

Scenariusz lekcji: Cyberbezpieczeństwo – jak skutecznie zwiększać cyberświadomość?

1. Temat lekcji: Cyberbezpieczeństwo – jak skutecznie zwiększać cyberświadomość i chronić się przed zagrożeniami w sieci?

2. Czas trwania: 45 minut

3. Cele lekcji:

- Uczeń zna podstawowe zagrożenia w sieci (phishing, spoofing, ataki hakerskie).
- Uczeń rozumie zasady bezpiecznego korzystania z Internetu.
- Uczeń potrafi stosować praktyczne metody ochrony swoich danych w sieci.
- Uczeń wie, jakie działania podejmują banki i instytucje w celu ochrony cyberfinansów.

4. Metody pracy:

- Mini wykład
- Dyskusja
- Analiza przypadków
- Praca w grupach
- Ćwiczenia praktyczne (identyfikowanie zagrożeń)

5. Środki dydaktyczne:

- Prezentacja multimedialna *Cyberbezpieczni 2025*
 - Komputer z dostępem do Internetu
 - Materiały informacyjne (broszury, infografiki)
-

6. Przebieg lekcji:

1. Wprowadzenie (5 minut)

- Nauczyciel pyta uczniów, jak rozumieją pojęcie cyberbezpieczeństwa.
- Krótka rozmowa o codziennych nawykach korzystania z Internetu i potencjalnych zagrożeniach.

2. Omówienie zagrożeń w sieci (10 minut)

- Pokazanie przykładowych ataków i oszustw internetowych.

3. Jak skutecznie zwiększać cyberświadomość? (10 minut)

- Omówienie metod edukacyjnych: szkolenia, marketing edukacyjny, social media, filmy edukacyjne, gry interaktywne.
- Analiza działań banków i firm w zakresie cyberbezpieczeństwa (szyfrowanie, bezpieczne aplikacje, monitoring transakcji).

4. Ćwiczenia praktyczne – identyfikacja zagrożeń (15 minut)

- Uczniowie w grupach analizują przykładowe e-maile i wiadomości SMS pod kątem phishingu.
- Wspólna dyskusja na temat metod rozpoznawania oszustw.
- Ćwiczenie polegające na konfiguracji dwuetapowej weryfikacji na różnych platformach.

5. Podsumowanie i refleksja (5 minut)

- Uczniowie podają zasady, które zapamiętali z lekcji.