Możliwość dofinansowania

Bezpieczny Pracownik Basic (forma zdalna)

Numer usługi 2024/11/07/166538/2401255

553,50 PLN brutto
450,00 PLN netto
138,38 PLN brutto/h
112,50 PLN netto/h

EXIMO PROJECT SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
4 h
20.12.2024 do 20.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie jest skierowane do wszystkich, którzy chcą poszerzyć swoją wiedzę na temat bezpiecznego użytkowania Internetu oraz dla Pracodawców, którzy chcą poprawić poziom cyberbezpieczeństwa w swojej firmie.
Minimalna liczba uczestników	12
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	18-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	4
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest wyposażenie uczestników w niezbędną wiedzę, umiejętności i postawy niezbędne do skutecznego radzenia sobie z cyberzagrożeniami oraz rozwój bezpieczeństwa w środowisku online.

To skondensowane szkolenie zapewni uczestnikom solidne podstawy w zakresie identyfikacji i reagowania na cyberzagrożenia, a także praktyczne umiejętności potrzebne do ochrony swoich danych i infrastruktury IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zrozumie podstawowe pojęcia związane z cyberzagrożeniami, takie jak: phishing, scam, ransomware.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik pozyska wiedzę na temat statystyk oraz przykładów znaczących incydentów cybernetycznych.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik będzie potrafił rozpoznawać podstawowe zagrożenia cybernetyczne.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Uczestnik zdobędzie praktyczne umiejętności w obszarze bezpieczeństwa poczty elektronicznej, zabezpieczania urządzeń mobilnych, korzystania z publicznych sieci bezprzewodowych i tworzenia bezpiecznych haseł.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik będzie gotów do stałego podnoszenia świadomości w zakresie cyberbezpieczeństwa.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik kształtuje postawę gotowości do skutecznego reagowania w sytuacjach kryzysowych, posiadając opanowane podstawowe kroki w przypadku ataku lub naruszenia bezpieczeństwa.	Samodzielna praca w środowisku wirtualnym	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

- Szkolenie realizujemy także w formie **zamkniętej dla poszczególnych firm**. Termin, cenę i liczbę osób w grupie ustalamy wówczas **indywidualnie**. Modyfikujemy wówczas program tak, aby trafił w specyfikę, potrzeby i sytuację firmy. Program możemy rozszerzyć o testy phishingowe, które pomogą w identyfikacji słabych punktów i zbudowaniu świadomości pracowników. Napisz na: **szkolenia@eximoproject.pl**, aby dowiedzieć się więcej :)

Wprowadzenie

1. Przywitanie uczestników.
2. Cel szkolenia – podkreślenie znaczenia świadomości cyberbezpieczeństwa.
3. Pre-test.
4. Przedstawienie statystyk dotyczących cyberataków na firmy i pracowników oraz wskazanie motywów hakerów.

Rozpoznawanie i reagowanie na techniki socjotechniczne

1. Definicja i przykłady technik socjotechnicznych:

   - Phishing: identyfikacja fałszywych e-maili i linków.

   - Scam: rozpoznawanie oszustw i manipulacji.

   - Ransomware: zrozumienie zagrożenia i środków zapobiegawczych.

2. Rzeczywiste przykłady ataków i ich skutki dla firm.

Dobre praktyki w cyberbezpieczeństwie

1. Bezpieczeństwo w obsłudze poczty elektronicznej:

   - Jak rozpoznać i unikać phishingu i scamu?

   - Zabezpieczenie urządzeń mobilnych: najlepsze praktyki.

   - Korzystanie z publicznych sieci bezprzewodowych: potencjalne zagrożenia i zasady bezpiecznego użytkowania.

2. Jak stosować bezpieczne hasła?

   - Tworzenie i zarządzanie hasłami.

   - Wieloetapowa weryfikacja dostępu do konta.

Podsumowanie i procedury na wypadek incydentów

1. Podsumowanie kluczowych punktów szkolenia.

2. Schemat działania dla sytuacji kryzysowych:

   - Kto kontaktować w przypadku podejrzenia naruszenia bezpieczeństwa.

   - Procedury reagowania na incydenty bezpieczeństwa.

Zakończenie

1. Sesja pytań i odpowiedzi.

2. Post-test.

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 przypadający na 1 uczestnika brutto	553,50 PLN
Koszt przypadający na 1 uczestnika netto	450,00 PLN
Koszt osobogodziny brutto	138,38 PLN
Koszt osobogodziny netto	112,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Damian Wierzyński

Damian Wierzyński – ma za sobą 10 lat doświadczenia w oswajaniu pracowników nietechnicznych z tajnikami technologii. Potrafi opowiedzieć o tych skomplikowanych sprawach w taki sposób, że nikt nie wyjdzie ze szkolenia bez większej wiedzy. Jego specjalnością jest cyberbezpieczeństwo, infrastruktura sieciowa, systemy zabezpieczeń i rozwiązania Microsoftu.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- Szkolenie będzie prowadzone w formie wykładu z analizą studiów przypadku. Elementem wykładu będą dyskusje z uczestnikami, a także quizy i testy wiedzy.
- W trakcie szkolenia zostaną wykorzystane: interaktywne prezentacje z wykorzystaniem rzeczywistych przykładów i statystyk.
- Prowadzący będzie korzystał z materiałów dydaktycznych takich jak: prezentacja multimedialna.

- Po zakończonym szkoleniu uczestnik otrzyma materiały dydaktyczne w formie elektronicznej (dostęp do materiałów autorskich, przygotowanych przez trenera, przesłane na adres e-mail uczestnika).

Informacje dodatkowe

- Jedna godzina szkoleniowa to 45 minut.
- Przewidujemy przerwy w szkoleniu (ok. 15 minut), dostosowane do grupy uczestników. Przerwy nie są wliczone do czasu szkolenia.
- Szkolenie prowadzone jest w języku polskim, materiały przekazane do doskonalenia wiedzy także są opracowane w tym języku.
- Zleceniodawca ma prawo zgłosić reklamację z tytułu niewykonania lub nienależytego wykonania usługi szkoleniowej. Termin składania reklamacji wynosi 14 dni roboczych, licząc od dnia, w którym usługa została zakończona lub miała zostać zakończona.
- Zleceniobiorca ma 14 dni roboczych na rozpatrzenie reklamacji; w przypadkach wymagających dodatkowych czynności wyjaśniających, czas rozpatrywania reklamacji może ulec wydłużeniu maksymalnie do 30 dni roboczych.
- Reklamacja powinna zostać przekazana mailowo na adres: support@eximoproject.pl.

Warunki techniczne

Komunikator: Usługa będzie prowadzona za pośrednictwem platformy Microsoft Teams.

Sprzęt: Uczestnik potrzebuje komputera z aktualnym systemem operacyjnym Microsoft Windows lub macOS.

Łącze internetowe: Uczestnik powinien dysponować łączem internetowym o przepustowości minimum 10Mbit.

Informacje organizacyjne: Uczestnik na tydzień przed planowanym szkoleniem otrzyma maila organizacyjnego, zawierającego szczegółową instrukcję dołączenia do sesji szkoleniowej na platformie MS Teams.

Kontakt

Marika Ptak-Broczek

E-mail szkolenia@eximoproject.pl
Telefon (+48) 52 5684 420