



Bezpieczny Pracownik Basic

Numer usługi 2024/07/19/166538/2228439

627,30 PLN brutto

510,00 PLN netto

156,83 PLN brutto/h

127,50 PLN netto/h

EXIMO PROJECT
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ

Brak ocen dla tego dostawcy

📍 Bydgoszcz / stacjonarna

🛠 Usługa szkoleniowa

🕒 4 h

📅 12.09.2024 do 12.09.2024

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	15
Data zakończenia rekrutacji	10-09-2024
Forma prowadzenia usługi	stacjonarna
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.	Samodzielną pracę w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik pozyska wiedzę na temat statystyk oraz przykładów znaczących incydentów cybernetycznych.	Samodzielną pracę w środowisku wirtualnym	Obserwacja w warunkach symulowanych
Uczestnik będzie potrafił rozpoznawać podstawowe zagrożenia cybernetyczne.	Samodzielną pracę 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.	Samodzielną pracę w środowisku wirtualnym	Obserwacja w warunkach symulowanych
• Uczestnik będzie gotów do stałego podnoszenia świadomości w zakresie cyberbezpieczeństwa.	Samodzielną pracę 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.	Samodzielną pracę 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	627,30 PLN
Koszt przypadający na 1 uczestnika netto	510,00 PLN
Koszt osobogodziny brutto	156,83 PLN
Koszt osobogodziny netto	127,50 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2

MARCIN CHLEBOWSKI

Marcin Chlebowski - Współzałożyciel i CEO Eximo Project, firmie specjalizującej się w integracji systemów informatycznych oraz projektującej rozwiązania z zakresu bezpieczeństwa informatycznego.

Specjalista z zakresu bezpieczeństwa IT (CCIE #21714 Security) i technologii sieciowych. Prowadzi szkolenia z zakresu cyberbezpieczeństwa od siedmiu lat. Zrealizował kilkadziesiąt projektów szkoleniowych, a spod jego skrzydeł wyszło kilka tysięcy uczestników szkoleń.



2 z 2

Damian Wierzyński

Damian Wierzyński – ma za sobą 10 lat doświadczenia w oswojaniu 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, flipchart.
- 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. 20 minut), dostosowane do grupy uczestników. Przerwy nie są wliczone do czasu szkolenia.
- Firma zapewnia dostęp do napojów (kawa, woda, herbata) i przekąsek.
- 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.

Adres

Bydgoszcz

Bydgoszcz

woj. kujawsko-pomorskie

Firma szkoleniowa zapewnia przerwy kawowe, z dostęp do napojów i przekąsek.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Udogodnienia dla osób ze szczególnymi potrzebami

Kontakt



Marika Ptak

E-mail eximo@eximoproject.pl

Telefon (+48) 52 5684 420