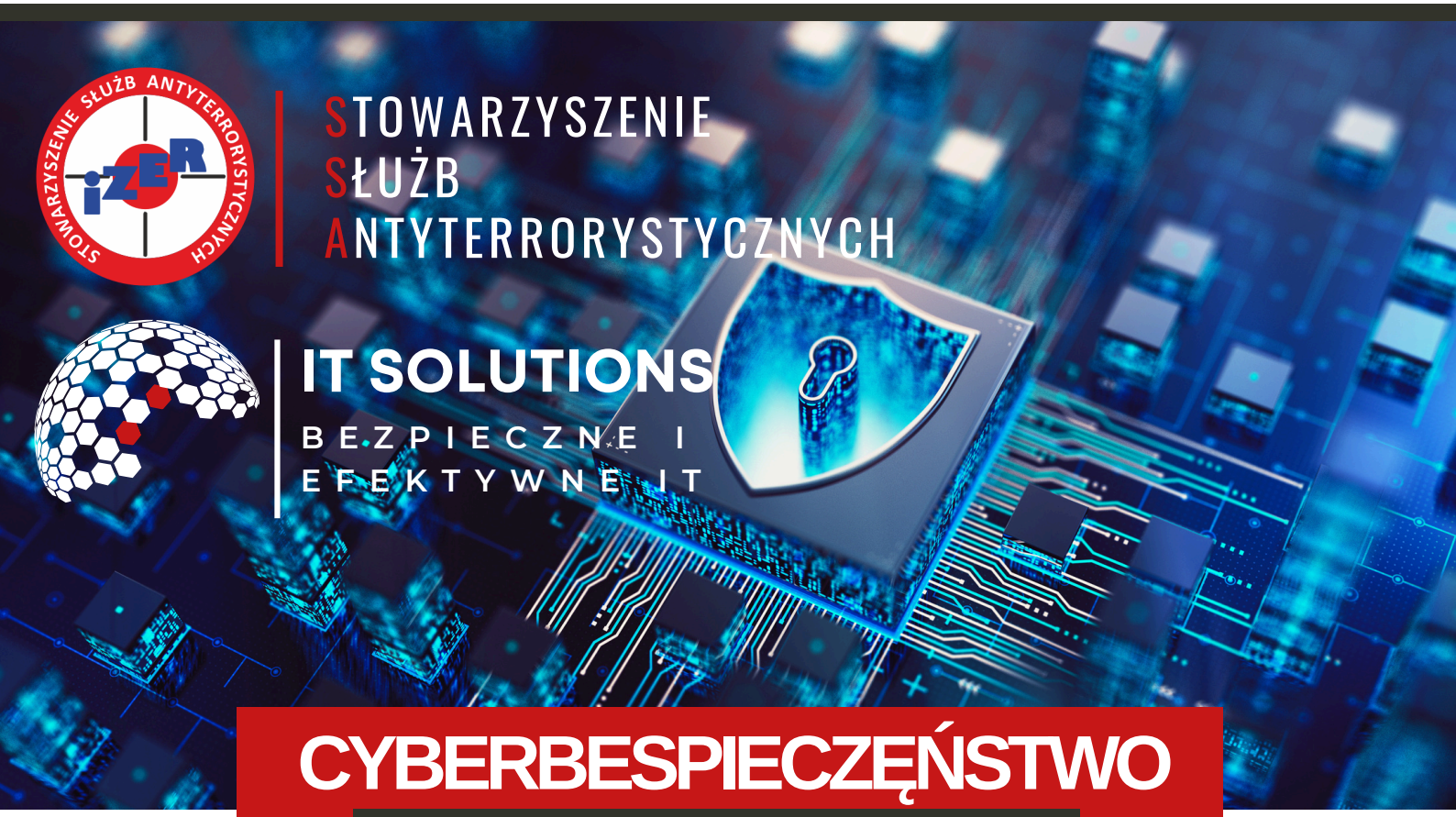

STOWARZYSZENIE SŁUŻB ANTYTERRORYSTYCZNYCH

STOWARZYSZENIE SŁUŻB ANTYTERRORYSTYCZNYCH

IT SOLUTIONS

BEZPIECZNE I EFEKTYWNE IT

CYBERBEZPIECZEŃSTWO

PRZECIWDZIAŁANIE DEZINFORMACJI

SZKOLENIE

Szkolenie z zakresu cyberbezpieczeństwa i przeciwdziałania dezinformacji to praktyczny program edukacyjny, którego celem jest zwiększenie świadomości zagrożeń w przestrzeni cyfrowej oraz budowanie bezpiecznych nawyków w codziennym korzystaniu z technologii. Uczestnicy poznają najczęstsze metody działania cyberprzestępców, uczą się rozpoznawać próby manipulacji oraz skutecznie chronić swoje dane i tożsamość. Program został dostosowany do różnych grup odbiorców – młodzieży, seniorów oraz osób aktywnie korzystających z narzędzi IT w pracy i życiu codziennym – i opiera się na realnych scenariuszach zagrożeń oraz praktycznych ćwiczeniach.

O NAS

Witamy w Stowarzyszeniu Służb Antyterrorystycznych IZER, organizacji, która od lat nieprzerwanie dąży do realizacji swojej misji: krzewienia świadomości narodowej, promowania wartości patriotycznych i obywatelskich oraz rozwijania umiejętności i wiedzy poprzez różnorodne formy edukacji i aktywności fizycznej.

WSPÓŁPRACA ZE SZKOŁAMI I KLASAMI MUNDUROWYMI

Współpracujemy z wieloma szkołami i klasami mundurowymi wspierając je w szkoleniach specjalistycznych.

PROMOWANIE POSTAW OBYWATELSKICH I PATRIOTYCZNYCH

