BEZPIECZEŃSTWO W SIECI

ADRIAN FLISEK ORAZ UCZNIOWIE:
DAWID CHLEWICKI, KL. II INF.; BARTOSZ BARAŃSKI, KL. I INF.; NATALIA SKŁADANOWSKA, KL. II G.

PLAN PREZENTACJI

1. WSTĘP
2. ZALETY INTERNETU
3. ZALETY INTERNETU CD.
4. ZAGROŻENIA W SIECI
5. JAK ZWIĘKSZYĆ SWOJE BEZPIECZEŃSTWO W SIECI?
6. PODSUMOWANIE I WNIOSKI
7. BIBLIOGRAFIA

1. WSTĘP

Początkowo Internet miał znacznie węższy zakres użytkowania. Wykorzystywany był głównie przez naukowców i wojsko.

Jednak postęp technologiczny sprawił, że sieć stała się dostępna dla każdego. Takie działanie wiąże się dla Nas ze znacznym udogodnieniem, ale nieostrożne użytkowanie Internetu może nieść za sobą poważne konsekwencje. [1]

1.1 INTERNET W CZASIE PANDEMII

Rok 2020 przyniósł wiele zmian w każdej dziedzinie życia.

Koronawirus ograniczył bezpośredni kontakt międzyludzki i zmusił Nas do odizolowania się od świata zewnętrznego.

Następstwem tego, szkoły oraz niektóre przedsiębiorstwa postanowiły uruchomić tzw „tryb zdalny”, który opiera się na wykonywaniu swoich obowiązków na odległość, m. in. za pomocą Internetu.

2. ZALETY INTERNETU

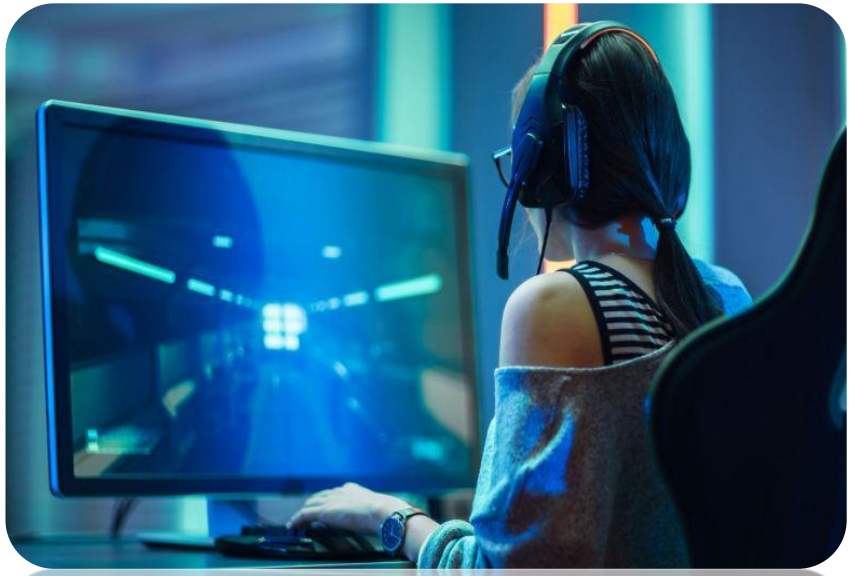
- łatwość i szybkość dostępu do mnóstwa informacji;
- możliwość komunikowania się z ludźmi niemalże na całym świecie;
- Internet jest narzędziem pracy wielu zawodów;
- dokonywanie zakupów w sklepach internetowych;
- ułatwienie regulacji wszelkiego rodzaju opłat; [2]

Źródło: https://www.freeimages.com/pl/premium/networking-comunication-connection-1474640, dostęp: 07.02.2021

3. ZALETY INTERNETU CD.

- udostępnianie serwisów takich jak: **YouTube**, **TikTok** czy **Vimeo**, które pozwalają na wypromowanie swojej twórczości na szeroką skalę;
- sieć oferuje mnogość serwisów streamingowych (np. **Netflix**, **Spotify**, itp.), telewizji internetowych (np. **Ipla.tv**), oraz platform dla graczy (np. **Steam**);
- możliwość pobierania plików dla własnego użytku.

