Możliwość dofinansowania

Cyberbezpieczeństwo BASIC: kompetencje, socjotechnika, świadomość zagrożeń, skuteczna obrona przed cyber-zagrożeniami.

Numer usługi 2026/06/26/204299/3652265

599,00 PLN brutto
599,00 PLN netto
92,15 PLN brutto/h
92,15 PLN netto/h
261,33 PLN cena rynkowa

LT MASTERY SZKOLENIA DLA BIZNESU PIOTR SZYMCZYK

4,5 / 5

5 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
06:30 h
31.07.2026 do 31.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, FELB.06.03-IZ.00-0003/24 ZIPH, FELB.06.08-IZ.00-0017/25, FELB.06.08-IZ.00-0083/24, FELB.06.08-IZ.00-0014/25
Grupa docelowa usługi	Szkolenie "Wprowadzenie do Cyberbezpieczeństwa-BASIC" skierowane jest do osób prywatnych, przedsiębiorców, kadry wszystkich szczebli Małych i Średnich Przedsiębiorstw oraz ich pracowników: administracyjnych, biurowych, działów sprzedaży i obsługi klienta oraz pracowników mających do czynienia z infrastrukturą IT narażoną na cyberataki. Stworzone jest w taki sposób aby do udziału w nim wystarczał podstawowy poziom wiedzy z zakresu IT; osoby bez wcześniejszego doświadczenia w cyberbezpieczeństwie zbudują solidny fundament pod dalszą eksplorację wiedzy w tym obszarze.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	28-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Cel szkolenia to przygotowanie, podniesienie oraz rozwinięcie świadomości cyfrowej pracowników oraz nabycie podstawowej wiedzy i praktycznych umiejętności w zakresie samodzielnej identyfikacji zagrożeń cyfrowych, indywidualne stosowania zasad bezpiecznej pracy z danymi w środowisku biurowym i zdalnym, niezależne zapewnienia bezpieczeństwa infrastruktury IT zgodnie z aktualnymi trendami zagrożeń w 2026 roku, cyberhigiena, rozpoznawanie / klasyfikacji zagrożeń, obrona przed socjo-technikami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Definiuje kluczowe zagrożenia (phishing, ransomware) oraz rozumie zasady ochrony tożsamości cyfrowej i rolę aktualizacji systemowych.	Uczestnik poprawnie wskazuje definicje co najmniej 3 rodzajów cyberzagrożeń (phishing, ransomware, socjotechnika) oraz wymienia 3 kluczowe korzyści wynikające z regularnych aktualizacji systemowych.	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Samodzielnie identyfikuje próby manipulacji (socjotechnika) oraz dobiera odpowiednie metody zabezpieczeń dla kont i urządzeń mobilnych.	Uczestnik na podstawie przedstawionych w teście przykładów (opisy) poprawnie odróżnia autentyczną wiadomość od próby phishingu oraz wskazuje prawidłowe parametry silnego hasła i konfiguracji 2FA/MFA.	Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Prezentuje postawę odpowiedzialności za bezpieczeństwo informacji i zna zasady etycznego oraz sprawnego reagowania na incydenty.	Uczestnik poprawnie wybiera z listy scenariuszy ścieżkę postępowania w przypadku wystąpienia incydentu oraz wskazuje właściwe organy/osoby wewnątrz organizacji, do których należy niezwłocznie zgłosić zagrożenie.	Test teoretyczny z wynikiem generowanym automatycznie

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

PROGRAM SZKOLENIA:

Wprowadzenie do cyberbezpieczeństwa BASIC

Część teoretyczna zawierająca zadania oraz ćwiczenia praktyczne:

1. Czym jest cyberbezpieczeństwo i dlaczego dotyczy każdego.

- Najczęstsze zagrożenia w codziennej pracy (phishing, ransomware, oszustwa online).
- Przykłady realnych ataków na polskie firmy.

2. Identyfikacja zagrożeń i socjotechnika

- Jak rozpoznać fałszywy e-mail, wiadomość lub link.
- Ćwiczenia: „Prawdziwy czy fałszywy?" – analiza przykładowych wiadomości.

3. Ochrona danych i haseł

- Zasady tworzenia bezpiecznych haseł i korzystania z 2FA/MFA.
- Bezpieczne przechowywanie danych i unikanie wycieków.

4. Bezpieczna praca zdalna i urządzenia mobilne

- Jak bezpiecznie pracować poza biurem.
- Ryzyka sieci publicznych i prywatnych urządzeń.

5. Ochrona urządzeń i aktualizacje

- Znaczenie regularnych aktualizacji.
- Jak chronić komputer, telefon, tablet przed złośliwym oprogramowaniem.

6. Reagowanie na incydenty

- Co zrobić, gdy coś pójdzie nie tak – krok po kroku.
- Kiedy i komu zgłosić incydent.

