Zasady bezpieczeństwa w sieci

Nauczanie może przyjmować różne formy oraz być prowadzone różnymi metodami. Jednym z nowoczesnych sposobów nauczania jest e-learning. Aby mógł on poprawnie funkcjonować, wymaga od organizatorów podejmowanie wielu działań i przestrzegania podstawowych zasad bezpieczeństwa.

1. Uważaj na wiadomości e-mail.
    - Nieodebrana przesyłka pocztowa lub kurierska;
    - Egzekucja zajęcia konta bankowego;
    - Blokada konta bankowego;
    - Od firm, których nie znasz;
    - Fałszywe faktury;
    - Fałszywe rezerwacje np. hoteli;
    - Lokalizacja numerów telefonu;
    - Szansa otrzymania wyjątkowej nagrody.

    Jak nie dać się złapać:

    - Nie pobieraj danych z nieznanych źródeł ;
    - Nie pobieraj aplikacji z nieznanych źródeł;
    - Nie otwieraj wiadomości spam;
    - Nie daj się ponieść emocjom związanym np. z szansą
    - wygrania nagrody;
    - Nie klikaj w nieznane linki;
    - Nie wpisuj swoich danych osobowych

2. Zagrożenie w trakcie korzystania z portali społecznościowych.
    - Kradzież tożsamości;
    - Przesłanie niebezpiecznego oprogramowania;
    - Inwigilacja;
    - Wykorzystanie danych przeciwko Tobie;
    - Kradzież hasła.

    Zasady bezpiecznego korzystania z portali społecznościowych:

    - Dostosuj do własnych potrzeb ustawienia prywatności swojego konta;
    - Unikaj klikania w nieznane linki;
    - Dodawaj do listy znajomych wyłącznie osoby, które rzeczywiście znasz i
    - którym ufasz;
    - Nie ufaj udostępnianym w serwisie aplikacjom;
    - Pamiętaj też o tym, by nie wrzucać do sieci tych danych, których nie chcesz upublicznić;
    - Stosuj różne hasła;
    - Najsłabszym ogniwem jest zwykle sam użytkownik.

- Pamiętaj pliki, zdjęcia pozostają w sieci na wiele lat !!!

3. Sugerowane reklamy – cookies – ciasteczka.

   a) Co robią:
      - Śledzą ruch użytkownika w internecie;
      - Wysyłają reklamy np. produktu, który wcześniej przeglądaliśmy;
      - Zapisują się na dysku twardym komputera i przeglądarkach internetowych.
      - Najczęściej są zapisywane ostatnie wizyty na stronach oraz czas w którym plik ma zostać usunięty automatycznie.

   b) Mogą przechowywać:
      - Login.
      - Zaszyfrowane hasło.

      W takim przypadku istnieje możliwość, że odpowiednio przygotowany wirus będzie wykradał nasze osobiste dane. Dzieje się tak kiedy ciasteczka zostają zapisane na naszym komputerze dłużej niż okres trwania zamknięcia przeglądarki.

   c) Jak pozbyć się ciasteczek?
      - Firefox - Narzędzia > Historia > Wyczyść historię przeglądania (zaznaczamy "ciasteczka") i wyczyść teraz;
      - Internet Explorer - Narzędzia > Bezpieczeństwo > Usuń historię przeglądania (zaznaczamy "ciasteczka") i usuń;
      - Google Chrome - Narzędzia > Historia > Wyczyść dane przeglądarki > zaznaczamy pole: Usuń pliki cookie oraz inne dane witryn i wtyczek naciskamy Wyczyść dane przeglądarki.

4. Hotspot na co uważać.
      - Dane mogą być przechowywane – ktoś może z nich skorzystać;
      - Loginy i hasła mogą być przejęte.
      - Cyberprzestępcy tworzą własne hot-spoty podszywając się pod Inne
      - Infekcja komputera, tableta, telefonu.
      - Jeżeli musimy skorzystać z Hot-spota pamiętajmy, aby nigdy nie korzystać zoperacji związanych z logowaniem do kontabankowego, poczty czy też portali społecznościowych

5. Jak dbać o swój komputer.
    - Używaj legalnego systemu;
    - Aktualizuj system;
    - Serwisuj komputer;
    - Zainstaluj i aktualizuj program antywirusowy;
    - Skanuj programem antywirusowym pliki z nieznanego źródła przed
    - ich otwarciem;
    - Aktualizuj przeglądarkę internetową;
    - Zabezpiecz komputer hasłem;
    - Nie dawaj osobom niezaufanym dostępu do swojego komputera.
    - Uwaga na przeglądarki internetowe ! W nich mogąbyć zapisane nasze hasła.
    - Pamiętaj by zmieniać hasła co jakiś czas.
6. Smartfony i tablety.
    a) O co zadbać aby korzystać bezpiecznie z naszych urządzeń mobilnych?
        - Aktualizować urządzenie;
        - Zainstalować i aktualizować program antywirusowy;
        - Nie korzystać w miejscach publicznych z logowania np.do konta bankowego;
        - Omijać darmowe Hot-spoty;
        - Korzystać z internetu oferowanego przez twojegooperatora sieci;

    b) O co zadbać aby korzystać bezpiecznie z naszych urządzeń mobilnych?
        - Blokadę ekranu zabezpieczyć hasłem;
        - Korzystać wyłącznie z zaufanych aplikacji;
        - Nie odwiedzać „dziwnych” stron internetowych;
        - Uważajmy na ważne sms-y od banku, np. polecenie zainstalowania najnowszej wersji aplikacji mobilnej;
        - Po zmianie lub utracie telefonu poinformować bank