Możliwość dofinansowania

Cyberbezpieczeństwo

Numer usługi 2024/07/29/132349/2240498

9 600,00 PLN brutto
9 600,00 PLN netto
188,24 PLN brutto/h
188,24 PLN netto/h

FUNDACJA INSTYTUT PROJEKT PRZEDSIĘBIORCZOŚĆ

★★★★★

Słupca / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Usługa szkoleniowa
51 h
21.10.2024 do 08.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	Nasza usługa cyberbezpieczeństwa jest przeznaczona dla osób fizycznych, które chcą chronić swoje dane osobowe i prywatność w sieci. Oferujemy kompleksowe rozwiązania obejmujące ochronę przed phishingiem, malware, kradzieżą tożsamości i innymi zagrożeniami cybernetycznymi. Zapewniamy wsparcie techniczne, regularne aktualizacje zabezpieczeń, audyty bezpieczeństwa oraz porady dotyczące bezpiecznego korzystania z internetu. Nasz zespół ekspertów dba o Twoje bezpieczeństwo, abyś mógł spokojnie korzystać z technologii bez obaw o swoje dane. Chroń swoją cyfrową prywatność z naszą pomocą!
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	20-10-2024
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	51
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 edukacyjnym programu cyberbezpieczeństwa jest zwiększenie świadomości i umiejętności w ochronie danych osobowych i bezpiecznym korzystaniu z internetu. Uczestnicy poznają podstawy cyberbezpieczeństwa, nauczą się tworzyć mocne hasła, korzystać z dwuskładnikowego uwierzytelniania, rozpoznawać zagrożenia (phishing, malware) oraz chronić dane na portalach społecznościowych. Program kończy się testem sprawdzającym zdobytą wiedzę i umiejętności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnicy będą wiedzieć, czym jest cyberbezpieczeństwo i dlaczego jest ważne. Będą potrafili zidentyfikować różne rodzaje zagrożeń, takie jak phishing, wirusy i malware.	Testy sprawdzające zrozumienie podstaw cyberbezpieczeństwa oraz rozpoznawania zagrożeń.	Test teoretyczny
Uczestnicy będą rozumieć, czym są dane osobowe i jak je skutecznie chronić.	Zadania praktyczne związane z ochroną danych osobowych oraz testy wiedzy teoretycznej.	Debata swobodna
Uczestnicy nauczą się tworzyć mocne hasła oraz korzystać z dwuskładnikowego uwierzytelniania. Będą potrafili rozpoznawać niebezpieczne e-maile i unikać phishingu.	Zadania praktyczne dotyczące tworzenia haseł i włączania dwuskładnikowego uwierzytelniania oraz symulacje ataków phishingowych.	Obserwacja w warunkach rzeczywistych
Uczestnicy zrozumieją, czym jest antywirus oraz jak go instalować i używać. Będą potrafili konfigurować ustawienia prywatności na portalach społecznościowych.	Symulacje i scenariusze związane z instalacją i konfiguracją oprogramowania antywirusowego oraz przeglądy ustawień prywatności na portalach społecznościowych.	Debata swobodna
Uczestnicy nauczą się włączać tryb prywatny w różnych przeglądarkach oraz zrozumieją jego korzyści.	Zadania praktyczne związane z włączaniem trybu prywatnego w przeglądarkach internetowych.	Wywiad swobodny
Uczestnicy będą wiedzieli, jak budować pozytywny wizerunek w internecie oraz jak dostosować treści do odbiorców. Nauczą się planować, harmonogramować i publikować treści na platformach społecznościowych.	Projekt końcowy związany z budowaniem wizerunku online oraz zarządzaniem treściami, w tym planowanie i publikacja postów na platformach społecznościowych.	Test teoretyczny
Powtórzenie kluczowych zagadnień oraz test końcowy sprawdzający całościowe zrozumienie i umiejętności.	Test końcowy oraz ocena projektów i zadań praktycznych.	Test teoretyczny