Wspieramy i promujemy postawy patriotyczne, zainteresowania obronnością kraju.

SZKOLENIA SPECJALISTYCZNE, OBOZY SPORTOWE, WARSZTATY

Prowadzimy szkolenia specjalistyczne z wielu zakresów. Dysponujemy profesjonalnym personelem i wyposażeniem.

WWW.IZER.ONLINE KONTAKT@IZER.ONLINE +48 602 263 064

BEZPIECZEŃSTWO ZACZYNA SIĘ OD WIEDZY

W dobie dynamicznego rozwoju technologii oraz rosnącej liczby zagrożeń w przestrzeni cyfrowej, umiejętność świadomego i bezpiecznego korzystania z Internetu staje się kluczową kompetencją każdego obywatela.
Stowarzyszenie Służb Antyterrorystycznych IZER, bazując na doświadczeniu szkoleniowym oraz podejściu praktycznym, przygotowało kompleksowy program szkoleniowy z zakresu:

- cyberbezpieczeństwa,
- ochrony danych,
- przeciwdziałania manipulacji informacyjnej i dezinformacji.

PROGRAM SZKOLENIA

1. MŁODZIEŻ (szkoły, klasy mundurowe)

Cel: budowanie świadomych, odpornych na manipulację użytkowników przestrzeni cyfrowej.

Bezpieczeństwo w sieci – podstawy
- czym są cyberzagrożenia i kto za nimi stoi,
- najczęstsze błędy młodych użytkowników Internetu,
- ślad cyfrowy – jak Internet „zapamiętuje" nasze działania,
- odpowiedzialność prawna w sieci (hejt, udostępnianie treści, stalking).

Social media – zagrożenia i ochrona
- jak działają algorytmy i jak wpływają na nasze decyzje,
- uzależnienie od mediów społecznościowych,
- ochrona prywatności (ustawienia kont, lokalizacja, dane),
- fałszywe profile i kradzież tożsamości.