[2]



Źródło: https://www.benchmark.pl/aktualnosci/jak-szybki-internet-do-gier.html, dostęp: 07.02.2021

Źródło: http://szkola-pawlokoma.pl/warsztaty-profilaktyczne-bezpieczni-w-sieci/, dostęp: 07.02.2021

4. ZAGROŻENIA W SIECI

4. 1. KRADZIEŻ DANYCH OSOBOWYCH

Kradzież danych osobistych często dokonuje się np. poprzez wyciek bazy danych.

Kolejną metodą na wyłudzenie naszych personaliów może być **Phishing**, czyli podszywanie się pod fałszywe osoby, firmy czy nawet instytucje (m.in. Urząd Skarbowy). Jest to szczególnie niebezpieczna forma kradzieży, ponieważ oszustwa zdarzają się drogą internetową, a także telefoniczną.

Ostatnio bardzo popularna była sprawa wyłudzenia 600 tys. zł. na leczenie amerykańskiego aktora.

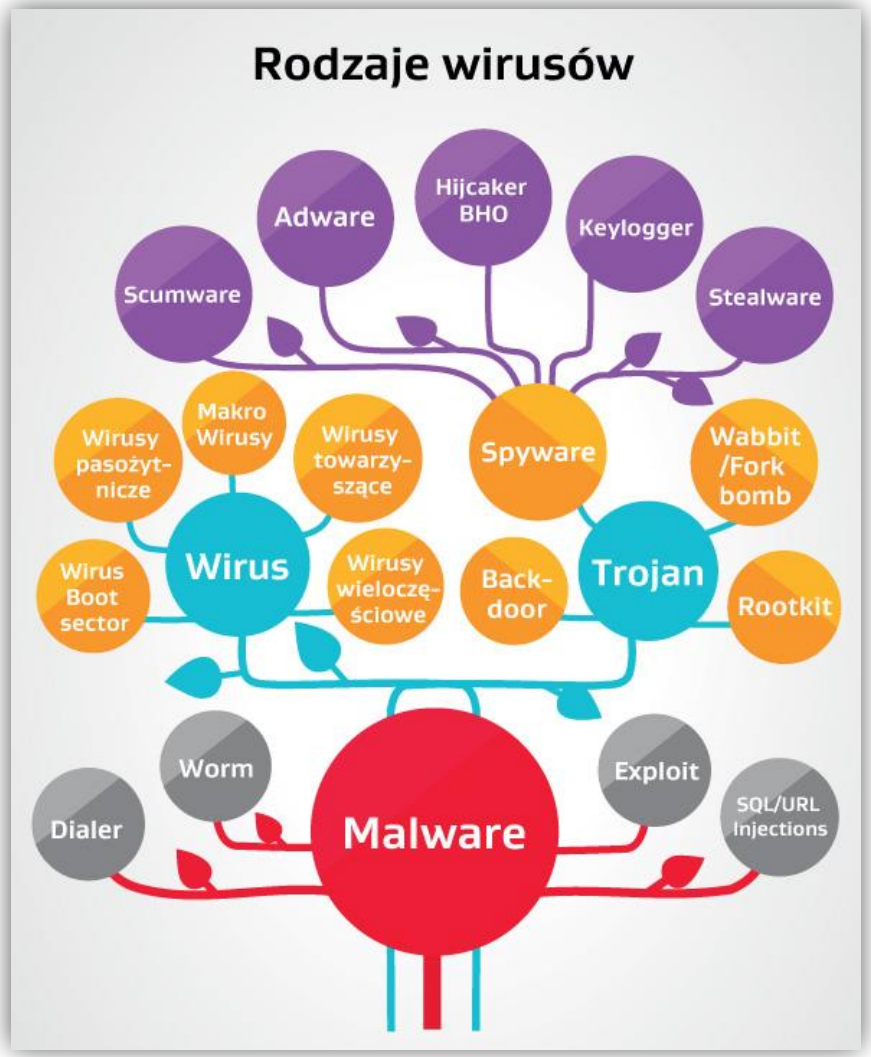
4. 2. WIRUSY KOMPUTEROWE

Wirusy komputerowe działają w różny sposób. Mogą powodować tylko drobne żarty graficzne. Niektóre z nich mogą się powielać, potrafią tworzyć tzw. „dziury" w naszych systemach, które osłabiają ochronę. Najgorsze z nich, są w stanie uszkodzić sprzęt lub wykraść dane.