Kwalifikacje

Kwalifikacje zarejestrowane w Zintegrowanym Systemie Kwalifikacji

Kwalifikacje	Certyfikat umiejętności komputerowych – poziom podstawowy
Kod kwalifikacji w Zintegrowanym Systemie Kwalifikacji	12622
Nazwa/Kategoria Podmiotu prowadzącego walidację	ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Podmiot prowadzący walidację jest zarejestrowany w BUR	Tak
Nazwa/Kategoria Podmiotu certyfikującego	ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Program

Dzień 1: Wprowadzenie do cyberbezpieczeństwa i podstawowe zasady bezpieczeństwa (8 godzin)

1. Wprowadzenie do cyberbezpieczeństwa
   - Co to jest cyberbezpieczeństwo?
   - Dlaczego jest ważne?
   - Przykłady zagrożeń (phishing, wirusy, malware)
2. Znaczenie ochrony danych osobowych
   - Co to są dane osobowe?
   - Jak je chronić?

Dzień 2: Bezpieczeństwo aktywności w sieci (8 godzin)

1. Tworzenie bezpiecznych haseł
   - Jak stworzyć mocne hasło?
   - Przykłady bezpiecznych i niebezpiecznych haseł
2. Dwuskładnikowe uwierzytelnianie
   - Co to jest?
   - Jak to włączyć?
3. Aktualizacje oprogramowania
   - Dlaczego są ważne?
   - Jak zaktualizować oprogramowanie?
4. Bezpieczne korzystanie z poczty e-mail
   - Jak rozpoznać niebezpieczne e-maile?
   - Co to jest phishing?

Dzień 3: Ochrona przed złośliwym oprogramowaniem i ustawienia prywatności (11 godzin)

1. Ochrona przed złośliwym oprogramowaniem
   - Co to jest antywirus?
   - Jak zainstalować i używać antywirusa?

2. Ustawienia prywatności w serwisach społecznościowych
    - Facebook: Ustawienia prywatności
    - Jak zmienić ustawienia prywatności na Facebooku?
    - Kto może zobaczyć nasze posty?
    - Instagram: Ustawienia prywatności
    - Jak zmienić ustawienia prywatności na Instagramie?

Dzień 4: Ustawienia prywatności i korzystanie z trybu prywatnego w przeglądarkach (8 godzin)

1. Twitter: Ustawienia prywatności
    - Jak zmienić ustawienia prywatności na Twitterze?
    - Jak ukryć swoje tweety?

2. Bezpieczne udostępnianie informacji
    - Co warto udostępniać?
    - Czego unikać w internecie?

3. Tryb prywatny w przeglądarkach
    - Tryb prywatny w przeglądarce Chrome
    - Jak włączyć tryb prywatny?
    - Co daje tryb prywatny?
    - Tryb prywatny w przeglądarce Firefox
    - Jak włączyć tryb prywatny?
    - Co daje tryb prywatny?
    - Tryb prywatny w przeglądarce Edge
    - Jak włączyć tryb prywatny?
    - Co daje tryb prywatny?
    - Tryb prywatny w przeglądarce Safari
    - Jak włączyć tryb prywatny?
    - Co daje tryb prywatny?

Dzień 5: Kształtowanie wizerunku w internecie i rozpoznawanie zagrożeń cyfrowych (8 godzin)

1. Budowanie pozytywnego wizerunku online
    - Co to jest personal branding?
    - Jak budować pozytywny wizerunek?

2. Analiza odbiorców i dostosowanie treści
    - Kim są nasi odbiorcy?
    - Jak dostosować treść do odbiorców?

3. Rodzaje zagrożeń cyfrowych
    - Phishing: co to jest i jak się przed nim chronić?
    - Malware: co to jest i jak się przed nim chronić?

