



TOMASZ
KOPCZYŃSKI
"SYNERGIA"



Cyberbezpieczeństwo w praktyce – ochrona danych i systemów w życiu codziennym i zawodowym

Numer usługi 2025/05/08/21247/2733471

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 24 h

📅 21.06.2025 do 29.06.2025

4 320,00 PLN brutto

4 320,00 PLN netto

180,00 PLN brutto/h

180,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	Szkolenie skierowane jest do osób w każdym wieku, niezależnie od poziomu wykształcenia i doświadczenia zawodowego, które chcą zdobyć lub rozwinąć kompetencje w zakresie bezpiecznego korzystania z urządzeń cyfrowych i systemów informatycznych – zarówno w codziennym życiu, jak i w środowisku zawodowym.
Minimalna liczba uczestników	7
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	20-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
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

Szkolenie ma na celu rozwinięcie kompetencji uczestników w zakresie rozpoznawania zagrożeń cyfrowych oraz stosowania praktycznych zasad ochrony danych i systemów w życiu prywatnym i zawodowym. Uczestnicy zdobędą

umiejętności umożliwiające świadome i bezpieczne korzystanie z technologii informatycznych oraz reagowanie na typowe incydenty bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpoznaje podstawowe zagrożenia cyberbezpieczeństwa (phishing, malware, ransomware, itp.)	Udział w teście teoretycznym obejmującym zagrożenia i sposoby ich rozpoznania	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady bezpiecznej pracy z danymi i systemami informatycznymi	Wypełnienie checklisty zachowań bezpiecznego użytkownika	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik potrafi zabezpieczyć urządzenia i konta (hasła, dwuetapowe logowanie, szyfrowanie)	Przeprowadzenie konfiguracji zabezpieczeń w ćwiczeniu praktycznym	Obserwacja w warunkach symulowanych
Uczestnik zna podstawowe procedury reagowania na incydenty bezpieczeństwa	Udział w symulacji incydentu bezpieczeństwa i prezentacja sposobu reakcji	Obserwacja w warunkach symulowanych
Uczestnik potrafi opracować plan działań bezpieczeństwa dla swojej organizacji lub środowiska domowego	Prezentacja planu działań opracowanego w grupie lub indywidualnie	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, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji

Program

Szkolenie odbywa się w godzinach zegarowych, z jedną 30-minutową przerwą po 3 godzinach zajęć dziennie.

Dzień 1 – Podstawy cyberbezpieczeństwa (6h)

Moduł 1: Czym jest cyberbezpieczeństwo i dlaczego nas dotyczy

- Wprowadzenie do cyberbezpieczeństwa – skala zagrożeń
- Typowe zagrożenia: phishing, malware, ransomware, spyware, scam
- Inżynieria społeczna – jak działają oszuści
- Praktyczne rozpoznawanie fałszywych wiadomości i stron (ćwiczenia)

Dzień 2 – Bezpieczne dane i urządzenia (6h)

Moduł 2: Ochrona danych i prywatności

- Bezpieczne hasła, menedżery haseł, MFA (weryfikacja dwuetapowa)
- Szyfrowanie danych i bezpieczne przechowywanie plików (lokalnie i w chmurze)
- Ochrona urządzeń mobilnych, pracy zdalnej i komunikatorów
- Praca z danymi osobowymi – RODO w praktyce codziennej

Dzień 3 – Reagowanie na zagrożenia i narzędzia wspierające (6h)

Moduł 3: Jak reagować na incydenty i chronić się proaktywnie

- Objawy ataków i naruszeń bezpieczeństwa
- Procedury reagowania – co robić, gdy coś pójdzie nie tak?
- Backup danych – rodzaje, cykle, narzędzia
- Przegląd programów i aplikacji wspierających bezpieczeństwo

Dzień 4 – Cyberbezpieczeństwo w praktyce (5h)

Moduł 4: Warsztaty praktyczne i planowanie działań

- Tworzenie własnej polityki bezpieczeństwa (indywidualnie lub w grupach)
- Symulacja incydentu – scenariusze i reakcje
- Tworzenie planu wdrożenia dobrych praktyk bezpieczeństwa
- Podsumowanie

WALIDACJA (1 h)

