



Mateusz Ellwardt
Business

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo dla osób zagrożonych wykluczeniem cyfrowym.

Numer usługi 2026/07/08/135879/3677624

4 800,00 PLN brutto

4 800,00 PLN netto

150,00 PLN brutto/h

150,00 PLN netto/h

261,33 PLN cena rynkowa ⓘ

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe z praktyką indywidualną
- 🕒 32:00 h
- 📅 07.12.2026 do 15.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Grupę docelową szkolenia stanowią osoby zagrożone wykluczeniem cyfrowym, w szczególności seniorzy, którzy chcą zwiększyć swoje kompetencje w zakresie bezpieczeństwa korzystania z technologii cyfrowych i internetu. Szkolenie skierowane jest do osób posiadających niewielkie lub podstawowe umiejętności cyfrowe, chcących nauczyć się rozpoznawania zagrożeń w sieci oraz skutecznej ochrony swoich danych i urządzeń.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	01-12-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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 szkolenia jest rozwinięcie wiedzy i umiejętności uczestników w zakresie bezpiecznego korzystania z internetu oraz nowoczesnych technologii cyfrowych. Po zakończeniu szkolenia uczestnik samodzielnie rozpozna najczęstsze zagrożenia w cyberprzestrzeni. Będzie bezpiecznie korzystać z poczty elektronicznej

, bankowości internetowej i mediów społecznościowych. Będzie tworzyć i zarządzać silnymi hasłami, chronić swoje dane osobowe oraz odpowiednio reagować na próby oszustw.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpoznaje najczęściej występujące zagrożenia cyberbezpieczeństwa oraz potrafi odpowiednio na nie reagować.	Uczestnik prawidłowo identyfikuje co najmniej 80% przedstawionych przykładów zagrożeń oraz wskazuje właściwy sposób postępowania w przypadku ich wystąpienia.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik bezpiecznie korzysta z internetu, poczty elektronicznej, komunikatorów i mediów społecznościowych.	Uczestnik wskazuje zasady bezpiecznego korzystania z narzędzi cyfrowych i poprawnie stosuje je podczas wykonywania ćwiczeń praktycznych.	Obserwacja w warunkach symulowanych
Uczestnik chroni swoje dane osobowe i prywatność podczas korzystania z usług cyfrowych.	Uczestnik rozpoznaje dane wrażliwe, wskazuje sytuacje wymagające ich ochrony oraz poprawnie dobiera działania zapobiegające ich ujawnieniu.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady tworzenia i zarządzania bezpiecznymi hasłami oraz dodatkowymi metodami zabezpieczania kont.	Uczestnik tworzy hasło spełniające wymagania bezpieczeństwa oraz potrafi wskazać korzyści wynikające ze stosowania uwierzytelniania dwuskładowego.	Obserwacja w warunkach symulowanych
Uczestnik potrafi identyfikować próby oszustw internetowych, wyłudzeń danych i dezinformacji.	Uczestnik poprawnie ocenia autentyczność przykładowych wiadomości, stron internetowych lub komunikatów oraz wskazuje cechy charakterystyczne oszustwa.	Obserwacja w warunkach symulowanych
Uczestnik bezpiecznie korzysta z bankowości elektronicznej, e-usług publicznych oraz zakupów online.	Uczestnik wskazuje zasady bezpiecznego korzystania z usług finansowych i publicznych online oraz prawidłowo wykonuje zadania symulacyjne związane z korzystaniem z tych usług.	Obserwacja w warunkach symulowanych
Uczestnik samodzielnie konfiguruje podstawowe ustawienia bezpieczeństwa na urządzeniach cyfrowych.	Uczestnik potrafi włączyć podstawowe zabezpieczenia urządzenia (np. blokadę ekranu, aktualizacje, ustawienia prywatności) zgodnie z instrukcją lub scenariuszem zadaniowym.	Obserwacja w warunkach symulowanych
Uczestnik świadomie i odpowiedzialnie korzysta z technologii cyfrowych, dbając o bezpieczeństwo własne i swojego otoczenia.	Uczestnik deklaruje i prezentuje właściwe postawy dotyczące bezpiecznego korzystania z technologii oraz wskazuje działania ograniczające ryzyko cyberzagrożeń dla siebie i innych użytkowników.	Wywiad swobodny