Dzień 6: Zarządzanie treściami, reagowanie na zagrożenia cyfrowe, podsumowanie i test (8 godzin)

1. Strategie reagowania na zagrożenia
    - Co robić w przypadku ataku?
    - Jak zgłaszać incydenty?

2. Zarządzanie treściami w serwisach społecznościowych
    - Planowanie treści
    - Jak planować posty?
    - Jak tworzyć harmonogramy publikacji?
    - Publikowanie treści
    - Jak dodawać posty na Facebooku, Instagramie, Twitterze?
    - Jak używać narzędzi do zarządzania treściami?

3. Podsumowanie i test końcowy
    - Powtórzenie kluczowych zagadnień

Harmonogram

Liczba przedmiotów/zajęć: 19

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 19 Wprowadzenie do cyberbezpieczeństwa i podstawowe zasady bezpieczeństwa	Łukasz Kopczyński	21-10-2024	08:00	11:00	03:00	Tak
2 z 19 Wprowadzenie do cyberbezpieczeństwa i podstawowe zasady bezpieczeństwa	Łukasz Kopczyński	21-10-2024	11:15	14:00	02:45	Tak
3 z 19 Wprowadzenie do cyberbezpieczeństwa i podstawowe zasady bezpieczeństwa	Łukasz Kopczyński	21-10-2024	14:15	16:30	02:15	Tak
4 z 19 Bezpieczeństwo aktywności w sieci	Łukasz Kopczyński	25-10-2024	08:00	11:00	03:00	Nie
5 z 19 Bezpieczeństwo aktywności w sieci	Łukasz Kopczyński	25-10-2024	11:15	14:00	02:45	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
6 z 19 Bezpieczeństwo aktywności w sieci	Łukasz Kopczyński	25-10-2024	14:15	16:30	02:15	Nie
7 z 19 Ochrona przed złośliwym oprogramowaniem i ustawienia prywatności	Zofia Kapczyńska	28-10-2024	08:00	11:00	03:00	Tak
8 z 19 Ochrona przed złośliwym oprogramowaniem i ustawienia prywatności	Zofia Kapczyńska	28-10-2024	11:15	14:00	02:45	Tak
9 z 19 Ochrona przed złośliwym oprogramowaniem i ustawienia prywatności	Zofia Kapczyńska	28-10-2024	14:15	16:30	02:15	Tak
10 z 19 Ochrona przed złośliwym oprogramowaniem i ustawienia prywatności	Zofia Kapczyńska	31-10-2024	09:00	12:00	03:00	Tak
11 z 19 Ustawienia prywatności i korzystanie z trybu prywatnego w przeglądarkach	Łukasz Kopczyński	04-11-2024	08:00	11:00	03:00	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
12 z 19 Ustawienia prywatności i korzystanie z trybu prywatnego w przeglądarkach	Łukasz Kopczyński	04-11-2024	11:15	14:00	02:45	Tak
13 z 19 Ustawienia prywatności i korzystanie z trybu prywatnego w przeglądarkach	Łukasz Kopczyński	04-11-2024	14:15	16:30	02:15	Tak
14 z 19 Kształtowanie wizerunku w internecie i rozpoznawanie zagrożeń cyfrowych	Łukasz Kopczyński	07-11-2024	08:00	11:00	03:00	Tak
15 z 19 Kształtowanie wizerunku w internecie i rozpoznawanie zagrożeń cyfrowych	Łukasz Kopczyński	07-11-2024	11:15	14:00	02:45	Tak
16 z 19 Kształtowanie wizerunku w internecie i rozpoznawanie zagrożeń cyfrowych	Łukasz Kopczyński	07-11-2024	14:15	16:30	02:15	Tak
17 z 19 Zarządzanie treściami, reagowanie na zagrożenia cyfrowe	Łukasz Kopczyński	08-11-2024	08:00	11:00	03:00	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
18 z 19 Zarządzanie treściami, reagowanie na zagrożenia cyfrowe	Łukasz Kopczyński	08-11-2024	11:15	15:15	04:00	Nie
19 z 19 walidacja	-	08-11-2024	15:15	16:15	01:00	Nie