Rodzaje wirusów komputerowych:

- **Malware** (Worm, Exploit, SQL/URL Injections, Dialer)- złośliwe oprogramowanie. W prosty sposób może dostać się na nasze urządzenie elektroniczne. Zwykle podczas pobierania aplikacji, zainfekowanych plików, lub zaakceptowaniu regulaminu zainfekowanej witryny. [3-4]

- **Trojany** (Wabbit, Backdoor, Rootkit)- podszywają się pod aplikacje i otwierane pliki, z których często korzystamy. [3-4]
- **Spyware** (Scumware, Adware, Hijacker BHO, Keylogger, Stealware)- to szkodliwe oprogramowanie szpiegujące, które ma na celu gromadzenie danych o użytkowniku oraz przesyłanie ich bez jego wiedzy innym osobom. [3-4]



Źródło: https://trybawaryjny.pl/rodzaje-wirusow/ , dostęp: 07.02.2021

4. 3. BRAK PRYWATNOŚCI

Problem niewątpliwie bardzo istotny w czasach świetności wszelakich portali społecznościowych. Co za tym idzie – bardzo łatwa możliwość namierzenia osób, czy też nawet wyśledzenia ich w realnym życiu tj. **stalking.**

4. 4. HAKERZY I ATAKI HAKERSKIE

Hakerami określamy osoby, które próbują się przedostać do cudzych urządzeń lub systemów aby wykraść dane i pliki, a nawet w celu wyżej wspomnianego stalkingu.

4. 5. MROCZNA STRONA INTERNETU

W Internecie jest ogromna ilość treści nieodpowiednich dla osób niepełnoletnich i niestety żadna lub niewielka ochrona przed dostępem do takich stron.

Warto zauważyć, że na co dzień korzystamy z niewielkiego procentu Internetu. Większość zasobów jest dla nas niewidoczna i dostępna tylko za pomocą specjalnych metod.

Chodzi tu kolejno o terminy takie jak: **deep web** i **dark web**, w których znajdują się skradzione bazy danych, dokumenty rządowe czy nawet nielegalne działalności zajmujące się handlem bronią, ludźmi, używkami.

4. 6. CYBERPRZEMOC

Może się objawiać w różny sposób. Wyśmiewanie prześladowanej osoby w Internecie, podszywanie się pod nią czy też nękanie jej, to tylko niektóre z możliwych wariantów takiego aktu przemocy.

Wymieniona na wcześniejszym slajdzie zaleta, dotycząca łatwej komunikacji z innymi, ma też swoje wady. Poznając nowe osoby w Internecie nigdy nie mamy pewności z kim rozmawiamy w danym momencie, więc nie jest trudno zawrzeć niebezpieczne znajomości. Ma to związek z nieustannym problemem **pedofilii**.

4. 7. FAKE NEWS

Duża liczba nieprawdziwych informacji – spora swoboda w Internecie ma też swoje wady.

Jedną z nich jest możliwość umieszczania wiadomości w zasadzie przez każdego użytkownika, które bywają sprzeczne z prawdą. Niestety, często weryfikacja takich publikacji może trwać zbyt długo, co może doprowadzić do wielu nieprzyjemnych okoliczności.

Za przykład niech posłuży przedwczesne ogłoszenie informacji o zgonie zagranicznej celebrytki.

