Co-funded by the
Erasmus+ Programme
of the European Union

INNOWACYJNE NARZĘDZIA EDUKACYJNE

VIRIBUS UNITIS
FUNDACJA ROZWOJU REGIONALNEGO

Temat: „BEZPIECZEŃSTWO W SIECI”

Tomasz Zacłona

Monika Makowiecka

I. Uzasadnienie wyboru tematu

Znajomość zagrożeń w sieci oraz sposobów zapobiegania ich występowaniu jest obecnie jednym z ważniejszych kwestii związanych z użytkowaniem komputera. Internet w dzisiejszych czasach jest bowiem nieodzownym elementem życia codziennego.

Warto a nawet wskazane jest posiadanie programu antywirusowego na swoim komputerze, laptopie, smartfonie. Z prostej przyczyny: program antywirusowy przesieje większą część wirusów, malwerów, koni trojańskich i innych zagrożeń, z tych które czychają na każdego Internautę w sieci.

II. Ogólne cele kształcenia

- Stworzenie uczniom szansy na zaznajomienie się z zagrożeniami związanymi z użytkowaniem komputera i sieci internet.
- Istotnym elementem realizacji tematu jest także poznanie sposobów przeciwdziałania występującym zagrożeniom.

III. Zakres tematyczny zajęć

1. Bezpieczeństwo w sieci
2. Do jakich tematów odnosi się bezpieczeństwo w sieci
3. Zagrożenia w Internecie
4. Czym jest antywirus
5. Sposoby na zachowanie bezpieczeństwa w sieci
6. Ćwiczenia

IV.Metody prowadzenia zajęć

1) Mini wykład (w oparciu o prezentację)
2) Materiały poglądowe – interaktywny film
3) Praca pod kierunkiem
4) Praca w grupie

1. Bezpieczeństwo w sieci

Termin "bezpieczeństwo sieci" odnosi się do każdego działania, które ma na celu chronić użyteczność i integralność danych na naszym komputerze

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

- Bezpieczeństwo urządzeń mobilnych
- Bezpieczeństwo aplikacji
- Kontrola dostępu
- Oprogramowania antywirusowe
- Zapobieganie wypływowi danych
- Bezpieczeństwo maili
- Zapory sieciowe (ang. firewall)

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Bezpieczeństwo urządzeń mobilnych

Cyberataki są coraz częściej kierowane w urządzenia mobilne - nic w tym dziwnego, biorąc pod uwagę ich rosnącą popularność.

Trzymają one nasze osobiste dane, mają też połączenie z portalami społecznościowymi, serwisami czy bankami.

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Bezpieczeństwo aplikacji

Każdy software, którego używasz i który jest podłączony do twojej sieci powinien być chroniony.

Pamiętaj, że aplikacje mogą zawierać luki w bezpieczeństwie, które atakujący mogą wykorzystać do infiltracji sieci.

Nie martw się, istnieją aplikacje ochronne, które domykają te luki.

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Kontrola dostępu

Uważaj! Nie każdy użytkownik powinien mieć dostęp twojej sieci!

Aby zmniejszyć ryzyko wejścia przez osoby niepowołane należy kontrolować każdego użytkownika i każde urządzenie.

Urządzenia nieautoryzowane mogę być odrzucane lub wpuszczane z ograniczonym dostępem.

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Oprogramowanie antywirusowe

Oprogramowanie złośliwe takie jak wirusy, robaki, trojany czy oprogramowanie szpiegowskie atakują naszą sieć lub nasze urządzenia infekując ich działanie.

Programy antywirusowe powinny wyszukiwać i zwalczać złośliwe aplikacje oraz dodatkowo śledzić zakażone pliki w celu odnalezienia anomalii czy zdalnie kontrolowanego złośliwego oprogramowania.

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Zapobieganie wypływowi danych

Firmy i stowarzyszenia muszą dbać o bezpieczeństwo wrażliwych informacji i uniemożliwić ich udostępnienie przez pracowników.

Technologie takie jak Data Loss Prevention (DLP) zapobiegają przesyłaniu, przekazywaniu czy nawet drukowaniu wrażliwych informacji.

