MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

Warszawa, dnia 06 września 2021 r.

BIURO CYBERBEZPIECZEŃSTWA
BC-II.133.1.2021

Zaproszenie do złożenia oferty na przeprowadzenie serii szkoleń z zakresu cyberbezpieczeństwa dla pracowników.

Zamawiający – Ministerstwo Sprawiedliwości zaprasza do złożenia oferty na przeprowadzenie serii szkoleń z zakresu cyberbezpieczeństwa dla pracowników.

W ramach rozeznania rynku oraz w celu oszacowania wartości zamówienia, w tym kosztów realizacji zamówienia, Ministerstwo Sprawiedliwości zaprasza Państwa do przesłania wstępnej kalkulacji ceny. W przedstawionej kalkulacji cenowej należy podać ceny netto i brutto w złotych, zgodnie z Formularzem Cenowym stanowiącym załącznik nr 2 do niniejszego zapytania.

Wymagania i warunki realizacji dotyczące przedmiotu zamówienia zostały określone w Opisie Przedmiotu Zamówienia – Załączniki nr 1 do niniejszego zaproszenia.

Ofertę cenową należy przedstawić zgodnie ze wzorem stanowiącym Załącznik nr 2 do Zaproszenia.

Ofertę należy złożyć w terminie do dnia 15 września 2021 r., do godz. 15:00, w formie elektronicznej format PDF, na adres Mariusz.Klimecki@ms.gov.pl oraz Damian.Madziala@ms.gov.pl

Zamawiający informuje, że przedmiotowe zaproszenie nie stanowi ofert w rozumieniu art. 66 KC, ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019, poz. 2019).

Załączniki:

1. Opis Przedmiotu Zamówienia
2. Formularz Cenowy

Opis Przedmiotu Zamówienia

I. Przedmiot zamówienia:

Przeprowadzenie serii szkoleń z zakresu cyberbezpieczeństwa dla pracowników.

II. Termin wykonania zamówienia:

1. Miejsce szkolenia:
   a) Ministerstwo Sprawiedliwości Al. Ujazdowskie 11, 00-950 Warszawa, sala wykładowa zostanie udostępniona przez Zamawiającego.
2. Zamawiający nie zapewnia transportu trenera/ trenerów na miejsce realizacji szkolenia.
3. Terminy szkoleń:
   a) Od dnia zawarcia umowy do dnia 20 grudnia 2022 roku.
   b) Wykonawca zaproponuje szczegółowy program szkoleń i przedstawi do akceptacji przez Zamawiającego.

III. Obowiązki Wykonawcy:

1. Opracowanie dedykowanych materiałów szkoleniowych wraz z określeniem form szkoleniowych (tj. warsztat, ćwiczenia, wykład, dyskusje, case study).
2. Opracowanie i uzgodnienie z Zamawiającym ostatecznego harmonogramu szkolenia i przedłożenie do akceptacji przez Zamawiającego.

IV. Obowiązki Zamawiającego:

1. Rekrutacja uczestników szkolenia.
2. Przygotowanie list obecności i przekazanie ich uczestnikom szkolenia do podpisu.
3. Rozdanie wśród uczestników, po zakończeniu szkolenia, Arkusza Indywidualnej Oceny Szkolenia.

V. Zakres i wymagania szczegółowe szkolenia:

1. Szkolenia zostaną przeprowadzone do dnia 20 grudnia 2022 roku.
2. W szkoleniach uczestniczyć będą pracownicy Zamawiającego.
3. Każdy uczestnik otrzyma dokument poświadczający ukończenie szkolenia.
4. Szkolenia muszą zostać przeprowadzone w języku polskim.
5. Wykonawca zobowiązuje się do zaproponowania co najmniej dwóch terminów każdego szkolenia z serii do wyboru przez Zamawiającego.
6. Cały cykl szkoleń powinien składać się z 8 wykładów.
7. Pojedynczy wykład powinien trwać 90 minut Dodatkowo należy uwzględnić 30 minut na udzielenie odpowiedzi na pytania oraz konsultacje z uczestnikami.
8. Zakres merytoryczny szkolenia musi obejmować minimalnie tematy wyszczególnione poniżej:

a) Przykłady ataków na firmy / pracowników [około 30 minut]