4. 8. PIRACTWO

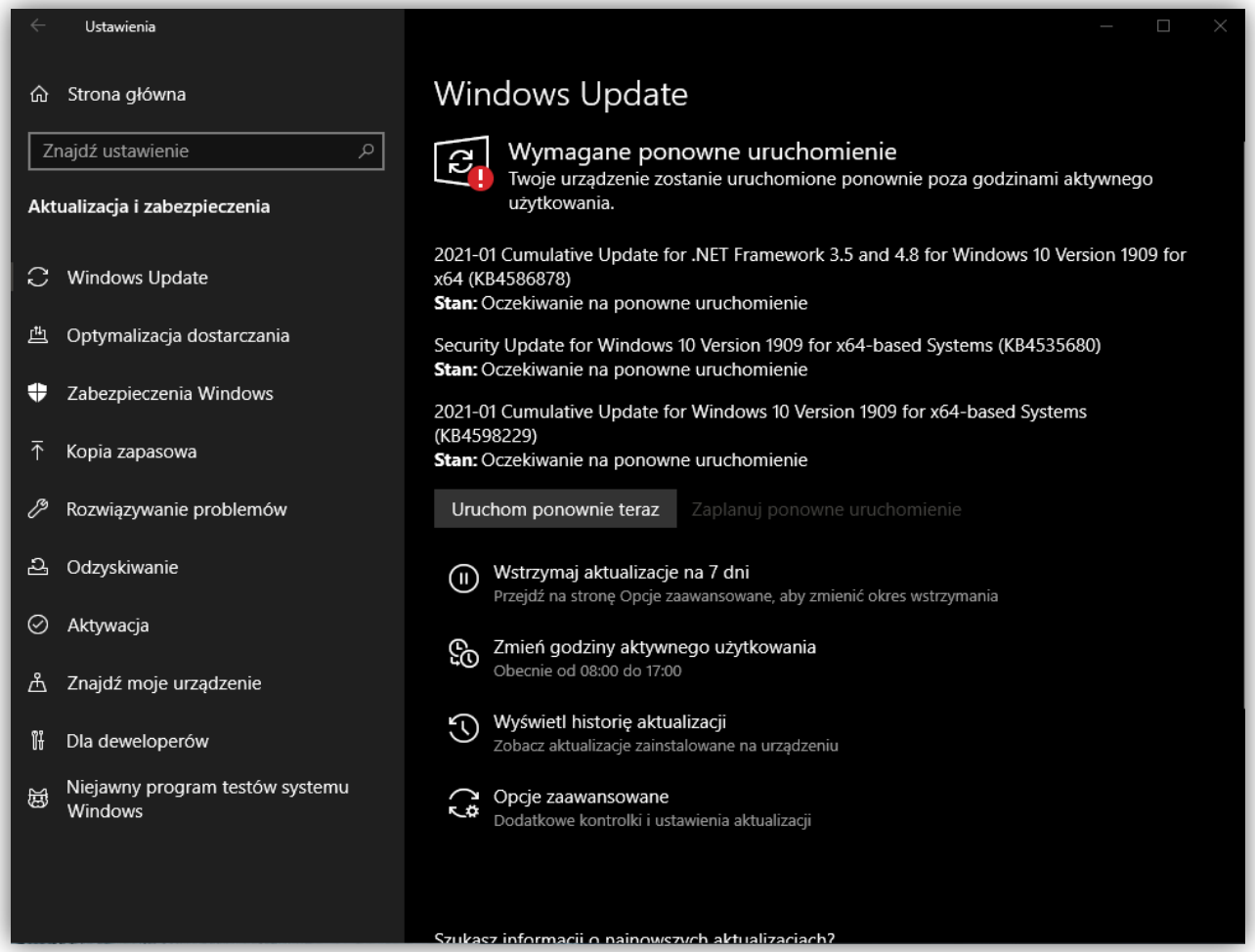
Piractwo komputerowe– nielegalne rozpowszechnianie plików i programów.

Warto zauważyć, że korzystanie z programów **P2P** (oprogramowanie służące do wymiany plików między użytkownikami) jest zawsze niezgodne z prawem, ponieważ nawet ustawiając wartość wysyłania na „0” w dalszym ciągu udostępniamy jakiś fragment danego pliku.

Źródło: https://panwybierak.pl/blog/bezpieczny-internet-jak-dbac-o-bezpieczenstwo-w-sieci/ , dostęp: 08.02.2021