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Bezpieczeństwo maili

Bramy poczty elektronicznej to miejsce, gdzie dochodzi do największej ilości naruszeń bezpieczeństwa.

Atakujący używają osobistych informacji i wyszukanych taktyk, aby zwieść i zainfekować odbiorcę. Aplikacje dbające o bezpieczeństwo maili blokują przychodzące ataki, jak i również kontrolują maile wychodzące.

2. Do jakich tematów odnosi się bezpieczeństwo w sieci

Zapory sieciowe

Zapory sieciowe to bariery stawiane między naszą zaufaną siecią a siecią zewnętrzną, taką jak Internet.

Ustalają one zasady, według których filtrują pakiety. Zapory mogą być oparte o software, hardware lub być rozwiązaniami hybrydowymi.

3. Zagrożenia w Internecie

- Cyberprzemoc
- Uzależnienie
- Niebezpieczne treści (przemoc)
- Łamanie prawa
- Kradzież danych osobowych
- Włamania komputerowe
- Zagrożenia techniczne (wirusy)
- Wyłudzanie poufnych informacji

3. Zagrożenia w Internecie

Cyberprzemoc

To zagrożenie polegające na wyrządzaniu krzywdy w sieci.

Do takich działań zalicza się m.in. wyzywanie, straszenie, czy poniżanie kogoś w Internecie. Może to odbywać się na przykład poprzez robienie komuś zdjęć bez jego zgody, a następnie publikowanie ich i rozsyłanie w sieci.

3. Zagrożenia w Internecie

Uzależnienia

Korzystając z Internetu, musisz sobie zdawać sprawę z zagrożeń, jakie mogą pojawić się podczas korzystania z jego usług.

Jednym z nich jest uzależnienie od Internetu, które może dotyczyć także i ciebie.

3. Zagrożenia w Internecie

Niebezpieczne treści

Wiele treści dostępnych w internecie ma charakter przemocy i negatywnie wpływa na psychikę zwłaszcza młodego odbiorcy informacji

3. Zagrożenia w Internecie

Łamanie prawa

Uważaj na strony, które proponują Ci wygraną niewielkim kosztem albo informują Cię, że zostałeś wylosowany i właśnie wygrałeś milion dolarów!

To podstęp!

3. Zagrożenia w Internecie

Kradzież danych osobowych

Wiele stron, zwłaszcza podejrzanych to takie, które wyłudzają Twoje dane. Np. proszą o hasło do bankowości elektronicznej

Włamania komputerowe

To jedno z częściej występujących zgrożeń.

Wydaje Ci się, że jak masz komputer w domu a dom ma dobre drzwi i niezawodny zamek, to nikt nie włamie Ci się na komputer?

Nic bardziej mylnego!

Wszystko odbywa się zdalnie!

Zagrożenia techniczne (wirusy)

Korzystając z komputera z dostępem do Internetu, jesteś narażony na ściągnięcie tzw. wirusów, czyli programów mających, w założeniu ich autora, uszkodzić twój komputer.

Mogą one skasować dane, wyłączyć komputer, odgrywać niepożądane dźwięki, spowodować wolniejszą pracę komputera, kraść informacje znajdujące się na dysku.

3. Zagrożenia w Internecie

Zagrożenia techniczne (wirusy)

Jednym z groźnych wirusów jest wirus nazwany koniem trojańskim, będący programem śledzącym twoje działania i pozwalający na kontrolowanie twojego komputera innym osobom.

Drugim, równie popularnym wirusem, jest tzw. robak, czyli program tworzący własne kopie. Jego działanie skutkuje, przede wszystkim, zmniejszaniem na dysku miejsca, które możesz wykorzystać na swoje potrzeby.

Wyłudzanie poufnych informacji

Internet wie o Tobie więcej niż myślisz, wystarczy, że śledzi odwiedzane przez Ciebie strony, wystarczy, że przestaniesz być czujny!

3. Zagrożenia w Internecie

Pamiętaj:

- Zbyt częste korzystanie z Internetu może spowodować uzależnienie od niego.
- Zainstaluj na komputerze program antywirusowy.
- Stosuj trudne do odgadnięcia hasła.
- W związku z zagrożeniami w sieci bądź ostrożny i nie podawaj wszystkich informacji o sobie oraz nie wysyłaj swoich zdjęć.
- Podczas przeglądania stron internetowych możesz spotkać się z próbami nawiązania kontaktu z tobą przez osobę podającą się za kogoś innego.

