



Centrum Wsparcia
Biznesu INCOM
Piotr Jasiek



Bezpieczeństwo w sieci i urządzeń mobilnych dla każdego - szkolenie

Numer usługi 2025/04/25/12833/2709835

📍 Itawa / stacjonarna

🏠 Usługa szkoleniowa

🕒 35 h

📅 13.05.2025 do 16.05.2025

5 450,00 PLN brutto

5 450,00 PLN netto

155,71 PLN brutto/h

155,71 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	Szkolenie skierowane jest do dorosłych mieszkańców województwa warmińsko-mazurskiego, korzystających ze wsparcia z własnej inicjatywy, z wyłączeniem osób fizycznych prowadzących działalność gospodarczą. W zajęciach udział mogą wziąć osoby, które korzystają lub chcą w bezpieczny sposób korzystać z Internetu, które chcą się dowiedzieć, jak uniknąć wyłudzenia danych, jak w sposób bezpieczny korzystać z aplikacji i konta mObywatel, bezpiecznego korzystania z telefonu komórkowego. Nie są wymagane szczególne wytyczne odnośnie uczestnika szkolenia.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	11-05-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	35
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

Przygotowanie uczestnika do bezpiecznego korzystania z Internetu, telefonu i funkcjonalności związanych z mObywatel.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Odpowiednio postępuje w przypadku wycieku swoich danych	Określa zasady postępowania w przypadku wycieku swoich danych	Wywiad swobodny
Rozpoznaje techniki socjotechniki stosowane przez oszustów	Charakteryzuje techniki socjotechniki stosowane przez oszustów	Wywiad swobodny
Rozpoznaje i broni się przed phishingiem	Charakteryzuje sposoby rozpoznania i ochrony przed phisingiem	Wywiad swobodny
Rozpoznaje i broni się przed Smishingiem	Charakteryzuje sposoby rozpoznania i ochrony przed Smishingiem	Wywiad swobodny
Stosuje politykę bezpieczeństwa w zakresie haseł	Wykorzystuje wiedzę w zakresie zarządzania hasłami	Obserwacja w warunkach symulowanych
Rozpoznaje Spoofing	Definiuje cechy Spoofingu	Wywiad swobodny
W bezpieczny sposób używa portale społecznościowe	Określa procedury i metody postępowania w przypadku wycieku danych i włamania się do konta	Wywiad swobodny
	Określa sposoby działania w przypadku zajęcia konta przez innego użytkownika.	Wywiad swobodny
W bezpieczny sposób korzysta z bankowości elektronicznej	Stosuje odpowiednią politykę haseł	Obserwacja w warunkach symulowanych
	Stosuje zasady uwierzytelniania dwuskładnikowego	Obserwacja w warunkach symulowanych
	Określa bezpieczne metody przechowywania haseł	Wywiad swobodny
W bezpieczny sposób używa funkcjonalności mObywatel	Stosuje politykę bezpieczeństwa w Internecie w aspekcie użytkowania mObywatel	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK, na dokumencie są zawarte efekty uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK, na dokumencie zawarto informację o formie i wyniku walidacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK, na dokumencie wpisano informację o rozdzieleniu procesu kształcenia i uczenia się od walidacji.

Program

Szkolenie skierowane jest do dorosłych mieszkańców województwa warmińsko-mazurskiego, korzystających ze wsparcia z własnej inicjatywy, z wyłączeniem osób fizycznych prowadzących działalność gospodarczą. W zajęciach udział mogą wziąć osoby, które korzystają lub chcą w bezpieczny sposób korzystać z Internetu, które chcą się dowiedzieć, jak uniknąć wyłudzenia danych, jak w sposób bezpieczny korzystać z aplikacji i konta mObywatel, bezpiecznego korzystania z telefonu komórkowego. Nie są wymagane szczególne wytyczne odnośnie uczestnika szkolenia.

