Możliwość dofinansowania

NET COMPLEX SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

„Bezpieczny pracownik”. Cyberbezpieczeństwo w pracy biurowej - szkolenie, poziom podstawowy dla pracowników biurowych i administracyjnych.

Numer usługi 2026/02/16/146961/3337460

Usługa szkoleniowa
zdalna
03:00 h
22.09.2026 do 22.09.2026

553,50 PLN brutto
450,00 PLN netto
184,50 PLN brutto/h
150,00 PLN netto/h
261,33 PLN cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Grupa docelowa:** Szkolenie przeznaczone jest dla wszystkich pracowników organizacji korzystających na co dzień z komputerów, laptopów, smartfonów, tabletów i Internetu – niezależnie od działu, poziomu zaawansowania technicznego czy zajmowanego stanowiska. **Cel usługi:** Celem szkolenia jest zwiększenie świadomości uczestników w zakresie aktualnych zagrożeń cybernetycznych oraz nauczenie ich skutecznych sposobów ochrony danych i bezpiecznego korzystania z urządzeń cyfrowych. Uczestnicy poznają metody identyfikacji zagrożeń, reagowania na incydenty oraz dobre praktyki związane z ochroną prywatności, poufności informacji i przestrzeganiem przepisów (np. RODO). Szkolenie pozwala zrozumieć, jak działania cyberprzestępców mogą wpłynąć na codzienną pracę i bezpieczeństwo organizacji.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	50
Data zakończenia rekrutacji	18-09-2026
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	3

Cel

Cel edukacyjny

Po zakończeniu szkolenia uczestnik:
rozumie podstawowe pojęcia związane z cyberbezpieczeństwem i socjotechniką,
potrafi rozpoznać typowe zagrożenia i właściwie na nie reagować,
zna zasady bezpiecznego korzystania z poczty elektronicznej, przeglądarki internetowej, urządzeń mobilnych oraz nośników danych,
wie, jak unikać wycieku danych i kradzieży tożsamości,
zna konsekwencje prawne wynikające z naruszeń bezpieczeństwa (RODO, tajemnica służbowa),

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje podstawowe zagrożenia cyberbezpieczeństwa (np. phishing, ransomware)	Poprawnie identyfikuje przykłady zagrożeń na podstawie omawianych scenariuszy	Test teoretyczny
Potrafi stosować zasady bezpiecznej pracy z hasłami i pocztą elektroniczną	Wskazuje dobre praktyki podczas pracy z hasłami i skrzynką mailową	Test teoretyczny
Rozumie, jak chronić dane osobowe i informacje firmowe	Rozróżnia informacje poufne, zna podstawy RODO w kontekście codziennej pracy	Test teoretyczny
Stosuje bezpieczne nawyki w codziennej pracy z komputerem i Internetem	Opisuje konkretne działania ograniczające ryzyko cyberataku w pracy biurowej	Test teoretyczny
Zna sposoby reagowania na podejrzane wiadomości i incydenty cyberbezpieczeństwa	Potrafi opisać procedurę zgłoszenia incydentu w firmie	Wywiad swobodny

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

Zakres tematyczny (program):

- Wprowadzenie do socjotechniki
- Bezpieczne poruszanie się w Internecie
- Zagrożenia związane z pocztą elektroniczną
- Smartfony i urządzenia mobilne – co może pójść nie tak?
- Nośniki danych – jakie ryzyka niesie pendrive?
- Otwarte sieci Wi-Fi – jak z nich korzystać bezpiecznie?
- Hasła – jak tworzyć silne i jak je przechowywać?
- Urządzenia IoT i inteligentny dom – czy mogą zagrażać?
- Podsumowanie i sesja pytań

Sposób organizacji usługi:

Szkolenie trwa 3 godziny zegarowe (w tym przerwa 20 minut). Realizowane jest w formie prezentacji z elementami dyskusji i wymiany doświadczeń.

Możliwość organizacji szkolenia w formie stacjonarnej lub zdalnej.

Szkolenie może zostać przeprowadzone również w formule zamkniętej, dedykowanej konkretnej firmie – z dostosowaniem treści do profilu działalności organizacji i poziomu wiedzy uczestników

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	553,50 PLN
Koszt przypadający na 1 uczestnika netto	450,00 PLN
Koszt osobogodziny brutto	184,50 PLN
Koszt osobogodziny netto	150,00 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Korzyści dla uczestników

Osiągnięcie umiejętności związanych z identyfikacją zagrożeń, tj. rozpoznanie i właściwa reakcja.Nabycie kompetencjidotyczących właściwej oceny ryzyka, unikania sytuacji, mogących prowadzić do naruszenia prywatności, poufności, strat materialnych, wizerunkowych (np. efekt kradzieży tożsamości). Ponadto dowiesz się więcej o konsekwencjach prawnych wynikających z wycieków poufnych danych, niedochowania tajemnicy służbowej, naruszania przepisów RODO. Dzięki szkoleniu poznasz sposoby ochrony przed cyberprzestępcami.

Ponadto:

- dowiesz się jak działają cyberprzestępcy i jaki może mieć to wpływ na twoją pracę
- poznasz metody ochrony przed atakami komputerowymi i socjotechnicznymi
- dowiesz się jak bezpiecznie korzystać z programów pocztowych i Internetu
- nauczysz się bezpiecznie przechowywać dane na laptopie i pendrive
- poznasz sytuacje w którychnie powinieneś podawać swoich danych (login i hasło)
- nauczysz się bezpiecznie korzystać z sieci Wi-Fi oraz zdalnego pulpitu

Program 3-godzinnego szkolenia z bezpieczeństwa dla pracowników "nie-informatyków":

1. Parę słów o socjotechnice
2. Bezpieczne poruszanie się w Internecie
3. Poczta elektroniczna
4. Smartfony i urządzenia mobilne
5. Co mogę "przynieść" na pendrivie?
6. Niebezpieczeństwa otwartych sieci WIFI
7. Czy moje hasła są bezpieczne?
8. Inteligentny dom i "Internecie Rzeczy"
9. Podsumowanie

Warunki techniczne

Laptop lub komputer stacjonarny , dostęp do internetu, przeglądarka internetowa, kamera internetowa , mikrofon, słuchawki lub głośniki

Kontakt

Karolina Błasiak

E-mail k.blasiak@netcomplex.pl

Telefon (+48) 798 396 359