# Scenariusz zajęć

*IV etap edukacyjny, informatyka*

## Temat: Zabezpieczenia sieci

### Treści kształcenia:

Informatyka:
1. Bezpieczne posługiwanie się komputerem, jego oprogramowaniem i korzystanie z sieci komputerowej. Uczeń:
3) korzysta z podstawowych usług w sieci komputerowej, lokalnej i rozległej, związanych z dostępem do informacji, wymianą informacji i komunikacją, przestrzega przy tym zasad netykiety i norm prawnych dotyczących bezpiecznego korzystania i ochrony informacji oraz danych w komputerach w sieciach komputerowych.

### Cele zoperacjonalizowane:

Uczeń:

- Rozumie wady i zalety podłączania komputera do sieci komputerowej
- Zna pojęcie zapory (firewall) i potrafi ją skonfigurować w systemie operacyjnym
- Zna pojęcie bezpiecznego połączenia poprzez protokoły SSL i SHTTP
- Rozumie zagrożenia związane z bezpieczeństwem sieci bezprzewodowych

### Nabywane umiejętności:

Uczeń:

- Potrafi sprawdzić konfigurację i aktualność zabezpieczeń w systemie Windows
- Potrafi zabezpieczyć komputer pracujący w sieci
- Zna metody szyfrowania danych w sieci komputerowej

### Kompetencje kluczowe:

- Kompetencje informatyczne
- Kompetencje społeczne i obywatelskie

### Środki dydaktyczne:

- Prezentacja: „Bezpieczeństwo sieci bezprzewodowych”
- Film (samouczek): „Zabezpieczenia internetowe”
- Komputery podłączone do Internetu
- Rzutnik
- Tablica

### Metody nauczania:

- Eksponujące: film
- Podające: prezentacja
- Problemowe: dyskusja
- Praktyczne: ćwiczenia
- Praktyczne: instruktaż



KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE Ośrodek Rozwoju Edukacji
scholaris
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Materiał edukacyjny wytworzony w ramach projektu „Scholaris – portal wiedzy dla nauczycieli” współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

## Formy pracy:

- Praca zbiorowa
- Praca indywidualna

## Przebieg zajęć:

### Etap wstępny

Nauczyciel rozpoczyna zajęcia od wskazania głównych zagrożeń dla komputera, płynących z Sieci: wirusy komputerowe i ich odmiany (trojany, robaki, keyloggery), phishing (kradzież poufnych danych). Wskazuje na niezgodną z prawem stronę działalności hackerów komputerowych.
Omawia zagadnienie aktualizacji systemu operacyjnego jako formy zabezpieczenia przed zagrożeniami płynącymi z Internetu, następnie wskazuje na konieczność aktualizacji popularnego oprogramowania, takiego jak przeglądarki internetowe, przeglądarka plików PDF czy przeglądarka animacji w formacie Flash.
Krótko omawia zagadnienie wirusów komputerowych, ich odmiany i źródła zarażania (poczta, nośniki danych, pliki edytorów tekstów lub PDF itd.) oraz wskazuje, że programy typu Internet Security są dobrym sposobem na zabezpieczenie komputera przed zagrożeniami.
Omawia również zagadnienie certyfikacji stron WWW oraz w skrócie zagadnienie sieci VPN (wirtualne sieci prywatne).

### Etap realizacji

Nauczyciel wyświetla prezentację multimedialną pt. „Bezpieczeństwo sieci bezprzewodowych”. W prezentacji omawiane są zagadnienia zasygnalizowane przez nauczyciela, poszerzone o dodatkowe informacje na temat najpopularniejszych typów włamań do sieci bezprzewodowych i zabezpieczeń sieci.
Następnie wyświetla film (samouczek) pt. „Zabezpieczenia internetowe”, ukazujący program antywirusowy połączony z oprogramowaniem typu Internet Security jako przykład skutecznego zabezpieczenia komputera. Zwraca szczególną uwagę na konfigurację zapory (firewall), kontroli rodzicielskiej i ochrony antyphishingowej.

Kolejnym zagadnieniem, które porusza nauczyciel, jest aktualność baz programu antywirusowego. Pokazuje on na kilku przykładowych stronach internetowych, w jaki sposób stwierdzić, czy połączenie z daną stroną WWW jest szyfrowane, czy nie. Tłumaczy, czym jest protokół SHTTP. Uczniowie sprawdzają, które moduły programu typu Internet Security lub antywirusowego, zainstalowanych w szkolnej pracowni, są aktywne i w jaki sposób skonfigurowana jest zapora (firewall).



KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE Ośrodek Rozwoju Edukacji
scholaris
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Materiał edukacyjny wytworzony w ramach projektu „Scholaris – portal wiedzy dla nauczycieli” współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

### Etap końcowy

Nauczyciel zadaje uczniom pytania kontrolne:

1. Czym jest wirus komputerowy?
2. Co to jest phishing?
3. Dlaczego aktualizowanie systemu operacyjnego jest ważne?
4. Czym jest protokół SHTTP?
5. Do czego służy firewall?

Zadanie domowe:
Sprawdź obecność i konfigurację omawianych zabezpieczeń na swoim domowym komputerze.

## Słowa kluczowe:

phishing, wirus, firewall, zapora



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
ORE Ośrodek Rozwoju Edukacji
scholaris
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Materiał edukacyjny wytworzony w ramach projektu „Scholaris – portal wiedzy dla nauczycieli"
współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.