CYBERBEZPIECZEŃSTWO W OBSZARZE SPRZEDAŻY I MARKETINGU – OCHRONA DANYCH KLIENTÓW ORAZ SYSTEMÓW WSPIERAJĄCYCH PROCES SPRZEDAŻY

Grupa docelowa

Szkolenie skierowane jest do pracowników sprzedaży, marketingu, e-commerce i obsługi klienta oraz osób zarządzających tymi obszarami, które w swojej pracy przetwarzają dane klientów i korzystają z systemów sprzedażowych oraz narzędzi marketingowych.

Termin szkolenia

lipiec – listopad 2026

Dokładny termin do ustalenia po zebraniu się grupy szkoleniowej (minimum 5 osób)

Miejsce szkolenia

Szkolenie online – dostęp do platformy zapewnia realizator

Cena za osobę

1500,00 zł za osobę (netto) / 8h dydaktycznych

Sposób przygotowania uczestników

Udział w kursie nie wymaga od uczestników wcześniejszego przygotowania.

Materiały szkoleniowe zostaną zapewnione uczestnikom.

Informacja o prowadzącym

Osoby posiadające doświadczenie i niezbędną wiedzę w zakresie zapewniania rozwiązań z zakresu cyberbezpieczeństwa oraz prowadzenia sprzedaży w formacie e-commerce.

697 007 059

Ratajczaka 44, 61-728 Poznań

FUNDACJA JEDEN UNIWERSYTET

CYBERBEZPIECZEŃSTWO W OBSZARZE SPRZEDAŻY I MARKETINGU – OCHRONA DANYCH KLIENTÓW ORAZ SYSTEMÓW WSPIERAJĄCYCH PROCES SPRZEDAŻY

Program szkolenia i przewidziana liczba godzin

Liczba godzin: 8 dydaktycznych

Moduł 1: Cyberbezpieczeństwo w sprzedaży i marketingu – wprowadzenie

- znaczenie ochrony danych klientów i systemów
- wartość danych w procesach sprzedażowych i marketingowych
- najczęstsze zagrożenia (phishing, przejęcia kont, wycieki danych)
- konsekwencje incydentów

Moduł 2: Ochrona danych klientów (RODO)

- rodzaje przetwarzanych danych
- zasady bezpiecznego przetwarzania (minimalizacja, dostępność)
- najczęstsze błędy i ich unikanie
- postępowanie w przypadku naruszeń

Moduł 3: Bezpieczeństwo systemów oraz zarządzanie dostępami

- systemy sprzedażowe i marketingowe (CRM, CMS, narzędzia reklamowe)
- zarządzanie dostępami i uprawnieniami
- hasła, MFA i dobre praktyki bezpieczeństwa
- onboarding/offboarding i kontrola dostępu
- ryzyka związane z integracjami i wtyczkami

Moduł 4: Phishing i socjotechnika

- mechanizmy i scenariusze ataków (fałszywe zamówienia, komunikacja)
- rozpoznawanie zagrożeń (maile, linki, załączniki)
- zasady bezpiecznego postępowania
- reagowanie na próby oszustwa

Moduł 5: Bezpieczeństwo w e-commerce, marketingu i obsłudze klienta

- zagrożenia w sprzedaży online i obsłudze klienta
- bezpieczeństwo kampanii, kont reklamowych i treści
- ryzyka we współpracy z partnerami
- zasady weryfikacji i ochrony danych klientów
- dobre praktyki operacyjne

697 007 059

Ratajczaka 44, 61-728 Poznań

FUNDACJA
JEDEN UNIWERSYTET

CYBERBEZPIECZEŃSTWO W OBSZARZE SPRZEDAŻY I MARKETINGU – OCHRONA DANYCH KLIENTÓW ORAZ SYSTEMÓW WSPIERAJĄCYCH PROCES SPRZEDAŻY

Cele szkolenia

Celem kształcenia jest zdobycie przez uczestników wiedzy z zakresu zagrożeń cyberbezpieczeństwa w sprzedaży i marketingu, zasad ochrony danych (w tym RODO) oraz funkcjonowania systemów i mechanizmów zabezpieczeń. Uczestnicy rozwiną umiejętności identyfikowania zagrożeń (np. phishing, wycieki danych), stosowania dobrych praktyk bezpieczeństwa oraz prawidłowego reagowania na incydenty. Nabędą również kompetencje umożliwiające bezpieczne zarządzanie danymi klientów, kontrolę dostępu do systemów oraz podejmowanie świadomych decyzji w codziennej pracy sprzedażowej i marketingowej zgodnie z obowiązującymi standardami bezpieczeństwa.

Efektry kształcenia

Uczestnik po zakończeniu szkolenia:

- Rozpoznaje podstawowe zagrożenia cyberbezpieczeństwa (np. phishing, przejęcie konta, wyciek danych) oraz wskazuje ich charakterystyczne cechy.
- Identyfikuje zasady przetwarzania danych osobowych zgodne z RODO, w tym zasadę minimalizacji i ograniczonego dostępu.
- Wskazuje poprawne praktyki zarządzania dostępami i hasłami, w tym zastosowanie MFA oraz zasady nadawania i odbierania uprawnień.
- Rozróżnia bezpieczne i niebezpieczne komunikaty (np. e-mail, link, załącznik) na podstawie ich cech formalnych i treści.
- Określa właściwe działania w przypadku incydentu bezpieczeństwa (np. zgłoszenie naruszenia, zabezpieczenie konta).
- Identyfikuje ryzyka związane z korzystaniem z narzędzi marketingowych i sprzedażowych (CRM, CMS, konta reklamowe, integracje).
- Wskazuje poprawne procedury ochrony danych klientów w obsłudze sprzedaży i marketingu, w tym w kontaktach z partnerami zewnętrznymi.
- Rozpoznaje konsekwencje naruszeń bezpieczeństwa danych dla organizacji i klientów (prawne, finansowe, wizerunkowe).

697 007 059

Ratajczaka 44, 61-728 Poznań

FUNDACJA
JEDEN UNIWERSYTET