1. Wprowadzenie do bezpieczeństwa w sieci i telefonach
2. Oszustwa telefoniczne i internetowe
 1. Jak rozpoznać fałszywe bramki płatności
 2. Co zrobić kiedy Twoje dane wyciekły
 3. Dezinformacja
3. Socjotechnika a oszustwa online
4. Czym jest phishing i jak się przed nim bronić?
 1. Definicja i odmiany *phishing'u*
 2. Załączniki w e-mailowych kampaniach *phishing'owych*
 3. Jak rozpoznać *phishing*
 4. Jak chronić się przed *phishingiem*
5. Smishing - jak się chronić przed fałszywymi SMSami?
6. Bezpieczne hasła i zarządzanie nimi,
 1. jak tworzyć dobre hasła
 2. czym jest uwierzytelnianie dwuskładnikowe
 3. metody przechowywania haseł
7. Nieoczekiwany telefon z banku lub policji? Zachowaj czujność, to może być oszustwo!
8. Spoofing czyli podszywanie się pod inny numer telefonu. Jak się bronić?
9. Strony www
 1. Co to jest domena, subdomena
 2. Czym są ataki z wykorzystaniem Typosquatting
 3. Jak sprawdzić wiarygodność linku
10. Bezpieczne korzystanie z portali społecznościowych
 1. Jakie dane publikujemy w portalach społecznościowych i czym mogą one grozić
 2. Co robić, gdy nasze konto zostało przejęte
 3. Jak zadbać o bezpieczeństwo naszych portali

11. Oszustwa romantyczne
12. Jak podnieść bezpieczeństwo urządzenia mobilnego
 1. Jak ochronić dane jeżeli straciliśmy smartphone
13. Bezpieczna bankowość elektroniczna –
14. Jak tworzyć dobre hasła
15. Czym jest uwierzytelnianie dwuskładnikowe (2FA)
16. Metody przechowywania haseł
17. Bezpieczne zakupy
18. Bezpieczne używanie mObywatel
19. Bezpieczeństwo używania komunikatorów

Na Zajęcia mają charakter warsztatów, z wykorzystaniem smartfona i komputerów, osoby są dzielone w grupy 2 lub 4 osobowe, tempo pracy dostosowane jest do możliwości poznawczych uczestników. Miejsce realizacji szkolenia dostosowane dla osób niepełnosprawnych. Usługa realizowana w godzinach dydaktycznych 1h =45 min, w trakcie szkolenia przewidziano przerwy, podczas których możliwe będą konsultacje. Trenerzy mogą prowadzić zajęcia naprzemiennie. Na zakończenie szkolenia zostanie przeprowadzona walidacja w formie zadań wykonywanych przez uczestników, na komputerze/telefonie i pod okiem Walidatora, który będzie połączony on-line z uczestnikami i jednocześnie zweryfikuje umiejętności obsługi aplikacji do komunikacji. **Walidacja realizowana jest w formie obserwacji podczas wykonywania przez uczestników warsztatów, dodatkowo przeprowadzona jest z uczestnikami rozmowa. Na koniec zajęć przeprowadzona są dodatkowe rozmowy/wywiad oraz warsztat, celem utrwalenia wiedzy i umiejętności. Ze względu na brak możliwości wpisania walidacji w momencie odbywania zajęć praktycznych uczestników wpisano czas walidacji na koniec szkolenia.**

Harmonogram

Liczba przedmiotów/zajęć: 26

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 Wprowadzenie do bezpieczeństwa w sieci, Oszustwa telefoniczne i internetowe	Monika Bohatyrewicz	13-05-2025	08:45	09:30	00:45
2 z 26 Socjotechnika a oszustwa online	Monika Bohatyrewicz	13-05-2025	09:30	10:30	01:00
3 z 26 Czym jest phishing i jak się przed nim bronić	Monika Bohatyrewicz	13-05-2025	10:30	12:00	01:30
4 z 26 Przerwa	Monika Bohatyrewicz	13-05-2025	12:00	12:15	00:15
5 z 26 Czym jest phishing i jak się przed nim bronić	Monika Bohatyrewicz	13-05-2025	12:15	13:15	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 26 Smishing - jak się chronić przed fałszywymi SMSami	Monika Bohatyrewicz	13-05-2025	13:15	14:15	01:00
7 z 26 Przerwa	Monika Bohatyrewicz	13-05-2025	14:15	14:30	00:15
8 z 26 Bezpieczne hasła i zarządzanie nimi,	Monika Bohatyrewicz	13-05-2025	14:30	15:30	01:00
9 z 26 Warsztaty - tworzenie haseł i zarządzanie nimi	Monika Bohatyrewicz	14-05-2025	08:15	10:30	02:15
10 z 26 Nieoczekiwany telefon z banku lub policji?	Monika Bohatyrewicz	14-05-2025	10:30	12:00	01:30
11 z 26 Przerwa i indywidualne konsultacje	Monika Bohatyrewicz	14-05-2025	12:00	12:15	00:15
12 z 26 Spoofing czyli podszywanie się pod inny numer telefonu. Jak się bronić?	Monika Bohatyrewicz	14-05-2025	12:15	14:15	02:00
13 z 26 Przerwa	Monika Bohatyrewicz	14-05-2025	14:15	14:30	00:15
14 z 26 Strony www	Monika Bohatyrewicz	14-05-2025	14:30	15:30	01:00
15 z 26 Bezpieczne korzystanie z portali społecznościowych	Monika Bohatyrewicz	15-05-2025	08:15	11:15	03:00
16 z 26 Przerwa	Monika Bohatyrewicz	15-05-2025	11:15	11:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 26 Bezpieczne korzystanie z portali społecznościowych - warsztaty	Monika Bohatyrewicz	15-05-2025	11:30	12:30	01:00
18 z 26 Bezpieczne używanie mObywatel-warsztat	Monika Bohatyrewicz	15-05-2025	12:30	13:30	01:00
19 z 26 Przerwa	Monika Bohatyrewicz	15-05-2025	13:30	13:45	00:15
20 z 26 Oszustwa romantyczne	Monika Bohatyrewicz	15-05-2025	13:45	14:45	01:00
21 z 26 Przerwa	Monika Bohatyrewicz	16-05-2025	08:15	11:15	03:00
22 z 26 jak podnieść bezpieczeństwo urządzenia mobilnego - warsztat	Monika Bohatyrewicz	16-05-2025	11:15	11:30	00:15
23 z 26 Bezpieczna bankowość elektroniczna i Bezpieczne zakupy- warsztat	Monika Bohatyrewicz	16-05-2025	11:30	12:30	01:00
24 z 26 Bezpieczeństwo używania komunikatorów i rządzeń mobilnych - warsztat	Monika Bohatyrewicz	16-05-2025	12:30	13:30	01:00
25 z 26 Przerwa	Monika Bohatyrewicz	16-05-2025	13:30	13:45	00:15
26 z 26 Walidacja	-	16-05-2025	13:45	14:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 450,00 PLN
Koszt przypadający na 1 uczestnika netto	5 450,00 PLN
Koszt osobogodziny brutto	155,71 PLN
Koszt osobogodziny netto	155,71 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Monika Bohatyrewicz

