SZKOLENIE ONLINE: Cyberbezpieczeństwo

2025-01-27

Centrum Obywatelskie – ul. Reymonta 20 wraz z Krakowskim Forum Organizacji Społecznych KraFOS zapraszają na szkolenie, podczas których zwiększycie Państwo świadomość na temat zagrożeń cyberbezpieczeństwa oraz podstawowych umiejętności ochrony danych i unikania zagrożeń w codziennym użytkowaniu technologii.

Szkolenie z cyberbezpieczeństwa dla osób nietechnicznych to praktyczny i zrozumiały program, który ma na celu zwiększenie świadomości na temat zagrożeń w sieci oraz nauczenie podstawowych zasad ochrony danych w codziennym życiu. Dzięki interaktywnym warsztatom i przykładom z życia codziennego uczestnicy dowiedzą się, jak unikać popularnych ataków, skutecznie chronić swoje dane oraz korzystać z internetu w bezpieczny sposób.

Szkolenie jest skierowane do pracowników, menedżerów oraz osób, które na co dzień nie zajmują się technologią, ale chcą zwiększyć swoją wiedzę i bezpieczeństwo w cyfrowym świecie.

Korzyści dla uczestników:

- Poznanie najczęstszych zagrożeń cyberbezpieczeństwa.
- Nabycie umiejętności rozpoznawania i unikania ataków phishingowych.
- Praktyczna wiedza na temat ochrony danych osobowych i firmowych.
- Lepsze przygotowanie do bezpiecznej pracy w środowisku cyfrowym.

Kiedy? Czwartek 6 lutego godz. 16.00 – 20.00
Gdzie? ONLINE

Formularz zapisu: https://forms.gle/MsbquKJYFisdzCYT6

Program szkolenia:

Wprowadzenie do cyberbezpieczeństwa

- Co to jest cyberbezpieczeństwo i dlaczego jest ważne?
- Najczęstsze zagrożenia w sieci: phishing, ransomware, ataki socjotechniczne.

- Przykłady ataków cybernetycznych w życiu codziennym (case study).

Ochrona danych osobowych i firmowych

- Jak chronić swoje dane w sieci (hasła, uwierzytelnianie wieloskładnikowe).
- Bezpieczne korzystanie z urządzeń mobilnych i komputerów.
- Oprogramowanie antywirusowe i aktualizacje – dlaczego są kluczowe?

Rozpoznawanie zagrożeń w sieci

- Jak rozpoznać podejrzane e-maile i wiadomości (phishing)?
- Bezpieczne korzystanie z mediów społecznościowych i komunikatorów.
- Fałszywe strony internetowe i linki – jak ich unikać?

Zasady bezpiecznej pracy zdalnej

- Podstawowe zasady ochrony danych podczas pracy zdalnej.
- Korzystanie z sieci Wi-Fi – zagrożenia publicznych sieci.
- Narzędzia do bezpiecznej współpracy online.

Warsztaty praktyczne: symulacje zagrożeń

- Rozpoznawanie ataków phishingowych w praktyce (analiza przykładowych e-maili).
- Tworzenie silnych haseł i stosowanie uwierzytelniania wieloskładnikowego.

Podsumowanie i sesja pytań (30 minut)

- Podstawowe zasady bezpieczeństwa w codziennym życiu.
- Sesja pytań i odpowiedzi.