Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
18 maja 2023 r.

OCHRONA PRZED CYBERZAGROŻENIAMI. PHISHING JAKO ZAGROŻENIE DLA BEZPIECZEŃSTWA INFORMACJI

INFORMACJE O SZKOLENIU:

Ataki typu ransomware są najczęstszym powodem unieruchomienia i paraliżu podmiotów publicznych, ich intensywność z roku na rok rośnie, a najskuteczniejszą metodą „przemycenia" złośliwego oprogramowania jest atak socjotechniczny. Ciągłe doskonalenie narzędzi i urządzeń IT w zakresie cyberbezpieczeństwa skutecznie uniemożliwia cyberprzestępcą na ataki bezpośrednie na instytucje publiczne. Zdecydowanie łatwiejszym wektorem ataku jest człowiek, który od lat uważany jest za najsłabsze ogniwo całego systemu cyberbezpieczeństwa. Podczas Webinarium uczestnicy poznają skutecznie przeprowadzone ataki na samorządy w Polsce wraz z omówieniem sposobu ich przeprowadzenia i potencjalnych innych scenariuszy tego ataku.

CELE I KORZYŚCI:

- Zaznajomienie pracowników JST z zagrożeniami wynikającymi z wykorzystania socjotechniki w atakach cyberprzestępców.
- Uczestnicy poznają jak rozpoznać oszustwa oraz jak reagować w sytuacjach zagrożenia bezpieczeństwa informacji.
- Konsultacje z doświadczonym ekspertem.

PROGRAM:

1. **Czym jest phishing i jakie są zagrożenia z nim związane. Prawdziwe przypadki naruszenia ochrony danych i bezpieczeństwa informacji w Jednostkach Samorządu Terytorialnego za pomocą phishingu:**
   a. Czym jest phishing?
   b. Scenariusze ataku. Omówienie najczęstszych scenariuszy.
   c. Omówienie wybranych przypadków skutecznych ataków na JST.
2. **Skutki ataku phishingowego. Co przestępca zyskuje atakując JST:**
   a. Czemy ataki socjotechniczne są tak popularne?
   b. Jakie profity uzyskuje atakujący?
   c. Czy phishing grozi tylko naszym portfelom?
3. **Rodzaje phishingu: spear-phishing, smishing, vishing itp. jakie techniki stosują cyberprzestępcy i jak można je rozpoznać:**
   a. Omówienie klasycznych metod podszywania z wykorzystaniem maila.
   b. Inne kanały wykorzystywane do oszustw.
4. **Techniki obrony przed phishingiem: techniki, które można zastosować, aby zminimalizować ryzyko i skutki ataku phishingowego:**
   a. Co warto robić, aby nie dać się oszustom?
   b. Jakie elementy technologiczne są skuteczne do przeciwdziałania phishingowi?
5. **Przykłady najlepszych praktyk: sposoby rozpoznawania ataków phishingowych, właściwe zachowania w celu uniknięcia ataku, minimalizacji jego skutków, a także działań prewencyjnych:**
   a. Co człowiek może poprawić w swoim zachowaniu?
   b. Co technologia może wspomóc?
6. **Zakończenie: Podsumowanie, wskazanie kanałów pomocy i informacji związanych z cyberoszustwami. To czas na pytania oraz powtórzenie omówionego materiału i podsumowanie zdobytej wiedzy.**

ADRESACI:

Kadra zarządzająca jednostek publicznych, pracownicy jednostek publicznych, którzy chcą poznać podstawy tematyki cyberbezpieczeństwa i bezpieczeństwa informacji (w tym danych osobowych) zgodnie z aktualnym stanem prawnym i zmieniającymi się zagrożeniami, informatycy, Inspektorzy Ochrony Danych Osobowych.

PROWADZĄCY:

Auditor wewnętrzny i wiodący ISO 27001, akredytowany Projekt Managerem Prince 2 2009 Foundation oraz certyfikowany analityk wymagań REQB. Z wykształcenia inżynier oprogramowania oraz ukończone studia podyplomowe Audytu wewnętrznego w Administracji i Gospodarce. Prelegent na licznych konferencjach m.in. Advanced Threat Summit, Forum Skarbników, a także konferencje organizowane przez ApexNet, Doskomp oraz ITSS. Autor opinii do projektu kodeksu postępowań dla jednostek oświaty, którą opracował na zaproszenie autorów tego kodeksu. W branży informatyzacji i ochrony danych osobowych administracji publicznej działa od 2006 roku. Członek Stowarzyszenia Praktyków Ochrony Danych oraz Stowarzyszenia do spraw Bezpieczeństwa Systemów Informacyjnych ISSA Polska, a także członek rady programowej projektu Cyfrowy Skaut. W swojej karierze przeprowadził dziesiątki audytów bezpieczeństwa informacji, zgodności z RODO oraz diagnoz cyberbezpieczeństwa, a także brał udział w wielu wdrożeniach informatyzacji największych samorządów i jednostek rządowych w Polsce.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Ochrona przed cyberzagrożeniami. Phishing jako zagrożenie dla bezpieczeństwa informacji

Szkolenie będziemy realizowali **w formie webinarium on line**.

18 maja 2023 r. **Szkolenie w godzinach 10:00-14:00**

Cena: 379 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera:	udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej Centrum Mazowsze; ul. Żurawia 43, 00-680 Warszawa; tel. 533 849 116; szkolenia@frdl.org.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy (dane do faktury)

Nazwa i adres odbiorcy

NIP **Telefon**

1. **Imię i nazwisko uczestnika,** stanowisko,
   E-MAIL i TEL. DO KONTAKTU
2. **Imię i nazwisko uczestnika,** stanowisko,
   E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe) TAK ☐ NIE ☐

Proszę o przesłanie faktury na adres mailowy: ……

Proszę o przesłanie certyfikatu na adres mailowy: ……

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora www.frdl.mazowsze.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przesyłać do 12 maja 2023 r.

UWAGA! Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej _____