Możliwość dofinansowania

Master Biznes Centrum Kształcenia Personalnego Sławomir Bargiel

★★★★☆

BEZPIECZEŃSTWO W SIECI INTERNETOWEJ I NA STANOWISKU PC W PRAKTYCE DLA PRACOWNIKÓW. BANKOWOŚĆ INTERNETOWA – DOBRE PRAKTYKI. KRADZIEŻ TOŻSAMOŚCI – SPOSOBY ZABEZPIECZEŃ. ANALIZA CYBERATAKÓW – SPOSOBY MINIMALIZOWANIA ZAGROŻEŃ. STRONA FIRMOWA OPARTA NA CMS WORDPRESS – KOMPLEKSOWE ZABEZPIECZENIE SYSTEMU.

Numer usługi 2024/07/08/13353/2212501

1 800,00 PLN brutto
1 800,00 PLN netto
120,00 PLN brutto/h
120,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
15 h
16.09.2024 do 20.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Kurs przeznaczony jest dla osób początkujących, które wcześniej nie miały nic wspólnego z Cyberbezpieczeństwem.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	6
Data zakończenia rekrutacji	13-09-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	15
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Zdobycie wiedzy, umiejętności i kompetencji społecznych niezbędnych do efektywnego zarządzania cyberbezpieczeństwem w kontekście zawodowym i prywatnym. Rozwinięcie świadomości zagrożeń cybernetycznych i zdolności do ochrony danych i przeciwdziałania atakom cybernetycznym. Zdobycie praktycznych umiejętności niezbędnych do zabezpieczania systemów informatycznych. Rozwiną kompetencje społeczne, takie jak współpraca w zespole, komunikacja o zagrożeniach i odpowiedzialność za bezpieczeństwo w sieci.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA • Rozumienie podstaw cyberbezpieczeństwa: Uczestnik zna podstawowe pojęcia i zasady związane z cyberbezpieczeństwem. • Zrozumienie zagrożeń cybernetycznych: Uczestnik potrafi zidentyfikować różne rodzaje zagrożeń, takie jak wirusy, phishing, ataki DoS itp. • Zasady bezpiecznego korzystania z bankowości internetowej: Uczestnik zna najlepsze praktyki związane z bezpiecznym dostępem do bankowości internetowej. • Ochrona tożsamości cyfrowej: Uczestnik wie, jak chronić swoją tożsamość w sieci i jakie są objawy kradzieży tożsamości. • Podstawy zabezpieczeń stron internetowych WordPress: Uczestnik rozumie, jak zabezpieczyć stronę internetową opartą na CMS WordPress. • Znajomość technik socjotechnicznych: Uczestnik zna różne techniki socjotechniczne wykorzystywane przez cyberprzestępców.	Poprawna odpowiedź na 80% pytań.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
UMIEJĘTNOŚCI • Tworzenie i zarządzanie silnymi hasłami: Uczestnik potrafi tworzyć i zarządzać silnymi, unikalnymi hasłami. • Korzystanie z oprogramowania antywirusowego: Uczestnik umie zainstalować, skonfigurować i regularnie aktualizować oprogramowanie antywirusowe. • Konfiguracja bezpiecznych sieci WiFi: Uczestnik potrafi skonfigurować i zabezpieczyć sieć bezprzewodową. • Wykrywanie i unikanie phishingu: Uczestnik jest w stanie rozpoznać podejrzane emaile i linki oraz wie, jak unikać ataków phishingowych. • Szyfrowanie dokumentów i danych: Uczestnik umie szyfrować ważne pliki i dokumenty. • Zarządzanie stroną internetową WordPress: Uczestnik potrafi zastosować podstawowe zasady bezpieczeństwa w celu zabezpieczenia strony opartej o CMS WordPress. • Rozpoznawanie i przeciwdziałanie socjotechnice: Uczestnik potrafi rozpoznać techniki socjotechniczne i wie, jak na nie reagować.	Poprawna odpowiedź na 80% pytań. Zadanie do wykonania.	Test teoretyczny Prezentacja
KOMPETENCJE SPOŁECZNE • Świadomość znaczenia cyberbezpieczeństwa: Uczestnik rozumie znaczenie ochrony danych zarówno w kontekście zawodowym, jak i prywatnym. • Odpowiedzialność za bezpieczeństwo w sieci: Uczestnik jest świadomy swojej roli i odpowiedzialności za bezpieczeństwo danych w organizacji. • Współpraca w zespole: Uczestnik potrafi efektywnie współpracować z innymi pracownikami w celu utrzymania bezpieczeństwa cyfrowego w firmie. • Komunikacja o zagrożeniach: Uczestnik umie komunikować się z zespołem na temat zagrożeń i incydentów bezpieczeństwa.	Obserwacja podejmowanych kroków podczas symulacji incydentów bezpieczeństwa - reagowanie zgodne z programem nauki.	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