Cyberprzemoc i zagrożenia społeczne
- formy cyberprzemocy (hejt, wykluczenie, nękanie),
- jak reagować i gdzie zgłaszać,
- konsekwencje psychologiczne i prawne,
- budowanie odporności psychicznej.

Gry online i komunikatory
- zagrożenia w grach (oszustwa, grooming, wyłudzenia),
- bezpieczeństwo mikrotransakcji,
- kontakty z nieznajomymi,
- kontrola rodzicielska i samokontrola.

Dezinformacja i manipulacja
- czym są fake newsy i jak je rozpoznawać,
- mechanizmy manipulacji (emocje, strach, sensacja),
- propaganda i wpływ informacji na społeczeństwo,
- podstawy weryfikacji informacji (fact-checking).

Cyberhigiena
- silne hasła i menedżery haseł,
- uwierzytelnianie dwuskładnikowe (2FA),
- aktualizacje i bezpieczeństwo urządzeń,
- podstawy ochrony przed wirusami i malware.

2. SENIORZY

Cel: zwiększenie poczucia bezpieczeństwa i samodzielności w korzystaniu z technologii.

Podstawy bezpiecznego korzystania z Internetu
- jak bezpiecznie przeglądać strony internetowe,
- czym są zagrożenia online i jak ich unikać,
- rozpoznawanie podejrzanych stron i komunikatów.

Oszustwa i wyłudzenia
- metody działania oszustów (na wnuczka, na policjanta, na bank),
- phishing (fałszywe SMS-y, maile, strony),
- fałszywe inwestycje i „okazje" internetowe,
- scenariusze realnych oszustw – analiza przypadków.

Bezpieczeństwo finansowe
- bezpieczne korzystanie z bankowości internetowej,
- płatności online – na co zwracać uwagę,
- jak chronić dane karty i konta bankowego,
- co zrobić w przypadku oszustwa.

Smartfon i komputer w praktyce
- podstawowe ustawienia bezpieczeństwa,
- aktualizacje systemu i aplikacji,
- instalowanie aplikacji tylko z zaufanych źródeł,
- zabezpieczenie urządzeń (PIN, biometryka).

Ochrona danych osobowych
- jakie dane są wartościowe dla przestępców,
- gdzie nie udostępniać swoich danych,
- zgody marketingowe i prywatność.

Dezinformacja i manipulacja
- fałszywe wiadomości (łańcuszki, „pilne ostrzeżenia"),
- manipulacja emocjami (strach, wzruszenie),
- jak nie dać się wciągnąć w udostępnianie nieprawdziwych treści.

3. DOROŚLI / ADMINISTRACJA / PRACOWNICY BIUROWI

Cel: podniesienie poziomu bezpieczeństwa informacji i odporności organizacyjnej.

Cyberbezpieczeństwo w organizacji
- najczęstsze wektory ataków na instytucje,
- rola pracownika jako „pierwszej linii obrony",
- incydenty bezpieczeństwa – jak powstają i jak im zapobiegać.

Ataki socjotechniczne
- phishing i spear phishing,
- vishing (telefoniczne wyłudzenia),
- impersonacja (podszywanie się pod przełożonych),
- analiza realnych scenariuszy ataków.

Bezpieczeństwo danych i informacji
- klasyfikacja informacji (jawne, wrażliwe, poufne),
- zasady przetwarzania i przechowywania danych,
- bezpieczne przesyłanie dokumentów,
- zagrożenia związane z pracą zdalną.

Zarządzanie dostępem
- polityka haseł,
- uwierzytelnianie wieloskładnikowe,
- zarządzanie uprawnieniami,
- zagrożenia związane z udostępnianiem kont.

Bezpieczeństwo urządzeń i środowiska pracy
- zabezpieczenie komputerów i nośników danych,
- korzystanie z publicznych sieci Wi-Fi,
- praca na urządzeniach prywatnych (BYOD),
- ochrona przed malware i ransomware.

