Możliwość dofinansowania

Wektor Wiedzy Sp. z o.o.

★★★★½

Księgowość, kadry i finanse w dobie cyberprzestępstw – kurs online

Numer usługi 2024/05/17/43371/2153795

2 693,70 PLN brutto
2 190,00 PLN netto
149,65 PLN brutto/h
121,67 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
18 h
29.10.2024 do 26.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Osoby zatrudnione w działach finansowo- księgowych oraz kadrowych w panującej wirtualnej rzeczywistości. Samodzielni księgowi, główni księgowi, dyrektorzy finansowi oraz pracownicy działów finansowych i księgowości, prowadzący i pracownicy biur rachunkowych. Szkolenie jest przydatne każdej osobie, która na co dzień w swojej pracy korzysta z komputera oraz innych urządzeń z dostępem do Internetu.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	28-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	18
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

Kurs przygotowuje do samodzielnej pracy w wirtualnej rzeczywistości, ze świadomością zagrożeń związanych z cyberprzestępczością oraz znajomością metod identyfikacji zagrożeń i reagowania na nie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Prawidłowo zabezpiecza swoje dane przed cyberatakiem	- uczestnik definiuje pojęcie cyberprzestępczość oraz najpowszechniejsze rodzaje ataków i zagrożeń. - charakteryzuje dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów. - - określa jakie zasady pracy zdalnej pomogą mu skutecznie zabezpieczyć się przed 99% ataków.	Test teoretyczny
Organizuje cyberbezpieczeństwo w kadrach i księgowości	- uczestnik monitoruje incydenty bezpieczeństwa teleinformatycznego. - korzysta z zabezpieczeń w codziennej pracy, unika aplikacji i programów, których należy się wystrzegać. Używa bezpieczne hasła oraz organizery haseł.	Test teoretyczny
Ocenia jak prawidłowo zachowywać się w różnych sytuacjach w pracy zawodowej	- pracuje ze świadomością poziomu swojej wiedzy i umiejętności, - definiuje swoje potrzeby w zakresie samokształcenia - prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	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, zawiera informacje dotyczące pozyskanej wiedzy, umiejętności i kompetencji społecznych.

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

Tak, zawiera potwierdzenie.

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

Tak, zawiera potwierdzenie.

Program

Temat 1 – Zagrożenia, ataki i incydenty cyberbezpieczeństwa w branży finansowo-kadrowej.

1. Podstawy cyberbezpieczeństwa.
- Czy w świecie cyfrowym jest bezpiecznie?
- Podstawowe narzędzia cyberbezpieczeństwa.
- Aktualność problemu bezpieczeństwa teleinformatycznego – socjotechnika i manipulacje przestępców.
- Z czego składa się system cyberbezpieczeństwa?
- Powszechność zagrożeń.
- Co ryzykujemy zaniedbując cyberbezpieczeństwo?

2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji).
- Czym jest socjotechnika?
- Dlaczego człowiek jest najsłabszym ogniwem.
- Przykłady podstępów socjotechnicznych – wyłudzenia dokumentów, loginów, haseł.
- Jak i skąd atakujący zbierają dane na twój temat?
- Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci.

3. Klasyfikacja zagrożeń dla sieci teleinformatycznej i ich źródeł - system i jego podatność.
- Antywirus i firewall.
- Niebezpieczeństwo ataków firmę/instytucję.
- Co zrobić, gdy zidentyfikujemy atak?
- Podatność systemu.
- Sposoby atakowania sieci, rodzaje włamań sieciowych.
- Niebezpieczny system.
- Niebezpieczne aplikacji i źródła.
- Podatność na ataki w związku z przelewami i bankowością.

4. Monitorowanie incydentów bezpieczeństwa teleinformatycznego.
- Zbieranie danych, diagnozowanie incydentów, podejmowanie działań naprawczych.

Temat 2 – Jak się nie dać zaskoczyć cyberzagrożeniom?

1. Mechanizmy i programy ochrony przed zagrożeniami cyberbezpieczeństwa.
- Jakie emocje wykorzystują oszuści w wyłudzeniach danych i finansów?
- Keyloggery – jak działają, jak się bronić?
- Malware i Spyware.
- Zagrożenia i zabezpieczenia laptopów i dysków.
- VPN – co to i kiedy korzystać?