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 600,00 PLN
Koszt przypadający na 1 uczestnika netto	9 600,00 PLN
Koszt osobogodziny brutto	188,24 PLN
Koszt osobogodziny netto	188,24 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

Łukasz Kopczyński

Łukasz Kopczyński to uznany ekspert w dziedzinie cyberbezpieczeństwa z ponad 5 letnim doświadczeniem w branży IT. Specjalizuje się w ochronie infrastruktury IT, zabezpieczeniach sieciowych oraz zarządzaniu ryzykiem cyfrowym. Jego bogata wiedza i praktyczne podejście

sprawiają, że jest cenionym trenerem i doradcą dla wielu firm, które stawiają na bezpieczeństwo w dobie cyfrowej transformacji.
Łukasz od lat prowadzi szkolenia i warsztaty, które pomagają specjalistom IT oraz menedżerom skutecznie chronić swoje organizacje przed zagrożeniami cybernetycznymi. Jego metody nauczania opierają się na rzeczywistych przypadkach i najnowszych trendach w dziedzinie cyberbezpieczeństwa, co zapewnia uczestnikom dostęp do aktualnych i praktycznych informacji. Podczas nadchodzącego szkolenia, Łukasz podzieli się swoimi sprawdzonymi strategiami i narzędziami, które pomogą uczestnikom skutecznie zabezpieczać systemy informatyczne oraz minimalizować ryzyko związane z cyberatakami. Posiada doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat.

2 z 2

Zofia Kapczyńska

Zofia Kapczyńska to doświadczona specjalistka w zakresie cyberbezpieczeństwa, z bogatym doświadczeniem w tworzeniu strategii ochrony danych i edukacji w obszarze bezpieczeństwa cyfrowego. Jej pasją jest ochrona prywatności i bezpieczeństwa w świecie online, co przekłada się na wieloletnie zaangażowanie w szkolenia oraz doradztwo w tej dziedzinie.

Od 5 lat Zofia współpracuje z firmami, instytucjami oraz indywidualnymi użytkownikami, pomagając im zrozumieć zagrożenia w cyberprzestrzeni oraz jak skutecznie im przeciwdziałać. Specjalizuje się w tematyce ochrony danych osobowych, zarządzania ryzykiem oraz bezpiecznego korzystania z technologii w życiu codziennym i zawodowym.
W swoich szkoleniach Zofia Kapczyńska kładzie nacisk na praktyczne podejście do cyberbezpieczeństwa, dostosowując treści do potrzeb różnych grup odbiorców. Jej celem jest budowanie świadomości oraz wdrażanie skutecznych rozwiązań, które minimalizują ryzyko i zwiększają poziom ochrony cyfrowej, zarówno w kontekście osobistym, jak i biznesowym.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Niezbędne materiały zostaną udostępnione uczestnikom podczas szkolenia.

Informacje dodatkowe

Harmonogram jest zaplanowany w godzinach zegarowych, przerwy zostały przewidziane pomiędzy modułami szkoleniowymi jednak nie są wliczone w czas usługi.

Harmonogram może ulec zmianie.

Warunki techniczne

1. Komputer lub urządzenie mobilne – w przypadku urządzenia mobilnego można pobrać odpowiednią aplikację „Google Meet” ze sklepu Google Play lub AppStore.

2. Szerokopasmowe połączenie z internetem.

3. Wymagania sprzętowe - procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy), 2GB pamięci RAM (zalecane 4GB lub więcej).

4. Mikrofon zewnętrzny lub mikrofon wbudowany w urządzeniu oraz głośniki zewnętrzne lub wbudowane w urządzeniu.

5.Kamera zewnętrzna lub wbudowana w urządzeniu.

Adres

ul. Stefana Batorego 1
62-400 Słupca
woj. wielkopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Weronika Montowska-Brzostowska

E-mail weronika.montowska-brzostowska@gmail.com.pl
Telefon (+48) 506 388 003