5. JAK ZWIĘKSZYĆ SWOJE BEZPIECZEŃSTWO W SIECI?

5. 1. AKTUALIZACJE

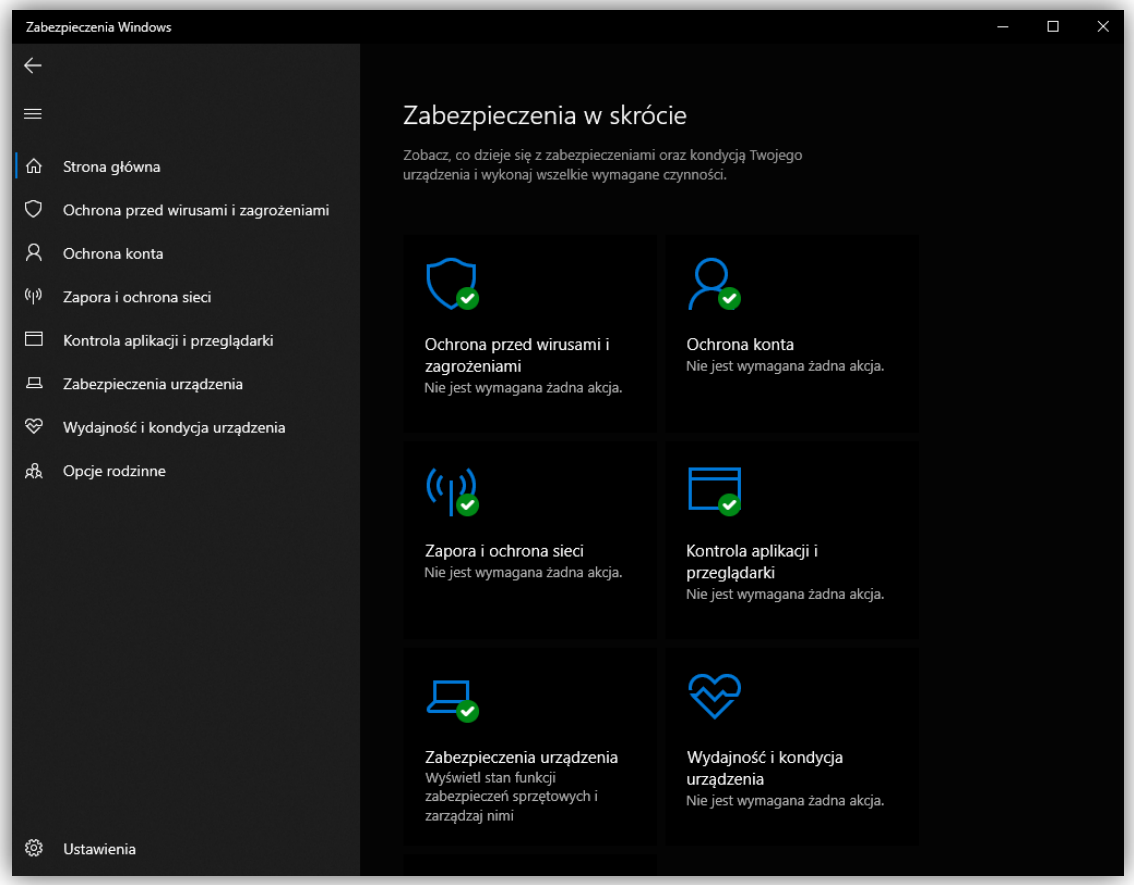


Należy pamiętać o aktualizacjach systemu i poprawkach bezpieczeństwa.

Domyślnie aktualizacje są wykonywane automatycznie, ale możemy sprawdzić to samemu.

W tym celu wchodzimy w **Ustawienia** > **Aktualizacja i zabezpieczenia** > **Windows Update**.

