Możliwość dofinansowania

CYBER+ Phishing dla Pracowników (grupa zamknięta do 20 osób) 4h - (S_54383) - online

Numer usługi 2026/02/26/7629/3365136

3 567,00 PLN brutto
2 900,00 PLN netto
891,75 PLN brutto/h
725,00 PLN netto/h
261,33 PLN cena rynkowa

ASSECO DATA SYSTEMS SPÓŁKA AKCYJNA

4,4 / 5

156 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
04:00 h
30.06.2026 do 30.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie realizowane dla grupy zamkniętej do 20 osób. Cena obejmuje całą grupę. • Pracownicy biurowi (nie-IT) • Pracownicy Jednostek samorządu terytorialnego • Pracownicy Uczelni wyższych • Pracownicy Podmiotów kluczowych i istotnych w rozumieniu NIS2
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	22-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	4
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Skupiając się na realnych scenariuszach ataków phishingowych oraz aktualnych metodach wykorzystywanych przez cyberprzestępców, szkolenie rozwija świadomość zagrożeń cyfrowych, doskonali umiejętność rozpoznawania prób

wyłudzeń oraz wzmacnia odpowiedzialne postawy w zakresie ochrony informacji. Celem szkolenia jest zwiększenie odporności organizacji na ataki socjotechniczne poprzez podniesienie wiedzy, umiejętności praktycznych i kompetencji społecznych pracowników.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik wyjaśnia mechanizmy działania phishingu oraz jego najczęstsze odmiany	• Rozróżnia phishing, spear phishing, smishing i vishing. • Opisuje podstawowy schemat ataku phishingowego. • Wskazuje możliwe skutki ataku dla organizacji.	Test teoretyczny
WIEDZA: Uczestnik identyfikuje czynniki psychologiczne wykorzystywane w atakach socjotechnicznych.	• Wskazuje przykłady technik manipulacyjnych. • Wyjaśnia wpływ presji czasu na decyzje użytkownika. • Rozpoznaje elementy budujące fałszywe poczucie autorytetu.	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik potrafi rozpoznać próbę phishingu w wiadomości elektronicznej.	• Analizuje adres nadawcy i domenę. • Identyfikuje podejrzane linki i załączniki. • Wskazuje błędy językowe i niespójności.	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik prawidłowo reaguje na podejrzane komunikaty zgodnie z zasadami bezpieczeństwa.	• Wskazuje poprawną sekwencję działań w przypadku kliknięcia w link. • Rozpoznaje konieczność niezwłocznego zgłoszenia incydentu. • Odróżnia bezpieczne zachowanie od ryzykownego.	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik przyjmuje odpowiedzialną postawę wobec bezpieczeństwa informacji.	• Rozumie swoją rolę w systemie bezpieczeństwa. • Wykazuje gotowość do zgłaszania incydentów. • Działa zgodnie z zasadą ograniczonego zaufania.	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik wykazuje czujność i krytyczne myślenie wobec nieoczekiwanych komunikatów.	• Analizuje komunikat przed podjęciem działania. • Wstrzymuje reakcję w sytuacji presji. • Konsultuje wątpliwości z właściwą osobą.	Test teoretyczny

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

MODUŁ I. Współczesne zagrożenia, dezinformacja i realne incydenty

1. 1. Wykorzystywanie sztucznej inteligencji (AI) w dezinformacji i oszustwach internetowych – przykłady
   2. Dezinformacja i fake news. Jak się bronić?
   3. Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa:

   - Jakie mamy obowiązki w naszej organizacji związane z ochroną informacji np. RODO, KRI, KSC, …?
   - Czy RODO jeszcze działa?
   - Czy dyrektywa NIS2 i nowa ustawa o KSC nas dotyczą i jakie nakładają obowiązki?
   - Wewnętrzne polityki procedury bezpieczeństwa to też prawo

   1. Budowanie kultury bezpieczeństwa (świadomości) jest kluczowe dla każdej organizacji

   - Od czego zacząć
   - Czy człowiek to najsłabsze ogniwo?
   - Rola kadry zarządzającej w budowaniu świadomości

   1. Co kontrolerzy NIK zobaczyli w urzędach i dlaczego wnioski z tych kontroli mogą dotyczyć naszej organizacji?

MODUŁ II. Incydenty i aktualne zagrożenia w cyberprzestrzeni

1. 1. Incydenty bezpieczeństwa

   - Co to jest incydent?
   - Kiedy i komu zgłaszać incydenty?
   - Rejestr incydentów jako narzędzie zapewnienia ochrony informacji
   - Dlaczego warto zgłaszać incydenty?
   - Dlaczego warto zgłaszać incydenty do CERTu?

