Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
11 października 2021 r.

CYBERBEZPIECZEŃSTWO W PRAKTYCE. JAK SAMODZIELNIE ZABEZPIECZYĆ SWOJE STANOWISKO PRACY?

INFORMACJE O SZKOLENIU:

Przykłady niedawnych ataków hakerskich na skrzynki mailowe przedstawicieli rządu RP wskazują, iż problem ten jest poważny we wszystkich jednostkach administracji publicznej. Zapewnienie cyberbezpieczeństwa powinno być jednym z kluczowych elementów każdej jednostki. By prawidłowo i skutecznie chronić swoje stanowisko pracy przed cyberatakami należy poznać najważniejsze aspekty związane z zapewnieniem bezpieczeństwa elektronicznego zasobom informatycznym. W związku z tym proponujemy Państwu uczestnictwo w szkoleniu, podczas którego omówimy zagadnienia związane z ochroną informacji (w tym danych osobowych) w jednostkach publicznych. Prowadzący w przystępny sposób wskażą zagrożenia związane z korzystaniem z Internetu oraz omówią sposoby zabezpieczania danych oraz monitorowania bezpieczeństwa przez pracodawcę.

CELE I KORZYŚCI:

Podczas szkolenia:

- Omówimy istotę bezpieczeństwa elektronicznych zasobów, z uwzględnieniem praktycznych wskazówek dotyczących prawidłowego zabezpieczenia sprzętu komputerowego.
- Wskażemy jak prawidłowo należy przechowywać dane na nośnikach zewnętrznych i w chmurze.
- Przedstawimy jak w prawidłowy sposób zabezpieczać zdalny dostęp do zasobów instytucji.
- Podpowiemy jakich narzędzi, pomocnych w budowaniu cyberbezpieczeństwa oraz kultury ochrony informacji w jednostce administracji publicznej można użyć.
- Wskażemy jak bezpiecznie szyfrować dokumenty, w jaki sposób bezpiecznie korzystać z przeglądarek i poczty elektronicznej.
- Wyjaśnimy jak samodzielnie i skutecznie zabezpieczyć stanowisko pracy.

PROGRAM:

I CZĘŚĆ: PODSTAWY BEZPIECZEŃSTWA ELEKTRONICZNYCH ZASOBÓW INFORMACYJNYCH:

1. Sześć złotych zasad zapewniających bezpieczeństwo sprzętu i informacji.
2. Podstawowe zagrożenia związane z korzystaniem z Internetu: phishing, ransomware, poczta e-mail, strony www, serwisy społecznościowe.
3. Reguły tworzenia i zmiany haseł do systemów informatycznych i aplikacji.
4. Bezpieczeństwo urządzeń mobilnych.
5. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
6. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.

7. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
8. Prawidłowe korzystanie z oprogramowania antywirusowego.
9. Zasady aktualizacji programów i aplikacji.
10. Monitorowanie przez pracodawcę stanu bezpieczeństwa systemów informatycznych oraz działań podejmowanych przez użytkowników.

II CZĘŚĆ: Konwersatorium – praktyczne wskazówki dotyczące bezpieczeństwa pracy na sprzęcie komputerowym:

1. Szyfrowanie dokumentów w ramach dostępnych funkcji w pakiecie Microsoft Office (Word, Excel, Power Point).
2. Szyfrowanie dowolnego pliku programem zewnętrznym (na przykładzie aplikacji 7- zip, IZArc, RAR).
3. Prezentacja prawidłowych ustawień przeglądarki internetowej (na przykładzie Google Chrome oraz Opera).
4. Przedstawienie alternatywnych rozwiązań zapewniających anonimowość i ochronę prywatności użytkowników (przeglądarka Brave oraz wyszukiwarka DuckDuckGo).
5. Zasady bezpiecznego korzystania z poczty e-mail (pokaz praktyczny).

ADRESACI:

Kadra zarządzająca jednostek administracji publicznej, pracownicy jednostek administracji publicznej, informatycy, którzy chcą poznać i zrozumieć podstawy tematyki cyberbezpieczeństwa w jednostkach administracji publicznej zgodnie z aktualnym stanem prawnym i zmieniającymi się zagrożeniami.

PROWADZĄCY:

Absolwent UMK w Toruniu oraz studiów podyplomowych WSAiB w Gdyni na kierunku zarządzanie bezpieczeństwem informacji, certyfikowany Inspektor Ochrony Danych, Menedżer Bezpieczeństwa Informacji oraz Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji. W latach 1992 - 2013 funkcjonariusz UOP/ABW, od 1999r. zajmuje problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009r. ekspert ABW z zakresu ochrony informacji niejawnych. Współorganizator szkoleń i konferencji poświęconych problematyce ochrony informacji oraz danych osobowych. W latach 2013 - 2017 pełnomocnik ds. ochrony informacji niejawnych w Urzędzie Wojewódzkim oraz innych jednostkach.

Absolwent Wojskowej Akademii Technicznej w Warszawie, studiów podyplomowych z zakresu bezpieczeństwa teleinformatycznego, posiada Certyfikat Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji, wieloletnie doświadczenie pracy w pionie ochrony informacji niejawnych na stanowiskach: inspektor BTI oraz administrator systemów TI przetwarzających informacje niejawne w administracji publicznej. W latach 2002 -2006 pracownik ABW na stanowisku kierowniczym w pionie bezpieczeństwa teleinformatycznego; odpowiedzialny m. in. za organizowanie i prowadzenie szkoleń z zakresu bezpieczeństwa TI, posiada doświadczenie w opracowywaniu dokumentacji bezpieczeństwa dla systemów TI przetwarzających informacje niejawne i administrowanie takim systemem.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w praktyce. Jak samodzielnie zabezpieczyć swoje stanowisko pracy?

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

11 października 2021 r. **Szkolenie w godzinach 9:00-13.00**

Cena: 325 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera:	udział w profesjonalnym szkoleniu on-line, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia, możliwość konsultacji z trenerem.
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej Podlaskie Centrum ul. Choroszczańska 31, 15-732 Białystok tel.: 85 732 17 88 | fax: 85 732 94 84 mail: frdl-pc@frdl.bialystok.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 certyfikat w formie: Papierowej ☐
Elektronicznej ☐ e mail……

Proszę o przesłanie faktury 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.rzeszow.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.bialystok.pl lub mailem na adres: frdl-pc@frdl.bialystok.pl do 7 października 2021 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 _____