Kwalifikacje i kompetencje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie „Bezpieczeństwo cyfrowe” to kompleksowy, 4-dniowy program o łącznym wymiarze ponad 29 godzin, który łączy wykłady teoretyczne z licznymi ćwiczeniami praktycznymi. Zakres tematyczny usługi obejmuje identyfikację i obronę przed różnorodnymi cyberatakami (takimi jak phishing, malware, DDoS) oraz zasady bezpiecznego korzystania z przeglądarek internetowych i rozpoznawania ukrytych zagrożeń, np. typosquattingu czy fingerprintingu. Ważną częścią programu jest ochrona danych osobowych w świetle przepisów RODO, w tym stosowanie silnych haseł, uwierzytelniania dwuskładnikowego (2FA) oraz narzędzi wspierających anonimowość w sieci, takich jak VPN. Ponadto szkolenie kładzie duży nacisk na szeroko pojętą higienę cyfrową w pracy zdalnej i życiu codziennym – uczy bezpiecznego korzystania z mediów społecznościowych, publicznych sieci Wi-Fi oraz aplikacji do spotkań online, a także zarządzania czasem w celu uniknięcia cyfrowego wypalenia. Uczestnicy zdobywają wiedzę poprzez aktywny warsztat, realizując m.in. symulacje incydentów bezpieczeństwa, analizę e-maili pod kątem oszustw, analizę ryzyka,

Harmonogram

Liczba pozycji harmonogramu: 28

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 28 Wstęp, przedstawienie programu i zasad. Wprowadzenie do Cyberbezpieczeństwa. Bezpieczeństwo informacji i zagrożenia w podziale na życie prywatne i zawodowe	Zajęcia	PAULINA LITKA	07-12-2026	09:00	11:00	02:00
2 z 28 -	Przerwa	-	07-12-2026	11:00	11:10	00:10
3 z 28 phishing, spear phishing, malware, ransomware, DDoS oraz socjotechnika na przykładach	Zajęcia	PAULINA LITKA	07-12-2026	11:10	12:45	01:35
4 z 28 -	Przerwa	-	07-12-2026	12:45	13:40	00:55
5 z 28 Warsztat praktyczny: analiza wiadomości e-mail pod kątem prób oszustwa. Rozpoznawanie fałszywych domen, niebezpiecznych linków i załączników.	Zajęcia	PAULINA LITKA	07-12-2026	13:40	15:50	02:10
6 z 28 -	Przerwa	-	07-12-2026	15:50	16:00	00:10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 28 Symulacja incydentu bezpieczeństwa. Reagowanie na próbę wyłudzenia danych oraz procedury zgłaszania incydentów.	Zajęcia	PAULINA LITKA	07-12-2026	16:00	17:00	01:00
8 z 28 Podsumowanie incydentów. Bezpieczne korzystanie z przeglądarek internetowych. Certyfikaty bezpieczeństwa, HTTPS, bezpieczne pobieranie plików oraz rozszerzenia przeglądarek.	Zajęcia	PAULINA LITKA	08-12-2026	09:00	11:00	02:00
9 z 28 -	Przerwa	-	08-12-2026	11:00	11:10	00:10
10 z 28 Rodzaje zagrożeń oraz wycieki danych. Higiena cyfrowa zawodowo i prywatnie. Zarządzanie czasem online, przebudźcowanie oraz profilaktyka cyfrowego wypalenia. Dobre praktyki bezpieczeństwa.	Zajęcia	PAULINA LITKA	08-12-2026	11:10	12:45	01:35
11 z 28 -	Przerwa	-	08-12-2026	12:45	13:40	00:55