   1. Aktualne zagrożenia w cyberprzestrzeni

   - Typy ataków / główne cyberzagrożenia / schematy działania cyberprzestępców
   - Kradzieże i wyłudzenia informacji – przykłady z polskich organizacji
   - Jak się bronić?

MODUŁ III. Bezpieczna praca i cyberhigiena w praktyce

1. 1. Bezpieczna praca zdalna – dobre praktyki

   - Zagrożenia dla urządzeń mobilnych i zasady bezpiecznego korzystania
   - Szyfruj komunikację i dane tam, gdzie tylko można

   1. Proste i skuteczne metody codziennej ochrony informacji przez pracowników – zasady cyberhigieny

   - Kopia bezpieczeństwa wg zasady „3-2-1”
   - Aktualizacja systemów i programów
   - Czy chmurze można zawsze ufać?

- Szyfrowanie danych jako jedyna skuteczne metoda zachowania poufności
- Używaj dwuskładnikowego uwierzytelnienia (MFA) zawsze …, jeśli jest to możliwe

1. Audyty i testy bezpieczeństwa mają sens, ponieważ lepiej sprawdzić własne zabezpieczenia zanim … zrobią to cyberprzestępcy

- Rodzaje testów bezpieczeństwa
- Korzyści z testów
- Jak przygotować pracowników i organizację do testów socjotechnicznych?

MODUŁ IV. Ochrona dostępu i tożsamości cyfrowej

1. 1. Zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych

- Pamiętaj hasło do poczty e-mail
- Szyfrowanie załączników do e-maili
- Korzystanie w „UDW”

1. Bezpieczne hasła do Twoich systemów:

- Jak tworzyć silne hasła?
- Jakie hasła musimy mieć zawsze „w głowie”?
- Menedżery haseł jako właściwe narzędzie do skutecznego zarządzania hasłami – przykłady

1. Dwuskładnikowe uwierzytelnienie (2FA/MFA) to już standard w pracy i życiu prywatnym

- Smsy, aplikacje, klucze sprzętowe (U2F)
- Należy lepiej zabezpieczać konta szczególnie istotne dla organizacji

1. Wycieki i kradzieże haseł

- Jak sprawdzić, czy moje hasła wyciekły? Przykładowe serwisy
- Co zrobić, gdy moje hasła wyciekną?

1. Phishing i Ransomware jako największe zagrożenia dla każdej organizacji

- Dlaczego ataki typu ransomware są tak niebezpieczne? Konsekwencje dla organizacji
- Spoofing, Phishing, Smishing, Vishing, …
- Jak odróżnić fałszywą korespondencję e-mail przychodzącą do naszej organizacji?
- Jak sprawdzić czy otrzymany link lub załącznik jest bezpieczny? Przykładowe narzędzia

1. Metadane w dokumentach BIP. Czy są cenne dla cyberprzestępców?

MODUŁ V. Systemowe podejście do bezpieczeństwa informacji

1. 1. Jak wdrażać System Zarządzania Bezpieczeństwem Informacji (SZBI) np. wg normy ISO 27001?
   2. Polityki Bezpieczeństwa Informacji (PBI) oraz procedury i instrukcje jako skuteczne narzędzie ochrony informacji

Harmonogram

Liczba pozycji harmonogramu: 5

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 MODUŁ I. Współczesne zagrożenia, dezinformacja i realne incydenty	Trener Asseco Academy	30-06-2026	10:00	11:00	01:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 5 MODUŁ II. Incydenty i aktualne zagrożenia w cyberprzestrzeni	Trener Asseco Academy	30-06-2026	11:00	11:30	00:30
3 z 5 MODUŁ III. Bezpieczna praca i cyberhigiena w praktyce	Trener Asseco Academy	30-06-2026	11:30	12:30	01:00
4 z 5 MODUŁ IV. Ochrona dostępu i tożsamości cyfrowej	Trener Asseco Academy	30-06-2026	12:30	13:15	00:45
5 z 5 MODUŁ V. Systemowe podejście do bezpieczeństwa informacji	Trener Asseco Academy	30-06-2026	13:15	14:00	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 567,00 PLN
Koszt przypadający na 1 uczestnika netto	2 900,00 PLN
Koszt osobogodziny brutto	891,75 PLN
Koszt osobogodziny netto	725,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Trener Asseco Academy

Trener z co najmniej 5 letnim doświadczeniem w prowadzeniu szkoleń, w tym z obszaru merytorycznego, którego dotyczy. W przypadku szkoleń akredytowanych i autoryzowanych nasi trenerzy posiadają stosowne uprawnienia do ich prowadzenia.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W cenie pakietu uczestnik otrzymuje