2. (Nie)bezpieczne płatności.
- Płatności niebezpieczne.
- Płatności bezpieczne.
- Płatności przez portale.
- Kto prosi mnie o płatność.

3. Fałszywi konsultanci.
- Jak przeprowadzane są ataki telefoniczne?
- Fałszywe załączniki.
- Fałszywe smsy.

4. Bezpieczne hasła i logowanie.
- Skuteczne organizowanie i zabezpieczanie haseł.
- Uwierzytelnianie dwuskładnikowe.
- Wrażliwe dostępny o które należy zadbać?
- Jak pracować z pocztą elektroniczną?

5. Metody i środki bezpieczeństwa – w branży finansowej.
- Bezpieczeństwo fizyczne.
- Kopie zapasowe i redundantność.
- Ochrona Danych Osobowych i zagrożenia.
- Kontrola dostępu.

- Zasady ochrony urządzeń mobilnych.
- Polityka stosowania rozwiązań kryptograficznych i szyfrowanie informacji
przedsięwzięcia organizacyjne.
- Zarządzanie uprawnieniami użytkowników systemów informatycznych, kontrola dostępu.

6. Atak „na komputery” - demonstracje wraz z objaśnieniem metod ochrony.
- Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących.
- Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC).
- Ataki przez pocztę e-mail (fałszywe e-maile).
- Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony?
- Ataki przez komunikatory (Skype, Facebook).
- Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.).
- Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam.

Temat 3 – Jak zorganizować cyberbezpieczeństwo w kadrach i księgowości?
1. Cyberprzestępczość - najpowszechniejsze rodzaje ataków i zagrożeń – praktyczne case study przypadków.
- Phishing i inne odmiany ataków socjotechnicznych.
- Pozostałe zagrożenia dla bezpieczeństwa sieci teleinformatycznej.
- Cracking.
- Sniffing.
- Metoda salami.
- Fałszywe powiadomienia z mediów społecznościowych.
- Oszustwo na „nigeryjskiego księcia”.
- Skimming.

2. Organizacja bezpiecznej sieci teleinformatycznej i bezpieczeństwa informacji – rozwiązania systemowe i wymagania prawne w Polsce.
- Norma ISO 27001:2017.
- Rozporządzenie o Ochronie Danych Osobowych.
- Rozporządzenie o Krajowych Ramach Interoperacyjności.
- Projektowanie bezpiecznej sieci teleinformatycznej.
- Narzędzia do weryfikacji bezpieczeństwa teleinformatycznego.

3. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów.
- Polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych.
- Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko”.
- Bezpieczeństwo danych osobowych kadrowych.
- Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop).
- Problem aktualnego oprogramowania i kopii zapasowych.
- Bezpieczna praca z pakietem biurowym Microsoft Office.
- Bezpieczna praca z programem pocztowym.
- Bezpieczna praca z przeglądarką internetową.
- Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty).

4. Aspekty prawne.
- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji.
- Nieautoryzowane użycie systemów komputerowych.
- Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego.
- Dane osobowe i dane wrażliwe.
- Jakie działania związane z cyberatakami kwalifikowane są jako przestępstwa?
- Jakie kary grożą za popełnianie cyberprzestępstw?
- Jakie prawa ma ofiara, która padła ofiarą cyberprzestępstwa?
- Nieautoryzowane użycie komputera.

Wymagania wstępne dla uczestników kształcenia:Umiejętność pracy z komputerem, znajomość środowiska Windows, Internet.

Usługa jest realizowana w godzinach zegarowych.

Kurs przeprowadzany będzie w formie online, bez podziału na grupy. Uczestnicy mają możliwość korzystania zarówno z kamerki jak i mikrofonu. Taką chęć mogą zgłaszać na bieżąco poprzez kliknięcie ikonki „dłoń”. Pytania można również zadawać za pomocą czatu.

