PROGRAM SZKOLENIA

„Cyberbezpieczeństwo e-usług”

w ramach MODUŁU – Wdrożeniowcy e-usług

I. Krótki opis szkolenia:

Szkolenie skierowane jest do pracowników administracji publicznej oraz instytucji realizujących e-usługi, którzy chcą skutecznie rozpoznawać zagrożenia i budować bezpieczeństwo cyfrowe w codziennej pracy.

Uczestnicy zapoznają się z podstawowymi typami ataków (phishing, malware, socjotechnika), uczą się zasad bezpiecznego korzystania z systemów i poczty elektronicznej oraz zdobywają umiejętności praktyczne w zakresie reagowania na incydenty.

Omawiane są także zagadnienia zarządzania politykami bezpieczeństwa, projektowania ankiet oceny świadomości, a także zastosowania AI (np. ChatGPT, Copilot) w wykrywaniu zagrożeń i prowadzeniu kampanii edukacyjnych. Zwieńczeniem szkolenia jest warsztatowa praca nad mini-strategią poprawy bezpieczeństwa informacji w organizacji oraz projektowanie własnych narzędzi edukacyjnych.

II. Forma szkolenia:

stacjonarna

III. Liczba godzin szkolenia:

16 godzin dydaktycznych + każdego dnia przerwa obiadowa 45 min i dwie przerwy kawowe po 15 min.

IV. Harmonogram szkolenia:

Dzień 1: 10:00 – 17:15

Godzina	Moduł i tematyka
10:00–10:30	**Moduł 1: Wprowadzenie do szkolenia** - Przywitanie i przedstawienie prowadzącego - Cele i program szkolenia - Ankieta wstępna / test wiedzy (opcjonalnie) - Krótkie poznanie uczestników
10:30–11:45	**Moduł 2: Wprowadzenie do cyberbezpieczeństwa e-usług**

	- Czym są e-usługi? (definicje, przykłady z sektora publicznego) - Dlaczego są podatne na ataki? - Podstawowe zagrożenia: phishing, malware, ransomware, ataki socjotechniczne - Przykłady realnych ataków na instytucje publiczne (z omówieniem skutków) - Dyskusja: „Czy jesteśmy przygotowani?” (burza mózgów)
11:45–12:45	**Moduł 3: Zasady bezpiecznego korzystania z systemów (część 1)** - Silne hasła i zarządzanie hasłami (manager haseł) - Uwierzytelnianie dwuskładnikowe (MFA) - Znaczenie aktualizacji oprogramowania i systemów - Bezpieczne logowanie i blokowanie urządzeń - Mini-ćwiczenie: rozpoznaj słabe hasło
12:45–13:00	Przerwa kawowa
13:00–14:00	**Moduł 4: Zasady bezpiecznego korzystania z systemów (część 2)** - Bezpieczne korzystanie z poczty elektronicznej i przeglądarek - Rozpoznawanie niebezpiecznych załączników i linków - Otwieranie dokumentów i PDF-ów – ryzyka - Konfiguracje lokalnego środowiska pracy: zapora, prywatność, aplikacje
14:00–15:30	**Moduł 5: Praktyczne ćwiczenia – analiza ryzyk i reagowanie (część 1)** - Symulacja scenariusza incydentu (prowadzący prezentuje sytuację) - Uczestnicy identyfikują: co się stało? jakie dane mogą być zagrożone? - Jakie są możliwe działania? - Wprowadzenie do polityk bezpieczeństwa informacji: czym są, przykłady
15:30–16:30	**Moduł 6: Praktyczne ćwiczenia – analiza ryzyk i reagowanie (część 2)** - Symulacja ataku phishingowego (e-mail) - Symulacja infekcji przez złośliwy załącznik - Reakcja na incydent: kogo powiadomić? jak zminimalizować skutki? jak zabezpieczyć dowody?
16:30–17:15	**Podsumowanie dnia 1** - Powtórka kluczowych zasad - Pytania i odpowiedzi

