Możliwość dofinansowania

FU2RES SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo w biurze: jak rozpoznawać zagrożenia i chronić dane organizacji

Numer usługi 2025/09/15/194418/3008775

mieszana (zdalna połączona z usługą zdalną w czasie rzeczywistym)

Usługa szkoleniowa

3 h

03.11.2025 do 03.11.2025

774,90 PLN brutto
630,00 PLN netto
258,30 PLN brutto/h
210,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Szkolenie przeznaczone jest dla wszystkich pracowników w organizacji (firmy i instytucje publiczne), ponieważ każdy, w mniejszym lub większym stopniu, ma do czynienia z ważnymi informacjami firmowymi.** **Wiedza przekazywana podczas naszego szkolenia jest zrozumiała dla każdego, niezależnie od stopnia zaawansowania technicznego.**
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	31-10-2025
Forma prowadzenia usługi	mieszana (zdalna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	3
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

Współczesne biuro to nie tylko dokumenty, telefony i komputery – to także codzienne korzystanie z poczty elektronicznej, systemów online, komunikatorów i chmury. Każdy pracownik, niezależnie od stanowiska, ma styczność z danymi, które mogą stać się celem ataku cyberprzestępców – od danych osobowych i finansowych po wewnętrzne informacje firmy.

Celem tego szkolenia jest zwiększenie świadomości zagrożeń cyfrowych oraz pokazanie, jak w prosty i praktyczny sposób można zabezpieczyć zarówno swoje życ

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zagrożenia w pracy biurowej	Uczestnik będzie w stanie wykazać cyber zagrożenia w pracy biurowej	Test teoretyczny
Zarządzanie hasłami i tożsamością	Uczestnik będzie wiedział jak bezpiecznie wybierać hasła logowania	Test teoretyczny
Reagowanie na incydenty	Uczestnik wie jak reagować w sytuacji powstania sytuacji kryzysowej	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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

TAK

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

TAK

Program

1. Wprowadzenie do cyberbezpieczeństwa

- Dlaczego cyberbezpieczeństwo dotyczy każdego pracownika biurowego.
- Przykłady realnych incydentów w firmach i ich skutki.
- Związek między bezpieczeństwem prywatnym a zawodowym.

2. Najczęstsze zagrożenia w pracy biurowej

- Phishing – fałszywe maile i komunikaty.
- Smishing i vishing – oszustwa telefoniczne i SMS.
- Ransomware – blokowanie danych i szantaż.
- Malware i fałszywe aktualizacje.
- Spoofing i fałszywe strony logowania.

3. Zarządzanie hasłami i tożsamością

- Jak tworzyć i zapamiętywać silne hasła.
- Rola menedżerów haseł.
- Wieloskładnikowe uwierzytelnianie (MFA).
- Najczęstsze błędy pracowników związane z hasłami.

4. Bezpieczeństwo poczty elektronicznej i komunikacji

- Jak rozpoznać podejrzane wiadomości i załączniki.
- Zasady bezpiecznej komunikacji służbowej i prywatnej.
- Ochrona danych przesyłanych mailem i w komunikatorach.

5. Bezpieczna praca biurowa i zdalna

- Podstawowe zasady ochrony komputera i smartfona.
- Aktualizacje i legalne oprogramowanie.
- Praca w chmurze – co robić, a czego unikać.
- Bezpieczne korzystanie z publicznych sieci Wi-Fi.

6. Ochrona danych osobowych i firmowych

- Podstawowe zasady zgodne z RODO.
- Jak nie dopuścić do wycieku danych z biura.
- Przechowywanie i niszczenie dokumentów (papierowych i cyfrowych).

7. Człowiek jako najsłabsze i najmocniejsze ogniwo

- Socjotechnika – jak cyberprzestępcy manipulują ludźmi.
- Budowanie świadomości i kultury bezpieczeństwa w pracy.
- Dlaczego warto zgłaszać incydenty.

8. Reagowanie na incydenty

- Co zrobić, gdy podejrzewamy atak lub naruszenie danych.
- Kiedy i komu zgłaszać problem.
- Rola zespołu IT i procedur wewnętrznych.

9. Dobre praktyki i podsumowanie

- Dyskusja: „Co zrobiłbyś w tej sytuacji?”
- Podstawowe zasady cyberhigieny na co dzień.
- Jak rozwijać swoje nawyki bezpieczeństwa w pracy i w życiu prywatnym.
- Sesja pytań i odpowiedzi.

Harmonogram

Liczba przedmiotów/zajęć: 3

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 3 Cyberbezpieczeństwo w biurze: jak rozpoznawać zagrożenia i chronić dane organizacji, cz1	-	03-11-2025	09:00	10:25	01:25

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 3 przerwa	-	03-11-2025	10:25	10:35	00:10
3 z 3 Cyberbezpieczeństwo w biurze: jak rozpoznawać zagrożenia i chronić dane organizacji, cz2	-	03-11-2025	10:35	12:00	01:25

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	774,90 PLN
Koszt przypadający na 1 uczestnika netto	630,00 PLN
Koszt osobogodziny brutto	258,30 PLN
Koszt osobogodziny netto	210,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzyma materiały szkoleniowe w formie elektronicznej.

Po szkoleniu uczestnik otrzyma certyfikat potwierdzający udział w szkoleniu.

Cena bez VAT dla opłacających szkolenie, w co najmniej 70% ze środków publicznych.

Warunki uczestnictwa

- Warunkiem ukończenia kursu jest frekwencja na poziomie co najmniej 80% zajęć.

Warunki techniczne

- komputer ze stabilnym łączem internetowym,

- przeglądarka internetowa (np. FireFox, Google Chrome, Opera, Safari),

- głośniki lub słuchawki,

- dodatkowo, dla osób oczekujących interakcji wizualnych - kamera internetowa (wbudowana lub podłączana na USB)

Kontakt

Mariusz Rejzerewicz

E-mail m.rejzerewicz@fu2res.eu

Telefon (+48) 579 044 794