- Ataki na „dopłatę” do aukcji / przesyłki
- Podszywanie się pod znane w organizacji osoby
- Jak przestępcy wysyłają fałszywe faktury, powodując wysyłkę pieniędzy na własne konta?

b) Sprzęt prywatny a sprzęt firmowy – różnice w kontekście bezpieczeństwa [około 30 minut]

- Instalacja oprogramowania
- Poczta elektroniczna
- Praca z informacjami firmowymi
- Bezpieczne usuwanie danych z komputera prywatnego
- Podstawy szyfrowania danych

c) Jak i skąd atakujący zbierają dane [około 30 minut]

- Jak sprawdzić czy dane mojego konta wyciekły i jeśli tak, co zrobić?
- Jak minimalizować skutki wycieku danych?
- Czym może grozić wyciek danych?
- Mail z informacją, że Twoje hasło wyciekło – sposób postępowania

d) Zarządzanie hasłami oraz ich przechowywanie [około 30 minut]

- Praktyczna nauka korzystania z managerów haseł
- Tworzenie łatwych do zapamiętania, ale trudnych do złamania haseł
- Pokaz na żywo łamania słabego hasła
- Praktyczny pokaz korzystania z mechanizmów dwuskładnikowego uwierzytelnienia (2FA)

e) Bezpieczna praca z pakietem biurowym [około 30 minut]

- Złośliwe makra – co to jest / jak się chronić / przykłady ataków wykorzystujących makra
- Kradzież danych logowania i inne potencjalne ataki
- Bezpieczna konfiguracja pakietu biurowego

f) Bezpieczne korzystanie z urządzeń mobilnych (Android oraz iOS) [około 60 minut]

- Przykłady ataków na telefony komórkowe
- Czym jest SIM Swap, mogący skutkować wyczyszczeniem całego konta bankowego? Jak się przed nim chronić?
- Czy łatwo jest się podszyć pod dowolny numer GSM?
- Aktualizacje
- Szyfrowanie danych na smartfonie
- Konfiguracja poczty na smartfonie
- Korzystanie z szyfrowanej poczty na smartfonie
- Instalacja aplikacji
- Czy warto używać antywirusa na smartfona?

g) Bezpieczne korzystanie z poczty elektronicznej [około 30 minut]

- Podstawowa weryfikacja bezpieczeństwa konfiguracji programu pocztowego
- Poczta prywatna a bezpieczeństwo

h) Podstawowe zasady bezpieczeństwa pracy na komputerze [około 60 minut]

- Problemy i zagrożenia związane z nieaktualnym oprogramowaniem

- Czy warto zakrywać kamerę?
- Zasady instalacji zewnętrznego oprogramowania
- Drukowanie / skanowanie dokumentów w domu – kwestie bezpieczeństwa

i) Bezpieczna praca w przeglądarkach internetowych [około 30 minut]

- Podstawy zabezpieczenia „kłódką"/https przy korzystaniu z aplikacji webowych
- Przypadki, w których mimo widocznej w przeglądarce „kłódki", przestępca nadal może widzieć przesyłane dane
- Przed jakimi atakami chroni https, a przed jakimi nie?

j) Bezpieczne przechowywanie i usuwanie danych [około 30 minut]

- Jak przeprowadzić proces szyfrowania danych na komputerze oraz nośniku zewnętrznym?
- Czy łatwo odzyskać skasowane dane?
- Czy zwykłe usuwanie plików tak naprawdę usuwa ich zawartość?
- Nieodwracalne metody usuwania danych poufnych

k) Bezpieczne korzystanie z sieci bezprzewodowych [około 30 minut]

