

HIGIENA CYFROWA I CYBERBEZPIECZEŃSTWO W PRAKTYCE. JAK CHRONIĆ SVOJE DANE, KONTA I URZĄDZENIA PRZED CYBERZAGROŻENIAMI? PRAKTYCZNE WARSZTATY Z PHISHINGU, HASEŁ, 2FA I RODO

WAŻNE INFORMACJE:

Cyberzagrożenia, próby wyłudzenia danych, fałszywe wiadomości i wycieki haseł to problemy, z którymi spotykamy się zarówno w pracy, jak i w życiu prywatnym. Aby skutecznie się przed nimi chronić, nie wystarczy sama znajomość zagrożeń – niezbędna jest umiejętność ich rozpoznawania i stosowania odpowiednich zabezpieczeń.

Zapraszamy na **praktyczne warsztaty z higieny cyfrowej i cyberbezpieczeństwa**, podczas których uczestnicy zdobędą wiedzę i umiejętności niezbędne do bezpiecznego korzystania z narzędzi cyfrowych. Szkolenie łączy krótkie wprowadzenie do najważniejszych zagadnień z ćwiczeniami, symulacjami oraz praktyczną konfiguracją zabezpieczeń.

Uczestnicy nauczą się rozpoznawać próby phishingu, tworzyć silne hasła, konfigurować uwierzytelnianie dwuskładnikowe, bezpiecznie udostępniać pliki oraz chronić dane osobowe zgodnie z zasadami RODO.

CELE I KORZYŚCI:

Celem szkolenia jest rozwinięcie praktycznych umiejętności w zakresie bezpiecznego korzystania z narzędzi cyfrowych, ochrony danych osobowych oraz zapobiegania najczęstszemu cyberzagrożeniu. Uczestnicy poznają narzędzia i procedury zwiększające bezpieczeństwo cyfrowe, a także opracują indywidualny plan działań, który będą mogli wykorzystać w codziennym życiu i pracy.

Dzięki szkoleniu uczestnicy:

- nauczą się rozpoznawać phishing, fałszywe wiadomości i próby wyłudzenia danych;
- poznają zasady tworzenia silnych haseł oraz korzystania z menedżerów haseł;
- zdobędą praktyczne umiejętności konfiguracji uwierzytelniania dwuskładnikowego (2FA) i zarządzania kodami zapasowymi;
- dowiedzą się, jak weryfikować podejrzaną linki, reputację stron internetowych i certyfikaty bezpieczeństwa;
- poznają zasady ochrony danych osobowych, minimalizacji zakresu przetwarzanych danych oraz stosowania anonimizacji i pseudonimizacji;
- nauczą się bezpiecznie przysyłać pliki i zabezpieczać poufne dokumenty;
- przygotują własną checklistę bezpieczeństwa cyfrowego, obejmującą m.in. konta internetowe, urządzenia, tożsamość cyfrową i finanse.

PROGRAM:

Moduł 1. Detekcja zagrożeń, ochrona kont i laboratorium haseł.

1. Rozpoznawanie Phishingu i wyłudzeń:

- Techniki manipulacji stosowane przez cyberprzestępców.
- Rozpoznawanie fałszywych wiadomości e-mail i SMS.
- Interaktywne testy wykrywania zagrożeń.

2. Tworzenie i badanie haseł:

- Projektowanie silnych i unikalnych fraz hasłowych.
- Korzystanie z menedżerów haseł.
- Sprawdzanie informacji o wyciekach danych z wykorzystaniem CERT Polska i Have I Been Pwned.

3. Uwierzalnianie dwuetapowe (2FA):

- Konfiguracja aplikacji Google Authenticator.
- Bezpieczne przechowywanie kodów zapasowych.
- Weryfikacja certyfikatów SSL/TLS i bezpieczeństwa odwiedzanych stron.

Moduł 2. RODO, ochrona danych i indywidualny plan bezpieczeństwa.

4. Praktyczne aspekty RODO i minimalizacja danych:

- Zasady ochrony danych osobowych w miejscu pracy.
- Anonimizacja a pseudonimizacja — różnice i zastosowanie.
- Ograniczanie zakresu zbieranych i przetwarzanych danych.

5. Ochrona prywatności i bezpieczny transfer plików:

- Bezpieczne przesyłanie dokumentów z wykorzystaniem TransferNow.
- Zabezpieczanie plików hasłem i kontrola czasu ich dostępności.
- Ryzyka związane z profilowaniem behawioralnym w mediach społecznościowych i quizach online.

6. Indywidualny plan cyberbezpieczeństwa:

- Ochrona tożsamości cyfrowej, kont i finansów.
- Bezpieczne postępowanie podczas pracy zdalnej.
- Opracowanie osobistej checklisty bezpieczeństwa.

ADRESACI:

Pracownicy administracji publicznej, jednostek samorządu terytorialnego oraz innych instytucji i organizacji, którzy na co dzień korzystają z narzędzi cyfrowych i przetwarzają dane. W szczególności osoby odpowiedzialne za ochronę danych osobowych, bezpieczeństwo informacji oraz obsługę dokumentacji i systemów informatycznych, a także wszystkich, którzy chcą podnieść swoje kompetencje w zakresie higieny cyfrowej i cyberbezpieczeństwa.

PROWADZĄCY:

od kilkunastu lat specjalizuję się w prowadzeniu szkoleń z zakresu kompetencji cyfrowych. Przedsiębiorca, trener szkoleń IT, biznesowych, mówca publiczny. Profesjonalnie przez wiele lat jako lider prowadził projekty i zespoły w działach: IT, sprzedaży, produktów i usług. Z powodzeniem łączy twarde umiejętności IT z kompetencjami miękkimi. Zrealizował ponad 9000 godzin dydaktycznych w projektach ogólnopolskich, współpracując z instytucjami publicznymi, organizacjami pozarządowymi oraz firmami szkoleniowymi. Szkolenia cechują się wysoką rzetelnością, jakością merytoryczną. Posiada doświadczenie w pracy projektowej.

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Higiena cyfrowa i cyberbezpieczeństwo w praktyce. Jak chronić swoje dane, konta i urządzenia przed cyberzagrożeniami? Praktyczne warsztaty z phishingu, haseł, 2FA i RODO



Szkolenie będziemy realizowali **w formie webinarium online.**



17 listopada 2026 r.

Szkolenie w godzinach 9:00-13:00



Cena: 489 PLN netto/os. Przy zgłoszeniach do 3 listopada 2026 r. cena wynosi: 449 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera:

udział w profesjonalnym szkoleniu online z możliwością zadawania pytań,
materiały szkoleniowe w wersji elektronicznej,
certyfikat ukończenia szkolenia.

DANE

DO

KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Reguńskiego, Centrum Mazowsze;
ul. Jelinka 6, 01-646 Warszawa;
tel. 533 721 103;
szkolenia@frdl.org.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy

NIP Nabywcy

(dane do faktury)

Nazwa i adres odbiorcy

NIP Odbiorcy

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 ☐

Faktura zostanie wystawiona jako faktura ustrukturyzowana w Krajowym Systemie e-Faktur (KSeF).

Uwagi:

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 przysyłać do 12 listopada 2026 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 faktury w KSeF.**

Podpis osoby upoważnionej _____