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 28 Ochrona i wymagania RODO. Zasady bezpiecznego przetwarzania informacji oraz odpowiedzialność. Analiza przypadków naruszenia ochrony danych osobowych.	Zajęcia	PAULINA LITKA	08-12-2026	13:40	15:50	02:10
13 z 28 -	Przerwa	-	08-12-2026	15:50	16:00	00:10
14 z 28 Identyfikacja danych osobowych, analiza ryzyka oraz dobór działań zabezpieczających. Omówienie pracy. Bezpieczne SocialMedia i komunikatory. Ochrona informacji oraz przeciwdziałanie dezinformacji.	Zajęcia	PAULINA LITKA	08-12-2026	16:00	17:00	01:00
15 z 28 Silne hasła i zarządzanie dostępem. Tworzenie bezpiecznych haseł, menedżery haseł, najczęstsze błędy użytkowników .	Zajęcia	PAULINA LITKA	14-12-2026	09:00	11:00	02:00
16 z 28 -	Przerwa	-	14-12-2026	11:00	11:10	00:10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 28 Uwierzytelnianie wieloskładnikowe (2FA/MFA). Praktyczne zastosowanie i konfiguracja zabezpieczeń kont internetowych.	Zajęcia	PAULINA LITKA	14-12-2026	11:10	12:45	01:35
18 z 28 -	Przerwa	-	14-12-2026	12:45	13:40	00:55
19 z 28 Ochrona urządzeń cyfrowych i służbowych. Aktualizacje, antywirusy, backup oraz szyfrowanie. VPN i TOR. Bezpieczeństwo pracy zdalnej, publiczne sieci Wi Fi.	Zajęcia	PAULINA LITKA	14-12-2026	13:40	15:50	02:10
20 z 28 -	Przerwa	-	14-12-2026	15:50	16:00	00:10
21 z 28 Warsztat praktyczny: konfiguracja 2FA, analiza ustawień prywatności oraz zabezpieczanie kont i urządzeń. Podsumowanie dnia, konsultacje indywidualne oraz omówienie dobrych praktyk bezpieczeństwa.	Zajęcia	PAULINA LITKA	14-12-2026	16:00	17:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
22 z 28 Kompleksowa symulacja cyberincydent u obejmująca analizę zagrożeń, ocenę ryzyka oraz wybór działań zabezpieczających	Zajęcia	PAULINA LITKA	15-12-2026	09:00	11:00	02:00
23 z 28 -	Przerwa	-	15-12-2026	11:00	11:10	00:10
24 z 28 Podsumowanie kursu i pytania przed egzaminem	Zajęcia	PAULINA LITKA	15-12-2026	11:10	12:45	01:35
25 z 28 -	Przerwa	-	15-12-2026	12:45	13:40	00:55
26 z 28 -	Walidacja	-	15-12-2026	13:40	15:50	02:10
27 z 28 -	Przerwa	-	15-12-2026	15:50	16:00	00:10
28 z 28 Podsumowanie wyników i pytania	Zajęcia	PAULINA LITKA	15-12-2026	16:00	16:30	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	24:20
w tym suma godzin walidacji	02:10
w tym suma przerw	05:00
w tym liczba godzin zajęć praktycznych indywidualnych	00:30
Suma godzin dydaktycznych bez przerw	36:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	4 800,00 PLN
Koszt osobogodziny brutto	150,00 PLN
Koszt osobogodziny netto	150,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	32:00
w tym liczba godzin zajęć praktycznych indywidualnych	00:30

Prowadzący

Liczba prowadzących: 1



1 z 1

PAULINA LITKA

Paulina to trenerka umiejętności cyfrowych z wieloletnim doświadczeniem i międzynarodowym certyfikatem trenera biznesu. Specjalizuje się w cyberbezpieczeństwie, bezpiecznym poruszaniu się w internecie, etykiecie komunikacji online oraz praktycznym wykorzystaniu AI w codziennym życiu.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dla uczestników:

Każdy uczestnik szkolenia otrzyma komplet materiałów dydaktycznych w formie cyfrowej (pliki PDF do pobrania) oraz stacjonarny pakiet biurowy.

1. Materiały dydaktyczne i warsztatowe (pliki PDF do pobrania):

- **Prezentacje i skrypty szkoleniowe:**

- Prezentacja/skrypt: *Bezpieczeństwo w przeglądarce internetowej – część 1 (teoretyczna)*
- Prezentacja/skrypt: *Bezpieczeństwo w przeglądarce internetowej – część 2 (praktyczna)*
- Prezentacja/skrypt: *Bezpieczeństwo danych osobowych – spotkanie online*
- Prezentacja/skrypt: *Anonimowość w Internecie – spotkanie online*
- Prezentacja/skrypt: *Higiena cyfrowa*

- **Karty pracy i materiały pomocnicze do ćwiczeń:**

- Szablon do opracowania projektu polityki bezpieczeństwa cyfrowego dla zespołu
- Zbiór przykładowych wiadomości e-mail do przeprowadzenia testu świadomości phishingu
- Arkusz analizy ryzyka podczas korzystania z publicznego Wi-Fi
- Scenariusz i materiały do symulacji incydentu bezpieczeństwa „Atak na firmę X”
- Formularze do audytu h

Warunki techniczne

Spotkanie na Microsoft Teams

Kontakt



MATEUSZ ELLWARDT

E-mail biuro@mpbusiness.eu

Telefon (+48) 516 674 880