- Dlaczego nie warto podłączać się do sieci otwartych?
- Pokaz na żywo - łamanie hasła do słabo zabezpieczonej sieci bezprzewodowej
- Podstawowa konfiguracja domowego routera WiFi

l) Wprowadzenie do bezpieczeństwa dla kadry zarządzającej [około 90 minut]

- Wycieki danych – jak do nich dochodzi, jak zmniejszyć ryzyko skutecznego ataku?
- Nowoczesny ransomware – zmiana sposobu działania napastników. Co zrobić by zmniejszyć ryzyko ataku?
- Szyfrowanie danych na komputerach / nośnikach przenośnych
- Podstawy ataków socjotechnicznych – przegląd kilku realnych scenariuszy
- Zagrożenia wynikające ze świadomego / nieświadomego naruszania zasad bezpieczeństwa przez pracowników. Kilka prostych kroków zmniejszenia ryzyka.

m) Ataki socjotechniczne [około 90 minut]

- Omówienie podstaw psychologicznych stojących za socjotechniką, zwiększenie świadomości użytkowników przez analizę najnowszych realnych ataków
- Jak przestępcy poszukują danych na temat firmy i użytkowników oraz jak łatwo sprofilować ofiarę za pomocą informacji udostępnianych w Internecie.
- W jaki sposób są przeprowadzane ataki na pracowników firm za pomocą telefonu i rozmowy? Uczulenie użytkowników na potrzebę weryfikowania rozmówcy
- Na co zwracać uwagę podczas uruchamiania plików pobranych z Internetu? Czy antywirus zawsze jest skuteczny?
- Przedstawienie najpopularniejszych metod atakowania użytkowników, przykłady niebezpiecznych maili tworzonych przez przestępców oraz metody obrony przed nimi.

n) Bezpieczeństwo fizyczne [około 30 minut]

- Zabezpieczenia przed kradzieżą
- Zabezpieczenia przed podglądaniem i fotografowaniem ekranu
- Zabezpieczenia przed możliwością podłączenia urządzeń zewnętrznych

- Blokowanie zagubionych i skradzionych urządzeń i zdalne wymazywanie danych
- Hasło systemu BIOS

o) Propozycje tematów z zakresu cyberbezpieczeństwa [czas ustalany pomiędzy Stronami na etapie zgłaszania potrzeby]

- Potrzeby z zakresu edukacji w obszarze bezpieczeństwa IT zgłoszone przez Zamawiającego
- Wykonawca uzgadnia z Zamawiającym czy zgłoszony temat jest możliwy do realizacji (Wykładowca posiada odpowiednią wiedzę, posiada materiały z podanego zakresu)
- Potrzeba rozszerzenia tematyki szkoleń zgłaszana jest przez Zamawiającego przynajmniej jeden miesiąc przed planowanym terminem szkolenia

9. W ramach szkolenia trener:
   a) przeprowadzi szkolenie w miejscu i terminie ustalonym z Zamawiającym
   b) przeprowadzi szkolenie zgodnie z opracowanym programem w sposób aktywizujący uczestników szkolenia
   c) będzie odpowiadał na pytania uczestników szkolenia i poprowadzi dyskusję podczas szkolenia, konsultacje.

Załącznik nr 2
do zamówienia nr BC-II.133.1.2021

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

FORMULARZ CENOWY

Na realizację zamówienia - przeprowadzenie serii szkoleń
z zakresu cyberbezpieczeństwa dla pracowników.

I. DANE DOTYCZĄCE OFERENTA:

Nazwa podmiotu	
Adres siedziby	
Numer NIP	
Numer REGON	
Telefon kontaktowy	
Adres e-mail	

II. CAŁKOWITA SZACOWANA WARTOŚĆ ZAMÓWIENIA:

…… zł. brutto

Słownie: ……

…… zł. netto

Słownie: ……