Dokładny harmonogram (następna zakładka) szkolenia będzie dostosowany do preferencji uczestników.

Usługa liczona w godzinach lekcyjnych (45 min.).

Moduł 1: Cyberbezpieczeństwo na stanowisku pracy i w życiu prywatnym

- **Wprowadzenie do cyberbezpieczeństwa**: Definicja cyberbezpieczeństwa, znaczenie ochrony danych w kontekście zawodowym i osobistym.
- **Rodzaje zagrożeń cyberbezpieczeństwa**: Omówienie różnych typów zagrożeń, takich jak złośliwe oprogramowanie, phishing, ataki DoS itp.
- **Techniki przeciwdziałania zagrożeniom**:
  - **Silne hasła**: Tworzenie i utrzymywanie unikalnych, silnych haseł.
  - **Oprogramowanie antywirusowe**: Instalacja i regularna aktualizacja programów antywirusowych.
  - **Aktualizacja oprogramowania**: Znaczenie regularnych aktualizacji systemów operacyjnych i aplikacji.
  - **Dwuskładnikowe uwierzytelnianie**: Korzyści z używania dwuskładnikowej autoryzacji.
  - **Bezpieczeństwo sieci WiFi**: Konfiguracja i zabezpieczenie sieci bezprzewodowych.
  - **Tworzenie kopii zapasowych**: Regularne backupy danych.
  - **Bezpieczeństwo linków i załączników**: Jak rozpoznawać i unikać podejrzanych linków i załączników.
  - **Phishing**: Techniki rozpoznawania i unikania phishingu.
  - **Aktualne oprogramowanie systemowe**: Znaczenie aktualizacji systemowych dla bezpieczeństwa.

Moduł 2: Cyberbezpieczeństwo w firmowym dostępie do bankowości internetowej

- **Zasady tworzenia i zarządzania hasłami**.
- **Bezpieczne połączenie z bankiem**: Upewnij się, że strona banku używa bezpiecznego połączenia (https://) i sprawdź certyfikat SSL.
- **Korzystanie z zaufanych urządzeń**: Unikaj logowania się do konta bankowego z publicznych lub niezaufanych komputerów i sieci.
- **Uwierzytelnianie dwuskładnikowe**: Aktywuj uwierzytelnianie dwuskładnikowe (2FA) dla dodatkowej warstwy zabezpieczeń.
- **Powiadomienia o transakcjach**: Włącz powiadomienia SMS lub email o każdej transakcji, aby szybko reagować na podejrzane aktywności.
- **Bezpieczne oprogramowanie bankowe**: Korzystaj z oficjalnych aplikacji bankowych, regularnie je aktualizuj i unikaj nieautoryzowanych źródeł.
- **Unikanie publicznych sieci WiFi**: Unikaj logowania się do bankowości internetowej przez publiczne WiFi; jeśli konieczne, używaj VPN.
- **Ochrona przed phishingiem**: Nigdy nie klikaj linków w nieznanych wiadomościach email lub SMS-ach, które twierdzą, że są od banku. Zawsze bezpośrednio wpisuj adres URL banku w przeglądarce.
- **Monitorowanie konta bankowego**: Regularnie sprawdzaj wyciągi bankowe i historię transakcji, aby szybko wykryć nieautoryzowane operacje.

