Scenariusz lekcji – cykl lekcji zrealizowanych w kl. 7 i 8
Temat: Ochrona bankowa pieniądza-zabezpieczenia i weryfikacje na koncie bankowym.

Cele

- *rozwinięcie u uczniów i uczennic kompetencji cyfrowych niezbędnych do bezpiecznego poruszania się w sieci, zwłaszcza podczas wykonywania transakcji finansowych on-line;*
- *zaznajomienie z prawami klientów w związku z autoryzowanym lub nieautoryzowanym dostępem do konta czy karty kredytowej;*
- *wskazanie instytucji pomagających ofiarom wybranych przestępstw o charakterze finansowym w sieci, takich jak np. phising.*

Metody
- metody ćwiczeń praktycznych
- metody eksponujące

Środki dydaktyczne
- praca z wykorzystaniem aplikacji internetowych
- prezentacje multimedialne

Lekcje przeprowadzone zostały w cyklu 2 spotkań.

1. Czy moje pieniądze są bezpieczne w sieci? Moje kieszonkowe – planowanie i kontrola wydatków własnych.

a) prezentacja multimedialna na temat zarządzania finansami osobistymi
b) dyskusja na temat kształtowania własnych potrzeb oraz roli czynników środowiskowo-społecznych w budowaniu bezpieczeństwa finansowego
c) zaprojektowanie tabeli wydatków z własnego kieszonkowego – analiza propozycji i opracowanie rozwiązania
d) poznanie portali internetowych, ułatwiających planowanie własnych wydatków, np. Money, Innim Mobile Exp
e) przygotowanie w kilku zespołach prezentacji multimedialnych oraz ich zaprezentowanie na forum klasy jako baza do dyskusji

2. Czy moje zakupy i przelewy internetowe są bezpieczne? – minidebata klasowa na podstawie prezentacji multimedialnej

a) wyszukiwanie w grupach argumentów potwierdzających stanowisko, że przelewy internetowe są bezpieczne (1. grupa) i że w przestrzeni on-line czyha wiele zagrożeń (2. grupa)
b) analiza argumentów, formułowanie wniosków
c) zapis wniosków w zeszycie w postaci notatki

3. Zagrożenia dla płatności on-line. Oszustwa i atak phisingowy

- *Pishing – co to takiego? Atak phishingowy (smishingowy) to metoda oszustwa, w której osoba trzecia podszywa się pod inny podmiot w celu wyłudzenia informacji (danych), które umożliwią zalogowanie się do bankowości elektronicznej (uwierzytelnienie) i zlecenie oraz autoryzowanie transakcji płatniczej (najczęściej przelewu).*
- *Jak wyłudzane są nasze dane? Wyłudzenie danych odbywa się przy pomocy różnego rodzaju socjotechnik:*

4.Jak sprawdzać autentyczność banknotów? Wykorzystanie materiałów ze strony NBP.

- *osoby w kontakcie telefonicznym podają się za pracowników banku, kancelarii prawnej lub firmy współpracującej z bankiem, i – powołując się na potrzebę zwiększenia bezpieczeństwa – proszą o podanie poufnych informacji;*

•*przy pomocy złośliwego oprogramowania (najczęściej instaluje się ono po otwarciu załączników do fałszywych e-maili, smsów lub wiadomości albo w związku z pobraniem aplikacji mobilnej);*
•*poprzez podmianę prawdziwego numeru rachunku bankowego użytkownika na fałszywy;*
•*poprzez podszywanie się pod konto FB znajomego i prośbę o wspomożenie przez dotpay czy Przelewy 24.*

4. Instytucje pomagające ofiarom wybranych przestępstw o charakterze finansowym w sieci – prezentacja.

5. Jak się chronić? Wnioski zapisane w formie mapy myśli

•*Zawsze korzystaj z legalnego oprogramowania i regularnie go aktualizuj.*
•*Stosuj programy antywirusowe oraz firewall.*
•*Nie wyszukuj stron internetowych banku przez przeglądarki.*
•*Nie otwieraj e-maili nieznanego pochodzenia, nie odpowiadaj na nie, a zwłaszcza nie otwieraj załączników lub linków w nich wskazanych.*
•*Zmieniaj regularnie hasło do konta.*
•*Nie kopiuj numerów rachunków ze „schowka".*
•*Weryfikuj dane zawarte w sms-ach autoryzacyjnych: rodzaj dyspozycji i dane transakcji w sms-ie powinny się zgadzać się z tymi, które wyświetlają się na ekranie.*
•*Nie loguj się do banku z otwartych sieci WiFi.*

6. Zagadnienia ekonomiczne przekazane w trakcie lekcji:
- *planowanie wydatków*
- *monitorowanie wydatków – rola monitoringu*
- *sposoby monitorowania wydatków, w tym poprzez aplikacje internetowe*
- *sposoby ochrony dostępu do konta*
- *budowa i zmiana hasła, hasło słabe i mocne*
- *oszustwa internetowe, pishing*
- *autoryzacja transakcji*
- *zabezpieczenia banknotówi jak sprawdzac ich auntentyczność.*
- *ochrona danych*