7. Podsumowanie i dobre praktyki

- 12 zasad bezpiecznego pracownika.
- Podsumowanie szkolenia oraz zdobytej wiedzy

8. Egzamin wewnętrzny oraz certyfikat uczestnictwa.

- Egzamin wewnętrzny z wiedzy zdobytej w czasie szkolenia (w pełni zdalny przy użyciu google forms)
- Certyfikat uczestnictwa (wersja elektroniczna - pdf)

Całkowity czas trwania szkolenia : 6:30 (5 godzin zegarowych przekazywania wiedzy + egzamin 30 + przerwy 60 min)

Czas szkolenia 5 godzin

Czas egzaminu / walidacji wiedzy: 30 min

Czas przerw: 60 minut (15 min + 30 min +15 min)

· Egzamin wewnętrzny / walidacja (30 min) jest wliczona w czas trwania szkolenia.

· Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba pozycji harmonogramu: 14

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Czym jest cyberbezpieczeństwo i dlaczego dotyczy każdego	Zajęcia	Piotr Szymczyk	31-07-2026	09:00	09:30	00:30
2 z 14 Najczęstsze zagrożenia w codziennej pracy	Zajęcia	Piotr Szymczyk	31-07-2026	09:30	10:15	00:45
3 z 14 Przykłady realnych ataków na polskie firmy	Zajęcia	Piotr Szymczyk	31-07-2026	10:15	10:30	00:15
4 z 14 -	Przerwa	-	31-07-2026	10:30	10:45	00:15
5 z 14 Identyfikacja zagrożeń i socjotechnika + ćwiczenie	Zajęcia	Piotr Szymczyk	31-07-2026	10:45	11:15	00:30
6 z 14 Ochrona danych i haseł	Zajęcia	Piotr Szymczyk	31-07-2026	11:15	11:45	00:30
7 z 14 Bezpieczna praca zdalna i urządzenia mobilne	Zajęcia	Piotr Szymczyk	31-07-2026	11:45	12:15	00:30
8 z 14 -	Przerwa	-	31-07-2026	12:15	12:45	00:30
9 z 14 Ochrona urządzeń i aktualizacje	Zajęcia	Piotr Szymczyk	31-07-2026	12:45	13:15	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 14 Reagowanie na incydenty	Zajęcia	Piotr Szymczyk	31-07-2026	13:15	13:45	00:30
11 z 14 Dobre praktyki - Cyberhigiena	Zajęcia	Piotr Szymczyk	31-07-2026	13:45	14:15	00:30
12 z 14 -	Przerwa	-	31-07-2026	14:15	14:30	00:15
13 z 14 Podsumowanie zdobytej wiedzy- 12 zasad bezpieczeństwa	Zajęcia	Piotr Szymczyk	31-07-2026	14:30	15:00	00:30
14 z 14 -	Walidacja	Piotr Szymczyk	31-07-2026	15:00	15:30	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	06:30
w tym suma godzin zajęć	05:00
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	07:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	599,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
Koszt przypadający na 1 uczestnika netto	599,00 PLN

Koszt osobogodziny brutto	92,15 PLN
Koszt osobogodziny netto	92,15 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	06:30

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Szymczyk

Piotr Szymczyk to doświadczony menedżer techniczny oraz ekspert w obszarze cyberbezpieczeństwa i usług IT, z ponad 25-letnią praktyką zdobywaną w międzynarodowych korporacjach technologicznych. Specjalizuje się w nadzorze nad usługami bezpieczeństwa, procesami dostępowymi, cyklem wdrażania, prowadzeniem przeglądów operacyjnych i bezpieczeństwa integrując w/g UoKSC (NIS2), SZBI, ISO27k, CRA. Jako lider zespołów technicznych zarządzał wielokulturowymi grupami specjalistów IT, realizując projekty, inicjatywy podnoszące poziom bezpieczeństwa oraz działania zapewniające ciągłość operacyjną.

W globalnym centrum usług biznesowych odpowiadał za procesy IT, Cybersec, operacyjno-finansowe, kontrolę SLA/KPI oraz komunikację z klientami na poziomie międzynarodowym. Doświadczenie korporacyjne uzupełnia praktyka przedsiębiorcza zdobyta podczas prowadzenia własnej działalności w USA, gdzie zarządzał pełnym zakresem operacji, finansów i relacji biznesowych.

Piotr posiada doświadczenie oraz liczne szkolenia/certyfikaty międzynarodowe nie starsze niż 5 lat z zakresu IT: EITCA/IS Academy of Information Security, EITCA/KC Academy of Key IT Competencies. Z obszaru usług projektowych: Agile PM Practitioner, Change Management, AI w Projektach oraz Security: Audytor ISO 27k, CompTIA Security+. Obecnie wykorzystuje swoje doświadczenie jako trener, prowadząc szkolenia z cyberbezpieczeństwa, higieny cyfrowej, odporności organizacyjnej oraz konsultant w zakresie NIS2 / UoKSC / SZBI /CRA / usług IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały szkoleniowe przygotowane przez Trenera wysłane na adres e-mail -- konspekt wiedzy przekazywanej / poruszanej w czasie szkolenia w formacie pdf, szablony materiałów do ćwiczeń, certyfikat udziału w szkoleniu.