Moduł 3: Dobre praktyki w zakresie cyberbezpieczeństwa

- **Zarządzanie poufnymi informacjami**: Najlepsze praktyki dotyczące ochrony informacji w miejscu pracy.
- **Zasady bezpiecznej obsługi komputera**: Ochrona danych poprzez bezpieczne użytkowanie komputerów.
- **Przechowywanie haseł**: Metody bezpiecznego przechowywania haseł.
- **Szyfrowanie dokumentów**: Techniki szyfrowania wrażliwych dokumentów.
- **Bezpieczne przechowywanie haseł**: Procedury szyfrowania haseł na wypadek kradzieży lub zgubienia.

- **Bezpieczne użytkowanie nośników danych**: Postępowanie z przypadkowo znalezionymi dyskami zewnętrznymi i pendrive'ami.

Moduł 4: Cyberbezpieczeństwo w aspekcie kradzieży tożsamości.

- **Ochrona tożsamości**: Jak zapobiegać kradzieży tożsamości i co robić w przypadku jej utraty:
  - **Rozpoznawanie kradzieży tożsamości**: Objawy kradzieży tożsamości, takie jak nieznane transakcje na koncie bankowym, niespodziewane odmowy kredytowe lub otrzymywanie korespondencji z nieznanych źródeł.
  - **Ochrona danych osobowych**: Unikaj udostępniania danych osobowych, takich jak numer PESEL, czy numer dowodu osobistego.
  - **Bezpieczne przechowywanie dokumentów**: Przechowywanie dokumentów zawierających dane osobowe w bezpiecznym miejscu; niszczenie dokumentów zawierających wrażliwe informacje przed ich wyrzuceniem.
  - **Szyfrowanie danych**: Szyfrowanie ważnych plików i dokumentów przechowywanych na komputerze lub w chmurze.
  - **Bezpieczne korzystanie z mediów społecznościowych**: Ograniczanie ilości udostępnianych informacji osobowych na profilach społecznościowych oraz ustawienia prywatności.
  - **Ochrona urządzeń mobilnych**: Korzystanie z funkcji blokady ekranu, szyfrowanie urządzeń mobilnych, regularne aktualizacje systemu i aplikacji oraz unikanie instalowania aplikacji z nieznanych źródeł.
  - **Monitorowanie kredytu**: Regularne sprawdzanie raportów kredytowych w celu wykrycia nieautoryzowanych działań.
  - **Reagowanie na kradzież tożsamości**: Kroki, które należy podjąć w przypadku podejrzenia kradzieży tożsamości, takie jak zgłoszenie sprawy do odpowiednich instytucji, kontakt z bankiem oraz zmiana haseł i danych logowania.
- **Bezpieczeństwo w mediach społecznościowych**: Najlepsze praktyki dotyczące prywatności i bezpieczeństwa na platformach społecznościowych.

Moduł 5: Socjotechnika

- **Wprowadzenie do socjotechniki**: Definicja socjotechniki i jej znaczenie w kontekście cyberbezpieczeństwa.
- **Techniki socjotechniczne**: Omówienie różnych technik wykorzystywanych przez cyberprzestępców, takich jak phishing, pretexting, baiting, tailgating, vishing i inne.
- **Rozpoznawanie prób socjotechnicznych**: Jak rozpoznawać i reagować na próby manipulacji i oszustw socjotechnicznych.
- **Bezpieczna komunikacja**: Najlepsze praktyki dotyczące bezpiecznej komunikacji z nieznanymi osobami oraz weryfikacja tożsamości rozmówców.
- **Szkolenie pracowników**: Znaczenie regularnych szkoleń z zakresu socjotechniki dla pracowników i sposoby ich przeprowadzania.
- **Studium przypadków**: Analiza rzeczywistych przypadków ataków socjotechnicznych, ich skutków i metod obrony.