Wykształcenie wyższe w tym Uniwersytet SWPS

Licencjat (Lic.) Bezpieczeństwo wewnętrzne,

Specjalistka mediów społecznościowych i Bezpieczeństwa Online | Trenerka Kompetencji Cyfrowych | Wspieram firmy i osoby indywidualne w efektywnym i bezpiecznym działaniu w Internecie.

Właściciel firmy

Socjalsfera prowadzi działalność związaną z IT i bezpieczeństwem

lis 2017 – obecnie 7 lat 6 miesięcy

◆ Tworzenie i realizacja kompleksowych strategii marketingowych – dostosowanych do indywidualnych potrzeb klientów, ze szczególnym naciskiem na bezpieczeństwo w sieci.

◆ Prowadzenie szkoleń i warsztatów – z zakresu marketingu online, zarządzania mediami społecznościowymi oraz cyberbezpieczeństwa dla firm, instytucji i osób indywidualnych, w tym seniorów.

◆ Konsultacje i mentoring – wspierające rozwój umiejętności w efektywnym i bezpiecznym korzystaniu z platform społecznościowych.

◆ Działania promocyjne i budowanie marki online – poprzez strategiczne kampanie i zarządzanie treściami na platformach takich jak Facebook, Instagram, TikTok.

Posiada doświadczenie w zakresie bezpieczeństwa sieci, finansowego pracowała w PKO BP w Departamencie Bezpieczeństwa

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypt szkoleniowy wydrukowany oraz przekazany w wersji elektronicznej,

Warunki uczestnictwa

Warunkiem skorzystania z usługi z dofinansowaniem jest bezpośredni zapis na usługę za pośrednictwem Bazy Usług Rozwojowych oraz wypełnienie ankiety oceniającej usługę rozwojową zamieszczoną w BUR.

Informacje dodatkowe

W cenę usługi nie są wliczone koszty noclegu i wyżywienia.

Karta usługi zawiera stawkę VAT zw na podstawie §3. 1pkt 14 rozporządzenia Ministra Finansów z 20 grudnia 2013 roku w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. 2015, poz. 736, z późn. zm.) w związku z tym ta karta dotyczy podmiotów które mają dofinansowanie na poziomie pow. 70%. W innym przypadku do podanej ceny doliczymy VAT 23%

Adres

ul. 1 Maja 6c
14-200 Iława
woj. warmińsko-mazurskie

Szkolenie odbędzie się w siedzibie Stowarzyszenia na rzecz osób niepełnosprawnych PROMYK

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe
- Dostosowane do osób niepełnosprawnych

Kontakt



Piotr Jasiek

E-mail biuro@cwbi-incom.eu

Telefon (+48) 694 265 200