Warunki uczestnictwa

Udział w szkoleniu z dofinansowaniem jest możliwy po spełnieniu następujących warunków:

- Konieczna jest rejestracja oraz utworzenie profilu użytkownika w Bazie Usług Rozwojowych (BUR).
- Zgłoszenie chęci udziału musi nastąpić poprzez system BUR.
- Uczestnik musi spełnić wszystkie kryteria formalne ustalone przez instytucję przyznającą dofinansowanie (Operatora).

Ważna informacja:

Zalecamy kontakt z nami w celu weryfikacji dostępności miejsc oraz potwierdzenia daty szkolenia, zanim podpiszą Państwo umowę o dofinansowanie z Operatorem. Informujemy również, że podmiot realizujący usługę musi być przygotowany na audyt lub wizytację (online lub stacjonarną) ze strony Polskiej Agencji Rozwoju Przedsiębiorczości (PARP), Operatora lub uprawnionej jednostki kontrolnej.

Informacje dodatkowe

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług orazszczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

W przypadku korzystania z dofinansowania do szkolenia obowiązuje wymóg uczestnictwa w co najmniej 80% zajęć. Weryfikacja frekwencji na podstawie: raportu logowań lub listy obecności lub zrzutu ekranu wykonanego na początku i końcu szkolenia.

Całe szkolenie jest rejestrowane w celach kontroli oraz audytu.

Wykorzystanie nagrania w innym celu niż kontrola czy audyt wymaga zgody trenera oraz uczestników.

Uczestnicy otrzymają zaświadczenie / certyfikat, potwierdzające ukończenie szkolenia.

Usługa zdalna w czasie rzeczywistym - prowadzona na żywo.

Warunki techniczne

Poniżej opisane są minimalne wymagania techniczne dotyczące uczestnictwa w szkoleniu przy pomocy platformy TEAMS:

1. Parametry urządzenia: komputer / laptop / tablet

- Procesor dwurdzeniowy 1–2 GHz minimalnie; zalecany dual-core 2 GHz lub lepszy (Intel i3/i5 lub równoważny)
- 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 10/11, macOS 10.13+ (lub nowsze), Linux (nowsze dystrybucje wspierane), iOS 13+/Android 8+
    - zainstalowany TEAMS (najświeższa wersja) oraz najnowsza wersja Chrome/Edge/Firefox;

1. Kamera i mikrofon

- TEAMS współpracuje z wbudowanymi kamerami w laptopach oraz większością kamer internetowych.
    - słuchawki z mikrofonem zalecane dla lepszej jakości dźwięku.
    - zaawansowane lub profesjonalne kamery/mikrofony, mogą wymagać zainstalowanie dodatkowego oprogramowania .

1. Urządzenia mobilne

- Jeżeli łączysz się z urządzenia mobilnego, pobierz i zainstaluj aplikację TEAMS z App Store (Apple) lub Google Play
- Aby korzystać z dźwięku i obrazu, użyj zestawu słuchawkowego z mikrofonem lub głośników podłączonych do urządzenia.
- Przed rozpoczęciem szkolenia sprawdź, czy urządzenie rozpoznaje wybrane urządzenie audio oraz czy nie jest ono jednocześnie zajęte przez inną aplikację
- Upewnij się, że aplikacja ma przyznane uprawnienia do korzystania z mikrofonu i kamery.

1. Wymagania dla łącza internetowego:

- *min. 1,5 Mbps download i upload* dla podstawowego udziału
- zalecane 3 Mbps+ dla stabilnego wideo HD i udostępniania ekranu
- najnowsza wersja używanej przeglądarki internetowej

1. Link do szkolenia oraz warunki / wymagania dodatkowe:
    - Link do szkolenia zostanie dosłany drogą elektroniczną przed rozpoczęciem usługi na adres email podany przez uczestnika szkolenia.

- Link do szkolenia będzie ważny w dniach i godzinach określonych w harmonogramie usługi.

1. Podczas szkolenia online zapewniamy:
    - Wygodną formę szkolenia, gdzie wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki.

- Szkolenie zdalne w czasie rzeczywistym w wirtualnym pokoju konferencyjnym, w niewielkiej grupie uczestników.
- Możliwość pełnej interakcji z trenerem, który prowadzi zajęcia "na żywo" z włączoną kamerą w czasie trwania całego szkolenia.
- Możliwości zadawania pytań, omawiania indywidulanych zagadnień oraz aktywny udział w ćwiczeniach.

Przed szkoleniem:

- Upewnij się, że masz stabilne połączenie internetowe, które spełnia minimalne wymagane prędkości dla transmisji audio oraz wideo.
- Przetestuj dostęp i uruchomienie aplikacji TEAMS w wykorzystaniem kamery oraz mikrofonu.
- Rekomenduje się przygotowanie zapasowego zestawu awaryjnego sprzętu w celu zapewnienia ciągłości realizacji szkolenia. Powinien on obejmować kluczowe komponenty: komputer, kamerę, mikrofon/głośnik, klawiaturę, myszkę oraz alternatywne źródło dostępu do Internetu (np. modem Hot-Spot).

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Kontakt

Piotr Szymczyk

E-mail piotr.szymczyk@legacyturn.com

Telefon (+48) 600 390 516