



Dagma sp. z o.o.



Cyberbezpieczeństwo pracowników biurowych - kurs o bezpieczeństwie IT

Numer usługi 2024/07/26/17164/2237989

zdalna w czasie rzeczywistym

Usługa szkoleniowa

6 h

15.11.2024 do 15.11.2024

356,70 PLN brutto

290,00 PLN netto

59,45 PLN brutto/h

48,33 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: podstawowa umiejętność obsługi komputera
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	08-11-2024
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 nabeǓdzie kompetencje społeczne takie jak samokształcenie, rozwiǓzywanie problemów, kreatywność w działaniu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po ukończonym szkoleniu uczestnik zdobywa wiedzę obejmującǓ bezpieczne zarządzanie miejscem pracy oraz danymi, a także zdobywa umiejętności umożliwiające ochronę przed atakami socjotechnicznymi	Dyskusja z trenerem, rozwiǓzywanie problemów	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

Moduł 1 Wprowadzenie do cyberprzestępczości: Poznaj podstawy cyberbezpieczeństwa - zajęcia teoretyczne (wykład)

- Zorganizowane grupy cyberprzestępcze: Jak działają i dlaczego są groźne.
- Czy cyberprzestępcy naprawdę nam zagrażają?
- Czy jestem atrakcyjnym klientem dla cyberprzestępcy?
- Korzyści dla cyberprzestępców: Co zyskują atakując Twoje dane?
- Rodzaje ataków na pracowników biurowych.
- Straty dla firmy: Skutki udanego cyberataku.
- Sieci Botnet: Jak cyberprzestępcy przejmują komputery.
- Skuteczne metody ochrony przed cyberatakami.

Moduł 2 AI w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji - zajęcia praktyczne (ćwiczenia)

- Spam jako niegroźny sposób na groźne ataki.
- Czy cyberprzestępcą jest zawsze anonimowy?
- Phishing jako metoda okradania naszych kont bankowych.

- Ataki DoS/DDoS: Zagrożenia dla instytucji.
- Ataki 0-day: Czy istnieje sposób obrony przed nimi?
- Opłacona faktura jako sposób przemycenia wirusa do naszego systemu.
- Bezpieczeństwo haseł: Jak cyberprzestępcy zdobywają Twoje hasła?
- Skanowanie kart płatniczych: Gdzie i kiedy ktoś może zeskanować Twoją kartę?

Moduł 3 Ataki socjotechniczne, czyli niewinne wyłudzanie danych - zajęcia teoretyczne (wykład)

- Kradzież tożsamości: Co? Jak? Kiedy? Gdzie?
- Bezpieczne przekazywanie haseł współpracownikom.
- Fizyczne bezpieczeństwo: Jak zabezpieczyć miejsce pracy.
- Znaleziony pendrive, jako pozwolenie na atak cyberprzestępcy.
- Zwiększenie odporności na cyberataki: Proste i skuteczne metody.
- Sprzęt prywatny vs. firmowy: Jak zarządzać bezpieczeństwem urządzeń.

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 6 godz. lekcyjnych). Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw.

Harmonogram

Liczba przedmiotów/zajęć: 5

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 Moduł 1 Wprowadzenie do cyberprzestępczości: Poznaj podstawy cyberbezpieczeństwa - zajęcia teoretyczne (wykład)	Paweł Majewski	15-11-2024	09:00	10:30	01:30
2 z 5 przerwa	Paweł Majewski	15-11-2024	10:30	10:45	00:15
3 z 5 Moduł 2 AI w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji - zajęcia praktyczne (ćwiczenia)	Paweł Majewski	15-11-2024	10:45	13:00	02:15
4 z 5 przerwa	Paweł Majewski	15-11-2024	13:00	13:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 5 Moduł 3 Ataki socjotechniczne, czyli niewinne wyłudzenie danych - zajęcia teoretyczne (wykład)	Paweł Majewski	15-11-2024	13:30	14:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	356,70 PLN
Koszt przypadający na 1 uczestnika netto	290,00 PLN
Koszt osobogodziny brutto	59,45 PLN
Koszt osobogodziny netto	48,33 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Paweł Majewski

Doświadczenie zawodowe: Trener IT, prowadzący szkolenia w DAGMA Szkolenia IT. Wieloletni praktyk metody OSINTu. Związany z sieciami i serwerami od 2007 roku. Specjalizujący się w dziedzinach Microsoftu, teorii i praktyk funkcjonowania sieci komputerowych, monitorowania i rozwiązywania problemów w sieciach komputerowych oraz bezpieczeństwem teleinformatycznym pracowników biurowych.

Certyfikaty i kursy, m.in.:

- Safetica Administrator - Management Server & Monitoring
- Certified Stormshield Network Expert (CSNE)
- ESET Client & Network Security Administrator
- Certified Ethical Hacker v 12

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (prezentacja przygotowana przez trenera, przesłana na adres mailowy uczestnika)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową

<https://szkolenia.dagma.eu/pl/training,catalog,6112/cyberbezpieczenstwo-pracownikow-biurowych-kurs-o-bezpieczenstwie-it> w celu rezerwacji miejsca.

Informacje dodatkowe

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzi koszt związany z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- 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 Szkolenia IT

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



Agnieszka Palenga

E-mail palenga.a@dagma.pl

Telefon (+48) 32 7931 139