Harmonogram

Liczba przedmiotów/zajęć: 3

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 3 Zagrożenia, ataki i incydenty cyberbezpieczeństwa w branży finansowo-kadrowej.	Daniel Lampart	29-10-2024	09:00	15:00	06:00
2 z 3 Jak się nie dać zaskoczyć cyberzagrożeniom?	Daniel Lampart	12-11-2024	09:00	15:00	06:00
3 z 3 Jak zorganizować cyberbezpieczeństwo w kadrach i księgowości?	Daniel Lampart	26-11-2024	09:00	15:00	06:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 693,70 PLN
Koszt przypadający na 1 uczestnika netto	2 190,00 PLN
Koszt osobogodziny brutto	149,65 PLN
Koszt osobogodziny netto	121,67 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Lampart

Trener, licencjonowany audytor wiodący norm ISO 9001 (zarządzanie jakością) oraz 27001(bezpieczeństwo informacji), Ekspert w zakresie zarządzania procesowego, podnoszenia

efektywności i wydajności biznesowej, wdrożeniowiec systemów zarządzania jakością oraz bezpieczeństwa informacji. Konsultant w zakresie bezpieczeństwa danych osobowych, Inspektor Ochrony danych Osobowych w wielu firmach prywatnych i jednostkach publicznych w Polsce. Doświadczenie zawodowe zdobywał na stanowiskach Inspektora Ochrony Danych Osobowych, Audytora wiodącego systemów zarządzania jakością i bezpieczeństwem informacji.
Ponad 150 zrealizowanych wdrożeń systemów bezpieczeństwa informacji. Od 5 lat auditor wiodący Normy ISO 27001 oraz 27701 realizujący Audyty certyfikacyjne dla międzynarodowych jednostek certyfikujących m.in. QS Zurich, ICVC, DeuZert GmbH.
Jako trener pro-aktywnie realizuje rocznie dziesiątki szkoleń w zakresie ochrony danych osobowych, zarządzania procesami, oraz bezpieczeństwa informacji dla branży handlowej, medycznej, urzędów państwowych oraz wymiaru sprawiedliwości, przygotowuje również do pełnienia funkcji Inspektora Ochrony Danych Osobowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik usługi otrzyma komplet materiałów szkoleniowych w formie PDF, przygotowany przez prowadzących:

- Skrypt

- dostęp do nagrania szkolenia na okres 21 dni.

Warunki uczestnictwa

Umiejętność pracy z komputerem, znajomość środowiska Windows, Internet

Informacje dodatkowe

Cena bez VAT dla opłacających szkolenie, w co najmniej 70% ze środków publicznych.

Zapraszamy do odwiedzenia naszej strony internetowej: https://wektorwiedzy.pl/

Warunki techniczne

Szkolenie bedzie prowadzone za pośrednictwem Platformy ClickMeeting.

Szkolenia na ClickMeeting nie wymagają instalowania żadnego programu, są transmitowane przez przeglądarkę. Bardzo ważne jest, żeby była ona zaktualizowana do najnowszej wersji (jeśli nie będzie aktualna, podczas testu nie pojawi się zielony "✓"). W razie potrzeby istnieje też możliwość pobrania aplikacji mobilnej i uczestniczenia w szkoleniu poprzez smartfon lub tablet.

Wymagania techniczne: procesor 2-rdzeniowy 2 GHz; 2 GB pamięci RAM; system operacyjny Windows 8 lub nowszy, MAC OS wersja 10.13; przeglądarka internetowa Google Chrome, Mozilla Firefox lub Safari; stałe łącze internetowe o prędkości 1,5 Mbps.

Konieczne jest posiadanie kamerki internetowej, umożliwiającej przeprowadzenie monitoringu realizacji usług szkoleniowych.

Najbezpieczniejszą opcją jest połączenie internetowe za pomocą kabla sieciowego. Gdy nie ma takiej możliwości i pozostaje korzystanie z WiFi, warto na czas szkolenia umieścić komputer jak najbliżej routera i zadbać, aby inni użytkownicy tej samej sieci WiFi ograniczyli w tym czasie aktywności mocno obciążające sieć (np. oglądanie filmów, rozmowy wideo lub pobieranie dużych plików). Jeśli jest taka możliwość zachęcamy do przetestowania połączenia w domu oraz miejscu pracy i uczestniczenia w szkoleniu z tego miejsca, w którym będzie lepszy Internet.

Jak dołączyć do spotkania: https://youtu.be/ZFWhNh2KHro, https://knowledge.clickmeeting.com/pl/infographic/jak-dolaczyc-do-wydarzenia-instrukcja-dla-uczestnika/

Link umożliwiający uczestnictwo w kursie ważny jest od dnia poprzedzającego rozpoczęcie kursu do zakończenia zajęć.

Kontakt

Anna Wilk

E-mail a.wilk@wektorwiedzy.pl

Telefon (+48) 17 2831 004