Możliwość dofinansowania

Cyberbezpieczeństwo - zastosowanie praktycznych technik bezpieczeństwa w pracy biurowej.

Numer usługi 2024/05/14/45589/2148829

4 100,00 PLN brutto
4 100,00 PLN netto
102,50 PLN brutto/h
102,50 PLN netto/h

Fundacja AKTYWNA GALICJA

★★★★★

zdalna
Usługa szkoleniowa
40 h
05.08.2024 do 31.08.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	02-08-2024
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	40
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

Usługa ma na celu zwiększenie świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz higieny w sieci, z naciskiem na rozumienie i praktyczne stosowanie najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym i osobistym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawowe pojęcia związane z cyberbezpieczeństwem i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Uczestnik poprawnie definiuje wymienione pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Test teoretyczny
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik wymienia i opisuje co najmniej trzy różne typy zagrożeń, podając przykłady oraz sposoby ich identyfikacji.	Test teoretyczny
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Test teoretyczny
Identyfikuje i reaguj na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania na te zagrożenia.	Test teoretyczny
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik potrafi skonfigurować bezpieczne połączenie sieciowe i stosuje praktyki ochrony prywatności podczas korzystania z sieci publicznych.	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

Dzień 1

1. wprowadzenie do szkolenia
2. audyt cyberbezpieczeństwa
3. istota i podstawowe terminy w zakresie cyberbezpieczeństwa
4. podstawy prawne cyberbezpieczeństwa i zalecenia ENISA
5. najpopularniejsze ataki cybernetyczne
6. ćwiczenie: phishing

Dzień 2

1. przestępstwa finansowe w przestrzeni cyfrowej
2. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
3. jak działa i jak wybrać menadżera haseł?
4. dlaczego tak często hakerzy łamią hasła?
5. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
6. szyfrowanie plików,folderów i pendrive'ów w praktyce

Dzień 3

1. jak chronić dane osobowe zgodnie z RODO?
2. zastrzeż swój PESEL
3. jak robić backup danych?
4. dlaczego warto korzystać z„chmury”?
5. wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?

Dzień 4

1. jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
2. co o nas wiedzą?
3. socjotechniki wykorzystywane przez hakerów 9:30 – 9:45 – przerwa kawowa
4. co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna
5. jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?

Dzień 5

1. jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
2. ćwiczenie grupowe: symulacje ataków cybernetycznych
3. narzędzia i programy wzmacniające bezpieczeństwo cyfrowe
4. Podsumowanie
5. Test

Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut.

W ciągu dnia zostały uwzględnione 2 przerwy po 30 minut które nie są wliczane do czasu trwania usługi.

Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 100,00 PLN

Koszt przypadający na 1 uczestnika netto	4 100,00 PLN
Koszt osobogodziny brutto	102,50 PLN
Koszt osobogodziny netto	102,50 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przesłane drogą mailową w formacie pdf. Uczestnik otrzyma:

1. skrypty

Warunki uczestnictwa

Warunkiem rozpoczęcia kursu jest zebranie minimalnej liczby uczestników.

Informacje dodatkowe

Każdy uczestnik po ukończeniu kursu musi przystąpić do egzaminu wewnętrznego.

Warunki techniczne

platforma click meeting

Kontakt

Katarzyna Tułecka

E-mail kasia@aktywnagalicja.pl
Telefon (+48) 664 387 707