4. Czym jest antywirus

Program antywirusowy przesieje większą część wirusów, malwerów, koni trojańskich i innych zagrożeń, z tych które czyhają na każdego Internautę w sieci.

Dobry program antywirusowy stanowi pewnego rodzaju bufor pomiędzy zagrożeniami a codzienną pracą.

4. Czym jest antywirus

Nie tylko wirusy stanowią ciągłe zagrożenie, duże szkody mogą także wyrządzić precyzyjnie wymierzone ataki hakerów.

Przed tymi zagrożeniami chronić ma firewall.

Niestety nie wszystkie spośród programów antywirusowych dysponują takim modułem, pozostawiając te zadania systemowemu narzędziu Windows.

4. Czym jest antywirus

Największym źródłem ataków stają się portale społecznościowe, z których Facebook jest arcyzagrożeniem. Najbardziej bolesnym zagrożeniem dla Internauty są strony podszywające się pod banki, które potrafią przychwytywać numery kont bankowych, kart kredytowych czy numer PIN.

Bezpłatne programy nie chronią nas w ogóle! Nie wierzcie w to, że wystarczy pobrać polecany przez sąsiada bezpłatny program i wszystko załatwione.

5. Sposoby na zachowanie bezpieczeństwa w sieci

- **Hasła, Hasła, Hasła!** - to Twoje podstawowe i w zasadzie najważniejsze zabezpieczenie. Nie idź pod tym względem na łatwiznę i na przykład nie dodawaj wszędzie takiego samego hasła, np. daty urodzenia albo imienia swojego czworonoga. Silne hasło to zdecydowanie lepsze zabezpieczenie.
- **Zachowaj szczególną ostrożność wchodząc w linki** - częstym sposobem atakowania prywatności i wyciągania danych są rozsyłane na skrzynki pocztowe wiadomości e-mail, zawierające dziwne załączniki lub proszące o kliknięcie w jakieś linki. To tak zwany phishing. Nie istnieje jeden i do tego 100-procentowo pewny sposób na obronę. Najlepiej po prostu uważać i nigdy ich nie otwierać.

5. Sposoby na zachowanie bezpieczeństwa w sieci

- **Szyfrowanie plików na dysku -** Dysk Twojego komputera to mnóstwo cennych danych i informacji na Twój temat. Aby dobrze go zabezpieczyć, konieczne jest jego szyfrowanie.
- **Weryfikacja dwuetapowa -** Tam, gdzie konieczna jest weryfikacja, na przykład przy płatnościach internetowych, konieczna jest jej dwuetapowość. Czyli oprócz zalogowania się na danej stronie, ustaw sobie dodatkowo na przykład kod otrzymywany w wiadomości SMS.
- **Virtual Private Network -** VPN to rozwiązanie pozwalające na bezpieczne przesyłanie danych bez pokazywania lokalizacji.

5. Sposoby na zachowanie bezpieczeństwa w sieci

- **Tryb incognito -** Wybranie tego trybu wpływa na brak zapisywania historii przeglądarki i nie pokazuje lokalizacji.
- **DuckDuckGo** - to nazwa wyszukiwarki internetowej, która dużo lepiej w porównaniu z Google chroni dane użytkowników. Ma to jednak minus, ponieważ jej wyniki nie są tak precyzyjne.
- **Komunikatory szyfrujące -** Lubisz dużo pisać i to poprzez internet najczęściej kontaktujesz się ze znajomymi? W takim razie wykorzystaj komunikator, który szyfruje przesyłane teksty.
- **Wylogowywanie się i używanie pseudonimów -** Zawsze po skończonej pracy powinno się wylogowywać z danej strony oraz z komputera. Dotyczy to również korzystania z pseudonimów, które nie pozwalają na łatwą identyfikację swojej osoby oraz podawania w internecie jak najmniejszej ilości informacji na swój temat.

6. Ćwiczenia praktyczne

Dziękuję za uwagę