczeństwo w pracy :

1. Skuteczne metody ochrony przed cyberatakami
2. Zwiększenie odporności na cyberataki – proste i skuteczne metody
3. Fizyczne bezpieczeństwo – jak zabezpieczyć miejsce pracy
4. Sprzęt prywatny vs firmowy – jak zarządzać bezpieczeństwem urządzeń
5. Bezpieczne przekazywanie haseł współpracownikom

6) Walidacja

Razem: 5 h*

***Wartość podana w godzinach dydaktycznych (45 min) bez wliczonych przerw**

Harmonogram

Liczba pozycji harmonogramu: 7

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 7 Podstawy cyberprzestępczości i zagrożeń w sieci	Zbigniew Wlazło	30-06-2026	09:00	09:42	00:42
2 z 7 Cyberprzestępcy i nowoczesne formy ataków	Zbigniew Wlazło	30-06-2026	09:42	10:24	00:42
3 z 7 Najczęstsze techniki ataków na użytkowników	Zbigniew Wlazło	30-06-2026	10:24	11:06	00:42
4 z 7 Przerwa	Zbigniew Wlazło	30-06-2026	11:06	11:21	00:15
5 z 7 Skutki cyberataków i kradzież danych	Zbigniew Wlazło	30-06-2026	11:21	12:03	00:42
6 z 7 Ochrona, prewencja i bezpieczeństwo w pracy	Zbigniew Wlazło	30-06-2026	12:03	12:45	00:42
7 z 7 Walidacja	-	30-06-2026	12:45	13:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	504,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	504,00 PLN
Koszt osobogodziny brutto	126,00 PLN
Koszt osobogodziny netto	126,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Zbigniew Wlazło

Ukończył studia podyplomowe na Wydziale Prawa Uniwersytetu Jagiellońskiego w Krakowie z zakresu bezpieczeństwa informacji w administracji i biznesie. Posiada ponad 10-cio letnie doświadczenie w kierowaniu archiwami (w latach 2017-2020 naczelnik Głównego Archiwum Policji KGP w Warszawie). Przez 7 lat pełnił funkcję pełnomocnika ds. ochrony informacji niejawnych oraz administratora bezpieczeństwa informacji w Szkole Policji w Pile. Od 2020r. prowadzi szkolenia z zakresu ochrony danych osobowych, ochrony informacji niejawnych, postępowania z dokumentacją oraz kursy archiwalne. Autor publikacji poświęconych bezpieczeństwu informacji niejawnych, ochronie danych osobowych i funkcjonowania archiwów wyodrębnionych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzyma skrypt szkoleniowy.

Informacje dodatkowe

Uczestnicy szkolenia otrzymają zaświadczenie z następującą podstawą prawną "Zaświadczenie wydano na podstawie Rozporządzenia Ministra Edukacji Narodowej z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz.U. z 2023, poz. 2175)."

Metodyka prowadzenia zajęć obejmuje wykorzystanie metod aktywizujących, takich jak wykład z elementami dyskusji, analiza przypadków, odgrywanie ról (symulacje sytuacji zawodowych) oraz autorefleksja uczestników. Ponadto uczestnicy będą mieli możliwość dzielenia się własnymi doświadczeniami zawodowymi, aby omawiać je w kontekście omawianych przypadków i zbliżać do rzeczywistych sytuacji w pracy.

Warunki techniczne

Szkolenie zdalne prowadzone przez komunikator Clickmeeting

Clickmeeting działa w aktualnej wersji oraz dwóch wcześniejszych głównych wersjach tych systemów operacyjnych:

Apple macOS,

Microsoft Windows,

Chrome OS,

Ubuntu i inne dystrybucje Linuksa oparte na Debianie.

Używanie obsługiwanej przeglądarki internetowej

Clickmeeting działa w aktualnej wersji wymienionych poniżej przeglądarek:

Chrome

Mozilla Firefox

Microsoft Edge

Dodatkowe wymagania sprzętowe i sieciowe

Jeśli chcesz uczestniczyć w spotkaniach wideo na Clickmeeting, potrzebujesz następujących rzeczy:

Szerokopasmowe połączenie z internetem.

Kamera internetowa (wbudowana lub podłączana przez USB).

Kontakt

KATARZYNA GŁOGOWSKA

E-mail k.glogowska@romaniszyn.com.pl
Telefon (+48) 508 117 752