Tytuł szkolenia: BEZPIECZNE ZACHOWANIA W SIECI

Grupa wiekowa uczestników: 15 – 18 lat

Cele szkolenia:

- Podczas szkolenia omówione zostaną rodzaje niebezpieczeństw w sieci.
- Uczestnicy dowiedzą się, gdzie szukać informacji związanych z bezpieczeństwem w sieci.
- Poznają narzędzia do bezpiecznego przechowywania plików i danych.
- Nauczą się również, jak się zabezpieczyć, gdy zaatakuje wirus.
- Poznają też dobre praktyki w bezpiecznym korzystaniu z narzędzi online.

Program szkolenia:

1. Gdzie szukać informacji związanych z bezpieczeństwem w sieci
    - Problemy z wyciekiem danych z serwisów
        - Dane statystyczne
        - Dane internetowe
        - Zasady bezpieczeństwa
    - Oszustwa (Phishing, Spear phishing, Clone phishing, Whaling, Pharming, Drive-by pharming, Fałszywe aktualizacje, Scam, Nigeryjski szwindel)
2. Jak się zabezpieczyć przed problemami z wyciekiem danych z serwisów oraz oszustwem?
    - Cookies
    - RODO
    - Oszczędne gospodarowanie danymi
    - Niedyskretny profil
    - Obowiązek czytania regulaminów
    - Hasła mocne i słabe
    - Uwierzytelnianie dwuetapowe
    - Nawyki
    - Rozsądek
3. Cyberprzemoc
    - Trolowanie
    - Hejter
    - Child grooming
    - Flejm
    - Flood
    - Przeciwdziałanie cyberprzemocy
4. Analiza narzędzi do komunikacji

- Internet jako narzędzie komunikacji
- Zasady komunikacji w sieci
- Narzędzia szyfrowane

5. Dobre praktyki zastosowań narzędzi do komunikacji
   - Wideokonferencja
   - Skype
   - Microsoft Teams
   - Google Hangouts
   - Messenger
   - E-mail
   - Trello
   - Slack
   - Asana
6. Jak trafiają do nas wirusy, czyli dobre praktyki w bezpiecznym korzystaniu z narzędzi online:
   - Maile
   - Załączniki
   - Pobieranie plików
   - Instalowanie oprogramowania
7. Jak bezpiecznie przechowywać pliki i dane
   - Nośniki zewnętrzne
   - Chmura
8. Co zrobić, gdy zaatakuje nas wirus
   - Procesy bezpieczeństwa
   - Narzędzia