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Podstawy cyberbezpieczeństwa	Łukasz Kopczyński	21-06-2025	09:00	12:00	03:00
2 z 9 Podstawy cyberbezpieczeństwa	Łukasz Kopczyński	21-06-2025	12:30	15:30	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 9 Bezpieczne dane i urządzenia	Łukasz Kopczyński	22-06-2025	09:00	12:00	03:00
4 z 9 Bezpieczne dane i urządzenia	Łukasz Kopczyński	22-06-2025	12:30	15:30	03:00
5 z 9 Reagowanie na zagrożenia i narzędzia wspierające	Łukasz Kopczyński	28-06-2025	09:00	12:00	03:00
6 z 9 Reagowanie na zagrożenia i narzędzia wspierające	Łukasz Kopczyński	28-06-2025	12:30	15:30	03:00
7 z 9 Cyberbezpieczeństwo w praktyce	Łukasz Kopczyński	29-06-2025	09:00	12:00	03:00
8 z 9 Cyberbezpieczeństwo w praktyce	Łukasz Kopczyński	29-06-2025	12:30	14:30	02:00
9 z 9 WALIDACJA	-	29-06-2025	14:30	15:30	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 320,00 PLN
Koszt przypadający na 1 uczestnika netto	4 320,00 PLN
Koszt osobogodziny brutto	180,00 PLN
Koszt osobogodziny netto	180,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Łukasz Kopczyński

Łukasz Kopczyński to doświadczony trener z zakresu technologii cyfrowych, absolwent informatyki na Uniwersytecie Ekonomicznym w Poznaniu. Od ponad 5 lat prowadzi szkolenia, łącząc wiedzę techniczną z praktycznym podejściem do nauki. Na swoim koncie ma już ponad 500 godzin szkoleniowych, zrealizowanych dla uczestników indywidualnych oraz firm z różnych branż.

Specjalizuje się w tematyce cyberbezpieczeństwa, marketingu internetowego, nowoczesnych narzędzi do zarządzania projektami, a także w szkoleniach z obsługi pakietu MS Office i innych narzędzi biurowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają komplet materiałów w formie elektronicznej, które będą dostępne do pobrania przed rozpoczęciem szkolenia oraz na bieżąco w trakcie jego trwania.

Materiały obejmują:

- **Podręcznik „Cyberbezpieczeństwo w praktyce”** – zawierający podsumowanie najważniejszych zagadnień omawianych podczas szkolenia, w tym typowe zagrożenia, dobre praktyki, checklisty oraz przykładowe scenariusze reagowania na incydenty.
- **Prezentacje multimedialne** wykorzystywane podczas zajęć – w formacie PDF.
- **Interaktywne arkusze ćwiczeń** – m.in. symulacje rozpoznawania phishingu, analiza ryzyka, tworzenie planu bezpieczeństwa.
- **Zestaw narzędzi rekomendowanych** do zwiększenia poziomu bezpieczeństwa cyfrowego (linki do aplikacji, rozszerzeń przeglądarkowych, menedżerów haseł itp.).
- **Certyfikat uczestnictwa** w formacie PDF (dla osób, które ukończą szkolenie i wezmą udział w walidacji).

Informacje dodatkowe

Szkolenie realizowane jest w godzinach zegarowych. W harmonogramie zostały uwzględnione 30 min. przerwy, które nie wliczają się w czas szkolenia.

Usługa zwolniona z VAT ze względu na dofinansowanie powyżej 70%, podstawa zwolnienia par. 3, ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2023 r., poz. 955 ze zm.)

Warunki techniczne

1. Komputer lub urządzenie mobilne – w przypadku urządzenia mobilnego można pobrać odpowiednią aplikację „Google Meet” ze sklepu Google Play lub AppStore.
2. Szerokopasmowe połączenie z internetem.
3. Wymagania sprzętowe - procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy), 2GB pamięci RAM (zalecane 4GB lub więcej).
4. Mikrofon zewnętrzny lub mikrofon wbudowany w urządzeniu oraz głośniki zewnętrzne lub wbudowane w urządzeniu. Szkolenie prowadzone będzie na platformie google meets lub clickmeeting

Kontakt



Tomasz Kopczyński

E-mail tomasz.kopczynski@synergia-pm.pl

Telefon (+48) 509 309 328