- Udział w 4-godzinnym szkoleniu CYBER+ Phishing dla Pracowników prowadzonym na żywo przez trenera eksperta ds. cyberbezpieczeństwa
- Komplet materiałów szkoleniowych w wersji elektronicznej
- Roczny dostęp do nagranego szkolenia wyłącznie dla pracowników organizacji
  - Zaświadczenie Asseco Academy o ukończeniu szkolenia.
  - Cena szkolenia dla 1 uczestnika została skalkulowana przy założeniu realizacji szkolenia dla grupy zamkniętej 20-osobowej

Organizacja szkolenia CYBER+ Phishing dla Pracowników

- Rodzaj szkolenia: dla grup zamkniętych
- Forma realizacji: zdalnie; więcej informacji: Formy Szkoleń Asseco Academy
- Język szkolenia: polski
- Język materiałów: polski
- Termin szkolenia do uzgodnienia z zamawiającym.

Opcja dodatkowo płatna: eLearning W obronie przed cyberatakami

- Rodzaj szkolenia: dla grup zamkniętych
- Forma realizacji: Roczny dostęp do eLearningu na Platformie Asseco Academy
- Język szkolenia: polski
- Język materiałów: polski

Organizacja szkolenia w Wirtualnej Klasie

- Szkolenie realizowane w godzinach 10:00-14:00 lub w innych ustalonych z Zamawiającym.
- Każdy uczestnik powinien dokonać rejestracji do zdalnej sesji szkoleniowej minimum 10 min przed rozpoczęciem szkolenia.
- Na koniec szkolenia realizowany jest test weryfikujący realizację efektów uczenia.
- Po każdej godzinie szkolenia przewidujemy 10-minutowe przerwy. Szczegółowy ustala trener z grupą.
- Na potrzeby Usługodawcy, jak również na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów kształcenia usługa zdalna może być rejestrowana.

Warunki uczestnictwa

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową https://academy.asseco.pl/szkolenie/cyber-phishing-dla-pracownikow/ w celu rezerwacji miejsca.

UWAGA! Dla usług z dofinansowaniem powyżej 70% istnieje możliwość wystawienia faktury ZW VAT. Prosimy o kontakt z Biurem Asseco Academy academy@assecods.pl Natomiast w przypadku dofinansowania usługi poniżej 70% ze środków publicznych, usługa nie jest zwolniona z podatku VAT. Należy wówczas doliczyć do usługi szkoleniowej należny VAT w wysokości 23%.

Warunki techniczne

Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji Webex Meeting. Aby wziąć udział, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny, laptop wyposażonego w stabilne połączenie internetowe oraz mikrofon i kamerę. Przed rozpoczęciem szkolenia uczestnicy będą mieli możliwość przetestowania swojego sprzętu podczas sesji próbnej, aby upewnić się, że połączenie internetowe, mikrofon i kamera/słuchawki działają poprawnie.

Minimalne wymagania sprzętowo-systemowe:

- Komputer PC z systemem Windows 7 lub nowszym, Max OX 10.13 lub nowszym. Istnieje możliwość korzystania z innych systemów, w tym Linux. Szczegółowe informacje można uzyskać pod adresem: https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-SystemRequirements.
- Przeglądarka internetowa (zalecamy korzystanie z Chrome lub Firefox).
- Karta LAN: min. 100 MBPS lub stabilne połączenie WiFi (zalecamy połączenie do sieci „kablem”). Nie dopuszcza się udziału w szkoleniu za pośrednictwem łączy GSM/LTE. Zalecane pasmo, to przynajmniej 2 MB/s (download i upload). W przypadku spadku przepustowości łącza poniżej 1,2 MB/s należy liczyć się z istotnym obniżeniem jakości połączenia. -Mikrofon i głośniki (zalecamy korzystanie z zestawu typu headset).
- Kamera internetowa.

Przed szkoleniem każdy uczestnik otrzyma na podany adres email link do platformy, gdzie odbędzie się szkolenie. Uczestnictwo w szkoleniu umożliwia aktywne uczestnictwo w zajęciach, w tym komunikację z trenerem oraz pozostałymi uczestnikami. Umożliwia to wymianę doświadczeń oraz aktywny kontakt zarówno z grupą, jak i prowadzącym. Dodatkowo, uczestnicy mają dostęp do funkcji czatu online, co jeszcze bardziej ułatwia interakcję.

Kontakt

Alicja Kozłowska

E-mail bur-szkolenia@assecods.pl
Telefon (+48) 801 303 030