Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
27 lutego 2024 r.

CYBERBEZPIECZEŃSTWO W INSTYTUCJACH PUBLICZNYCH

WAŻNE INFORMACJE:

Cyberbezpieczeństwo w instytucjach publicznych jest niezwykle ważne, ponieważ chroni poufne informacje oraz zapewnia integralność i dostępność usług publicznych. W posiadanych zbiorach informacji znajdują się dane obywateli, ich majątku, sprawy socjalne itp. dlatego zapewnienie odpowiedniego poziomu bezpieczeństwa a szczególnie bezpieczeństwa w przestrzeni internetowej ma istotne znaczenie dla ochrony ich interesów i zapewnienia stabilności usług publicznych. Urząd ze względu na wagę posiadanych informacji stanowi atrakcyjny cel dla różnych rodzajów cyberzagrożeń (wyciek danych, phishing, atak na infrastrukturę). Aby chronić się przed tymi zagrożeniami, urząd powinien stosować środki ochronne takie jak: zabezpieczenia techniczne (np. firewalle i antywirusy), monitoring aktywności w sieci oraz regularne szkolenia pracowników. Dzięki proponowanemu szkoleniu pracownicy nabędą wiedzę na temat bezpieczeństwa w sieci. Podczas zajęć słuchacze poznają punkt widzenia hakera oraz motywy, którymi się kieruje. Poznają również sposoby walki z jego atakami a przede wszystkim sposoby zabezpieczeń aby nie doszło do takich sytuacji. Zadbanie o przeszkolenie swoich pracowników oraz kadry zarządzającej ma również duży wpływ na uniknięcie konsekwencji finansowych jak i wizerunkowych. Wyszkolony pracownik to bezpieczny urząd.

CELE I KORZYŚCI ZE SZKOLENIA:

- Zwiększenie świadomości wśród pracowników i osób odpowiedzialnych za infrastrukturę instytucji zagrożeń i podniesienie poziomu wiedzy nt. cyberbezpieczeństwa. Ochrona wizerunku organizacji.
- Umiejętność rozpoznawania ataków z cyberprzestrzeni.
- Nabycie umiejętności zapobiegania utracie danych przetwarzanych w instytucji a w szczególnych przypadkach zapobieganie utracie środków finansowych z kont instytucji.

PROGRAM:

1. Cyberbezpieczeństwo – wprowadzenie.
2. Tożsamość w sieci, ochrona prywatności, ślady.
3. Wycieki danych, zasady korzystania z hasła, menadżery haseł.
4. Jak odzyskać konto, uwierzytelnianie wieloskładnikowe.
5. Phishing czyli ataki na użytkownika.
6. Poczta elektroniczna, zalety, zagrożenia oraz zasady bezpiecznego korzystania, spam.
7. Kryptografia, szyfrowanie urządzeń i pamięci przenośnych.
8. Socjotechnika czyli po co łamać zabezpieczenia.
9. Urządzenia mobilne, zabezpieczenia.
10. Bezpiecznie w podróży. Korzystanie z obcych WiFi.
11. Podsumowanie.

ADRESACI:

- Pracownicy działów IT i informatycy odpowiedzialni za bezpieczeństwo systemów informatycznych.
- Specjaliści ds. bezpieczeństwa informacji i cyberbezpieczeństwa.
- Kierownictwo i kadra zarządzająca, odpowiedzialna za podejmowanie decyzji dotyczących bezpieczeństwa cybernetycznego.
- Wszystkie osoby zainteresowane omawianą podczas szkolenia tematyką.

PROWADZĄCY:

Dyrektor Departamentu Cyfryzacji Urzędu Marszałkowskiego Województwa Opolskiego. Od roku 1995 zajmuje się cyfryzacją Urzędu oraz Regionu Opolskiego propagując funkcjonowanie elektronicznej administracji publicznej. Realizuje projekty z zakresu społeczeństwa informacyjnego, których celem jest generowanie e-usług dla mieszkańców w celu upowszechniania korzystania z nowoczesnych technologii. Jednocześnie podejmuje działania na rzecz podnoszenia kompetencji cyfrowych, a w swojej codziennej pracy zwraca szczególną uwagę na zagrożenia związane z cyberprzestępczością dotykające instytucje publiczne. Ukończył studia podyplomowe na kierunku Informatyka Śledcza Politechniki Opolskiej. Jest audytorem wewnętrznym Systemu Zarządzania Bezpieczeństwem Informacji PN-EN ISO/IEC 27001:2017-06. W pracy zawodowej podejmuje szereg inicjatyw wprowadzania zmian w Urzędzie mających na celu usprawnienie działania poprzez cyfryzację procesów, co ma znaczący wpływ na przejrzyste, bezpieczne oraz sprawne realizowania zadań przez urzędników. Członek Zespołu Ekspertów ds. Społeczeństwa Informacyjnego przy Związku Województw RP. Członek Polskiego Towarzystwa Informatycznego – Sekcja Informatyków Administracji Publicznej.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w instytucjach publicznych

	Szkolenie będziemy realizowali **w formie webinarium on line**.
	27 lutego 2024 r. **Szkolenie w godzinach 10:00-14:00**
	Cena: 435 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych. **Przy zgłoszeniu do 15 lutego 2024 r cena: 399 PLN netto/os.**
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. Jelinka 6, 01-646 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 20 lutego 2024 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 _____