Możliwość dofinansowania

# Cyberbezpieczeństwo pracowników biurowych - kurs o bezpieczeństwie IT

**Numer usługi** 2026/01/20/17164/3270916

725,70 PLN brutto
590,00 PLN netto
120,95 PLN brutto/h
98,33 PLN netto/h

Dagma sp. z o.o.

4,5 / 5

441 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
6 h
20.05.2026 do 20.05.2026

# Informacje podstawowe

| | |
|---|---|
| **Kategoria** | Informatyka i telekomunikacja / Bezpieczeństwo IT |
| **Grupa docelowa usługi** | Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania:<br>• podstawowa umiejętność obsługi komputera |
| **Minimalna liczba uczestników** | 10 |
| **Maksymalna liczba uczestników** | 100 |
| **Data zakończenia rekrutacji** | 11-05-2026 |
| **Forma prowadzenia usługi** | zdalna w czasie rzeczywistym |
| **Liczba godzin usługi** | 6 |
| **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 dostarczenie kompetencji w zakresie Bezpieczeństwa teleinformatycznego, dzięki którym uczestnik będzie samodzielnie rozpoznawał próby ataku cyberprzestępczego, bezpiecznie zarządzał miejscem pracy oraz danymi, do których ma dostęp oraz chronił własność firmy przed atakami socjotechnicznymi. Uczestnik po ukończonym szkoleniu nabędzie kompetencje społeczne takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| Efekty dotyczące wiedzy: uczestnik chroni siebie i dane firmowe przed atakami socjotechnicznymi | Rozpoznaje próby ataku na firmowe sieci, weryfikując adresy mailowe nadawcy, bezpieczeństwo linków, prawdziwość informacji | Obserwacja w warunkach symulowanych |
| Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu. | Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji | Wywiad swobodny |
| Efekty dotyczące umiejętności: uczestnik bezpiecznie zarządza miejscem pracy oraz danymi | Zabezpiecza wysyłane maile hasłem, szyfruje udostępniane dane firmowe | Obserwacja w warunkach symulowanych |
| Zwiększa bezpieczeństwo firmowych stron i platform | Przeprowadza próby ataków DoS/DDoS i ataków 0-day na firmowe zasoby, w celu wykrycia błędów w zabezpieczeniach | 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

**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 cyberprzestępczości: Poznaj podstawy cyberbezpieczeństwa.
2. Krajobraz zagrożeń 2024–2025 w Polsce i na świecie.
3. Czy jestem atrakcyjnym klientem dla cyberprzestępcy?
4. Rodzaje ataków na pracowników biurowych.
5. Straty dla firmy: Skutki udanego cyberataku.
6. Spam jako niegroźny sposób na groźne ataki.
7. Phishing jako metoda okradania naszych kont bankowych.
8. Opłacona faktura jako sposób przemycenia wirusa do naszego systemu.

9. KSeF – czym jest i dlaczego może stać się atrakcyjnym celem ataków.
10. Dlaczego KSeF nie musi zostać „zhakowany” aby doszło do nadużyć.
11. Użytkownik jako najsłabsze ogniwo systemów informatycznych.
12. Skuteczne metody ochrony przed cyberatakami.
13. AI w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji.
14. AI – deepfake co to jest i jakie są rodzaje (generowanie głosu, spreparowanych dokumentów, komunikatów czy obrazów)
15. Procedura weryfikacji danych i użytkowników na dwa kanały.
16. Czy cyberprzestępca jest zawsze anonimowy?
17. Ataki DoS/DDoS: Zagrożenia dla instytucji.
18. Aktualizacja oprogramowania jak ważną rolę spełnia?
19. Sieci Botnet: Jak cyberprzestępcy przejmują urządzenia.
20. Bezpieczeństwo haseł: Jak cyberprzestępcy zdobywają Twoje hasła?
21. Menadżer hasłem program, który zwiększa bezpieczeństwo.
22. Metody logowania 2FA oraz MFA.
23. Ataki socjotechniczne, czyli niewinne wyłudzanie danych z użyciem sztucznej inteligencji.
24. Socjotechnika stara metoda w nowoczesnych atakach.
25. Kradzież tożsamości w sieci, jakie to łatwe.
26. Skimming kart płatniczych: Gdzie i kiedy ktoś może zeskanować Twoją kartę?
27. Fizyczne bezpieczeństwo: Jak zabezpieczyć swoje miejsce pracy.
28. Ataki za pomocą przenośnych nośników danych, co zrobić z takimi nośnikami.
29. Sprzęt prywatny vs. firmowy: Jak zarządzać bezpieczeństwem urządzeń.

Walidacja jest wliczona w czas trwania szkolenia. Przerwy nie są wliczone w czas trwania szkolenia

# Harmonogram

Liczba przedmiotów/zajęć: 0

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| Brak wyników. | | | | | |

# Cennik

## Cennik

| Rodzaj ceny | Cena |
|---|---|
| **Koszt przypadający na 1 uczestnika brutto** | 725,70 PLN |
| **Koszt przypadający na 1 uczestnika netto** | 590,00 PLN |
| **Koszt osobogodziny brutto** | 120,95 PLN |
| **Koszt osobogodziny netto** | 98,33 PLN |

# Prowadzący

Liczba prowadzących: 0

Brak wyników.

# Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

- - materiały dydaktyczne w formie elektronicznej (link do materiałów producenta lub e-book, lub dostęp do materiałów autorskich, przygotowanych przez trenera, przesłane na adres e-mail uczestnika)

## Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl** w celu rezerwacji miejsca.

## Informacje dodatkowe

- Jedna godzina lekcyjna to 45 minut.
  - W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
  - Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia.
  - Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA Sp. z o.o.

# Warunki techniczne

**WARUNKI TECHNICZNE:**

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM i/lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.

- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie:
https://szkolenia.dagma.eu/pl/training,catalog,6112/cyberbezpieczenstwo-pracownikow-biurowych-kurs-o-bezpieczenstwie-it

# Kontakt


## Michalina Krzyszkowska

**E-mail** krzyszkowska.m@dagma.pl
**Telefon** (+48) 327 931 015