Dzień 2: 09:00 – 16:00

Godzina	**Moduł i tematyka**
09:00–09:15	**Wprowadzenie do dnia 2**

	- Powitanie uczestników, krótkie przypomnienie dnia 1
	- Cel dnia: od ankiet po mini-strategię
09:15–10:30	**Moduł 7: Tworzenie i analiza ankiet bezpieczeństwa – teoria i narzędzia**
	- Dlaczego warto mierzyć świadomość?
	- Przykłady dobrych i złych pytań w ankietach (zamknięte, otwarte, Likerta)
	- Krótkie omówienie wyników rzeczywistej ankiety (case study)
	- Wprowadzenie do Google Forms i MS Forms
	- Mini-demo: jak zbudować poprawny formularz
10:30–11:30	**Moduł 8: Zastosowanie AI w cyberbezpieczeństwie**
	- Wykrywanie phishingu, automatyzacja reakcji, analiza zachowań (UEBA)
	- Wykorzystanie ChatGPT/Copilot: komunikaty, ankiety, scenariusze edukacyjne
	- Dyskusja: „Zagrożenia i szanse AI w naszej organizacji”
11:30–11:45	Przerwa kawowa
11:45–13:00	**Moduł 9: Ćwiczenia praktyczne – ankiety**
	- Projektowanie ankiety oceniającej poziom świadomości pracowników
	- Wybór narzędzia (Forms), testowanie ankiet nawzajem
	- Krótka analiza wyników (wykresy, statystyki), prezentacja wybranych formularzy
13:00–14:00	**Moduł 10: Komunikacja i edukacja użytkowników**
	- Jak mówić o bezpieczeństwie, by nie straszyć?
	- Przykłady skutecznych kampanii: plakaty, checklisty, quizy, newslettery
	- Narzędzia do komunikacji: Canva, Mailchimp, intranet
	- Współpraca z IT, DPO, administratorami – jak się dogadać?
	- Mini-ćwiczenie: zaplanuj tygodniową kampanię uświadamiającą
14:00–15:30	**Moduł 11: Projekt końcowy – opracowanie polityki/strategii**
	- Opracowanie mini-strategii zwiększającej bezpieczeństwo informacji
	- Zawartość: ryzyka, zasady, edukacja, procedury, narzędzia
	- Forma dowolna: dokument, prezentacja, plakat
15:30–16:15	**Podsumowanie i prezentacja projektów**
	- Prezentacja prac, feedback, sesja Q&A, refleksja nad dwoma dniami

V. Efekty szkoleniowe:

Wiedza (co uczestnik wie po szkoleniu):

- zna podstawowe zagrożenia dla e-usług i systemów IT,
- rozumie zasady bezpieczeństwa cyfrowego w organizacjach,

- zna dobre praktyki ochrony przed phishingiem, malware i atakami socjotechnicznymi,
- ma świadomość znaczenia ankiet i edukacji w budowaniu kultury cyberbezpieczeństwa,
- zna narzędzia wspierające bezpieczeństwo (AI, formularze, kampanie komunikacyjne).

Umiejętności (co uczestnik potrafi wykonać):

- identyfikuje typowe zagrożenia i reaguje na incydenty cyberbezpieczeństwa,
- stosuje zasady bezpiecznej pracy z pocztą, plikami i przeglądarką,
- projektuje i wdraża proste ankiety oceny świadomości w zakresie bezpieczeństwa,
- wykorzystuje narzędzia cyfrowe i AI do działań edukacyjnych i komunikacyjnych,
- tworzy i prezentuje mini-strategię poprawy bezpieczeństwa informacji w organizacji.

Postawy (co uczestnik prezentuje po szkoleniu):

- rozwija odpowiedzialność za bezpieczeństwo cyfrowe swojej organizacji,
- promuje dobre praktyki i współpracę z zespołami IT oraz inspektorami ochrony danych,
- wykazuje otwartość na rozwój kompetencji w zakresie cyberbezpieczeństwa,
- angażuje się w działania edukacyjne i wzmacniające kulturę bezpieczeństwa.

VI. Zaliczenie szkolenia:

Na podstawie materiałów wypracowanych przez uczestników podczas zajęć w ramach szkolenia.

VII. Dokument potwierdzający ukończenie szkolenia:

Certyfikat ukończenia szkolenia.

VIII. Przed szkoleniem:

Odbycie i ukończenie 3 webinarów, w wymiarze 60 minut każdy, z zakresu:

- Podstawy e-usług,
- Cyberbezpieczeństwo – podstawy,
- Technologia AI – wprowadzenie.

Webinary będą dostępne do odtworzenia na **trzy tygodnie** przed rozpoczęciem szkolenia.

Osoba Uczestnicząca w Projekcie ma obowiązek ukończyć webinary na **jeden tydzień**

przez rozpoczęciem szkolenia.