Moduł 6: Analiza cyberataków – studium przypadku

- **Analiza przypadków**: Studium rzeczywistych incydentów bezpieczeństwa, analiza przyczyn i skutków.
- **Plan reagowania na incydenty**: Kroki, które należy podjąć po wykryciu cyberataku, współpraca z zespołem IT i organami ścigania.
- **Raportowanie incydentów**: Dokumentowanie incydentów bezpieczeństwa, zgłaszanie naruszeń do odpowiednich instytucji.

Moduł 7: Zabezpieczenie stron internetowych opartych na CMS WordPress

- **Podstawy bezpieczeństwa WordPress**: Aktualizacje systemu, wtyczki i motywy, zarządzanie użytkownikami.
- **Szyfrowanie i certyfikaty SSL**: Konfiguracja certyfikatów SSL i znaczenie szyfrowania komunikacji.
- **Zarządzanie uprawnieniami**: Ograniczanie dostępu do panelu administracyjnego, zasady tworzenia kont użytkowników.
- **Kopie zapasowe i odzyskiwanie danych**: Tworzenie regularnych kopii zapasowych strony i procedury odzyskiwania danych.
- **Monitorowanie i audyty bezpieczeństwa**: Regularne skanowanie strony pod kątem zagrożeń, przeprowadzanie audytów bezpieczeństwa.

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 usługi brutto	1 800,00 PLN
Koszt usługi netto	1 800,00 PLN
Koszt godziny brutto	120,00 PLN
Koszt godziny netto	120,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Sławomir Bargiel

Tworzy stron internetowe w oparciu o własne szablony do systemu CMS (Joomla) oraz Wordpress, programista (HTML CSS, Java Script, React, Angular, PHP). Specjalista w zakresie bezpieczeństwa IT, SEO oraz reklamy Google Ads. Doświadczenie zawodowe z ww. tematów zdobywa od 18 lat . Od ponad 15 lat trener oraz właściciel firmy szkoleniowej Master Biznes Centrum Kształcenia Personalnego. Przed założeniem firmy szkoleniowej pracował jako specjalista w zakresie utrzymania i rozbudowy serwisów internetowych oraz bezpieczeństwa IT. Zajmował się reklamą Google AdWords (poprzednia nazwa obecnej nazwy Google Ads) oraz pozycjonował strony internetowe (SEO). Posiada 15 letnie doświadczenie w szkoleniach z obszaru IT, twórca programów szkoleniowych, tworzy autorskie materiały szkoleniowe oparte o gotowe szablony symulacji działania kodu danego języka programowania.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe formie elektronicznej zawierają:

- Plik pdf zawierający opis prezentowanych zagadnień.
- Prezentacja treści merytorycznej kursu programie PowerPoint.
- Skrypty kodu HTML, CSS oraz Java Script do lekcji związanych z tymi zagadnieniami.

Warunki uczestnictwa

Wymagania wstępne odnośnie uczestnika kursu:

- Podstawowa znajomość obsługi komputera.
- Podstawowa znajomość edytora tekstu - Microsoft Word.

Wymagania wstępne. Walidacja spełnienia tego kryterium będzie polegać na rozmowie kwalifikacyjnej z uczestniczką/kiem kursu sprawdzającej umiejętności odnośnie podstawowej znajomości obsługi komputera oraz edytora tekstu (Microsoft Word).

Informacje dodatkowe

Usługa liczona w godzinach lekcyjnych (45 min.).

Warunki techniczne

Kurs będzie przeprowadzany w formie zdalnej na żywo (video i audio) na platformie ClickMeeting.

Wymagania sprzętowe:

- Stabilny dostęp do Internetu.
- Prędkość łącza (pobieranie/przesyłanie) - min. 2 Mbps.
- Komputer z systemem Windows (7,8,10,11) wyposażony w kamerkę internetową i mikrofon.
- Przeglądarka internetowa.

Kontakt

Sławomir Bargiel

E-mail edu@masterbiznes.pl

Telefon (+48) 509 229 182