



Instrukcja obsługi eduHEZO dla użytkownika



Oto 6 kroków koniecznych do pełnej satysfakcji z usługi eduHEZO!

Krok 1:

Rejestracja w portalu myHEZO

Naszą współpracę zaczynamy od rejestracji i założenia konta na portalu myHEZO pod adresem



Tutaj znajdziesz instrukcję rejestracji na portalu myHEZO.

Krok 2:

Przygotowanie listy użytkowników i uzgodnienia

Aby rozpocząć współpracę należy założyć pierwsze zgłoszenie w umowie związanej z zakupioną usługą na portalu myHEZO.pl

W odpowiedzi na zgłoszenie nasz koordynator skontaktuje się z Tobą oraz:

- prześle plik ankiety, którą należy wypełnić; informacje w niej zawarte będą potrzebne nam do ustalenia indywidualnego harmonogramu szkoleń
- poprosi o przesłanie listy użytkowników wraz z ich adresami mailowymi
Ważne: każdy użytkownik powinien posiadać własny adres mailowy – otrzyma na niego dedykowany link do szkoleń.
- przeprowadzi wywiad techniczny, w celu spersonalizowania części działań phishingowych skierowanych na użytkowników.

Krok 3:

Przygotowanie środowiska

Na tym etapie razem postaramy się pomóc zrekonfigurować sieć, by prowadzone działania były skuteczne, ale jednocześnie bezpieczne.

Składają się na to dwa elementy:

1. Uwierzytelnienie/weryfikacja domeny

Jest to krok mający na celu zweryfikowanie, że klient, dla którego będziemy świadczyć usługę szkoleniową (a także dokonywać phishing'u), jest pełnoprawnym właścicielem domeny. Stosujemy takie zabezpieczenie, aby w sytuacji pojawienia się jakiegokolwiek błędu lub „zamierzonego działania” podana domena byłaby właściwa, a nasze działania phishingowe nie trafiły do nieodpowiedniego adresata.

A. Dodać do wpisów DNS Twojej domeny nowy rekord tekstowy np.:

Type Name/Host/Alias	TXT @
Value/Answer/Definitions	ppe-6ccc6f80ab1ed7b0154022bcce641068af9eadd3
TTL	3600

B. Lub dodać tzw. META TAG do nagłówka we wpisach DNS o treści:

<meta name="ppe-verify" content="ppe-6ccc6f80ab1ed7b0154022bcce641068af9eadd3">

Nasi inżynierowie zawsze pomogą w konfiguracji tych wpisów w rekordach DNS u operatora Twojej domeny. Jeśli taka pomoc jest potrzebna – daj nam o tym znać.

1. Dodanie na firewallu (i innych zabezpieczeniach) adresów IP i domen wykorzystywanych do szkoleń i phishingu do whitelisty

Jest to działanie dające pewność, że szkolenia będą w pełni dostępne dla wszystkich, a wysyłane maile będą docierać do wszystkich wskazanych użytkowników.

Krok 4:

Ustalenie harmonogramu szkoleń

Nasz koordynator przekaze propozycję harmonogramów szkoleń wraz z ich podziałem na poszczególne tygodnie. Możesz zmienić kolejność, intensywność szkoleń, podział na grupy. Można także dokonać podziału uczestników na zespoły i przydzielić im różne szkolenia, w zależności od zakresu ich pracy.

Krok 5:

Ustalenie harmonogramu phishingu

Bardzo ważnym elementem procesu szkoleniowego jest weryfikacja umiejętności uczestników. W przypadku cyberzagrożeń najlepszą metodą jest sprawdzenie czujności użytkowników za pomocą spreparowanego maila, zawierającego podejrzany link, w którym nadawca podszywa się pod osobę z organizacji.

Na tym etapie ustalamy też terminy i formę sprawdzania oraz działania, jakie należy podjąć względem osób, które „złapały się” w pułapkę. Akcją może być ponowne skierowanie użytkownika na szkolenie z odpowiedniego zakresu.

Ustalimy również treść komunikacji jakiej będziemy używać, aby była ona jak najbardziej dopasowana do środowiska klienta.

Krok 6:

Rozpoczęcie procesu szkoleniowego

W tym kroku, wykonujemy trzy działania:

- › wysyłamy wstępny phishing do uczestników, by zbadać poziom zaufania.
- › Koordynator po Twojej stronie wysyła wiadomość inicjującą proces do wszystkich uczestników kursu z oficjalną informacją o inicjatywie szkoleniowej – otrzymasz od nas przykłady takich treści.
- › z poziomu platformy każdy użytkownik dostanie maila z unikalnym linkiem do szkoleń, wraz z krótką instrukcją i informacją.

Treść tego powiadomienia również będzie ustalana i omawiana w kroku 4.

Co tydzień (lub w innym odstępie czasu – w zależności od ustaleń) będą wysyłane wiadomości kończące i podsumowujące poszczególne okresy oraz powiadomienia o nowych modułach szkoleniowych.

Krok 7:

Raportowanie

W trakcie procesu szkoleniowego będziemy przygotowywać i udostępniać Twojemu koordynatorowi listę użytkowników, którzy wykonali szkolenia, podsumowania i tabele zawierające szczegółowe informacje takie jak:

- › wynik testu dla poszczególnych szkoleń,
- › wynik testu dla poszczególnych uczestników,
- › ranking użytkowników,
- › listę uczestników i listę nieobecności.

Będziemy także udostępniać wyniki poszczególnych etapów phishing w tym:

- › listę osób, które otworzyły wiadomość,
- › listę osób, które kliknęły link,
- › listę osób, które kliknęły link wielokrotnie,
- › czas oraz adres IP, z którego osoby się łączyły,
- › statystyki otwarć,
- › czas otwarcia i kliknięcia.

Są to informacje pozwalające na weryfikację i analizę postępów oraz wiedzy uczestników.

Całość cyklu szkoleniowego kończy się ogólnym raportem zbiorczym.



Instrukcja obsługi eduHEZO dla użytkownika



all of
security