Dezinformacja jako zagrożenie
- wpływ dezinformacji na instytucje publiczne,
- operacje informacyjne i ich cele,
- rozpoznawanie kampanii dezinformacyjnych,
- zarządzanie informacją w sytuacjach kryzysowych.

Reagowanie na incydenty
- jak rozpoznać incydent bezpieczeństwa,
- procedury zgłaszania,
- minimalizowanie skutków ataku,
- podstawy budowania procedur bezpieczeństwa.

ELEMENTY PRAKTYCZNE (dla wszystkich grup)

- analiza rzeczywistych przypadków (case study),
- symulacje ataków (np. phishing),
- ćwiczenia z rozpoznawania manipulacji,
- warsztaty z ustawień bezpieczeństwa na urządzeniach,
- scenariusze „co zrobić gdy…”

CERTYFIKAT

Po pozytywnym ukończeniu wszystkich modułów szkoleniowych, i po uzyskaniu pozytywnej oceny prowadzącego szkolenie, każdy uczestnik otrzyma certyfikat potwierdzający pomyślne ukończenie kursu.

FORMA SZKOLENIA

- szkolenia stacjonarne (szkoły, urzędy, instytucje),
- webinar
- szkolenia wyjazdowe,
- warsztaty praktyczne,
- możliwość realizacji dla grup zorganizowanych,

KADRA

Szkolenia prowadzone są przez doświadczonych specjalistów z wieloletnią praktyką w obszarze IT, architektury systemów oraz cyberbezpieczeństwa. Na co dzień pracują w wiodących firmach z branży technologicznej i finansowej, gdzie odpowiadają za bezpieczeństwo systemów, danych oraz procesów w środowiskach o podwyższonym poziomie ryzyka.

Prowadzący posiadają ugruntowaną, popartą praktyką wiedzę z zakresu cyberbezpieczeństwa, zachowań użytkowników w sieci oraz socjotechnicznych aspektów ataków. Specjalizują się m.in. w ochronie infrastruktury IT, zabezpieczeniach cyfrowych i fizycznych, identyfikacji zagrożeń oraz przeciwdziałaniu dezinformacji.

Doświadczenie zdobywane w środowiskach regulowanych i szczególnie narażonych na cyberataki pozwala im przekazywać wiedzę w sposób praktyczny, oparty na realnych scenariuszach i aktualnych zagrożeniach.

CENA SZKOLENIA

PAKIETY SZKOLEŃ CYBERBEZPIECZEŃSTWA

BASIC

Podstawy bezpieczeństwa w sieci
- najważniejsze zagrożenia (phishing, oszustwa)
- bezpieczne korzystanie z Internetu
- wprowadzenie do dezinformacji

2–3 godziny
do 30 osób
od 1 500 zł netto

PRO

Szkolenie rozszerzone + praktyka
- cyberzagrożenia i socjotechnika
- ochrona danych i prywatności
- dezinformacja i manipulacja
- ćwiczenia i analiza przypadków

4–6 godzin
do 30 osób
od 3 000 zł netto

PREMIUM

Kompleksowe szkolenie + warsztaty
- pełny zakres cyberbezpieczeństwa
- symulacje ataków (np. phishing)
- warsztaty i scenariusze realnych zagrożeń
- rekomendacje dla organizacji

1 dzień (6–8 godzin)
do 25 osób
od 5 500 zł netto

INDYWIDUALNA WYCENA

Każde szkolenie możemy dopasować do potrzeb konkretnej grupy, instytucji lub gminy.

DODATKOWE OPCJE (UPSELL)

Audyt cyberbezpieczeństwa (podstawowy)
Symulowany atak phishingowy (dla organizacji)
Materiały szkoleniowe dla uczestników

*ceny netto (+ VAT)
**dojazd ustalany indywidualnie
***możliwość negocjacji przy większych grupach
****możliwość przygotowania dedykowanego programu