5. 2. ANTYWIRUS

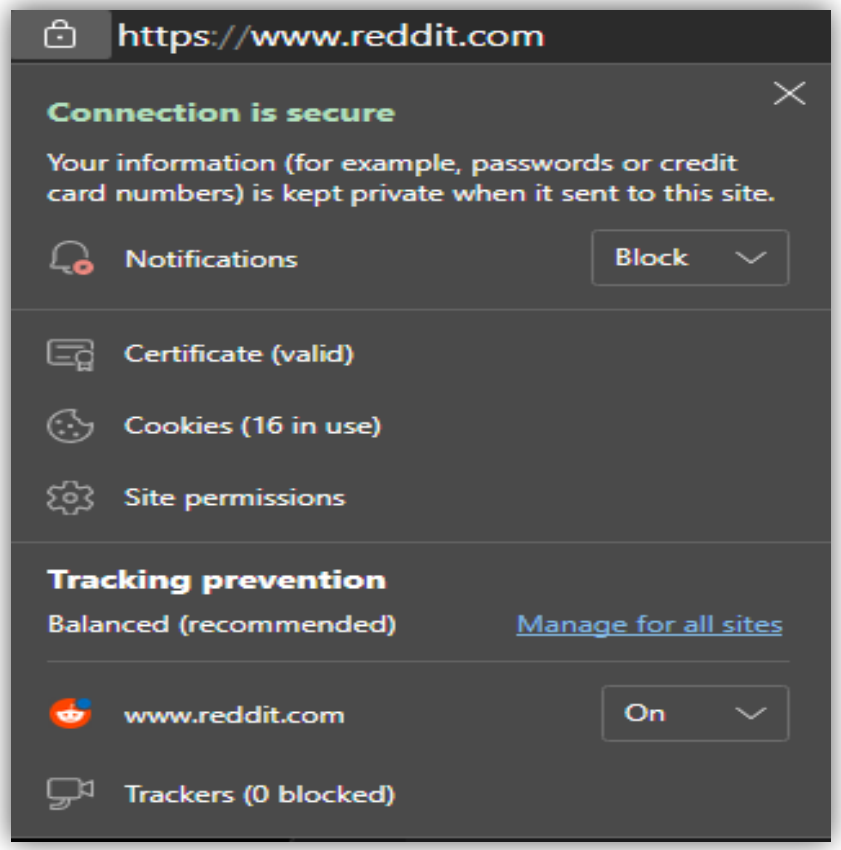


Dla użytkowników Windowsa 10 najkorzystniejszym rozwiązaniem będzie domyślny **Windows Defender**. Jest to propozycja dla osób, które używają komputera do codziennych zadań.

Należy pamiętać, że żaden antywirus nie jest w stanie nam zapewnić całkowitej ochrony.

Dlatego korzystając z komputera musimy być rozważni. Aby przejść do okna Defendera musimy wejść w Ustawienia > Aktualizacja i zabezpieczenia > Zabezpieczenia Windows > Otwórz usługę Zabezpieczenia Windows.

5. 3. SZYFROWANIE DANYCH

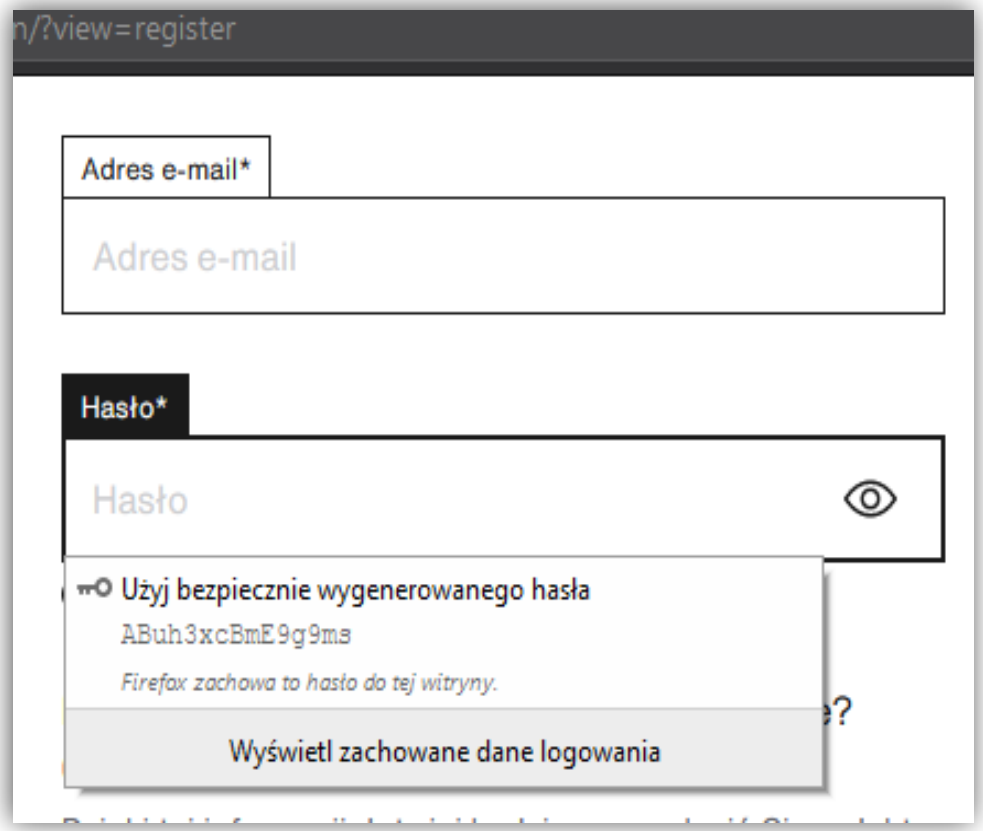


Na stronach internetowych istotne jest, aby zwracać uwagę czy strony są szyfrowane – **protokół https.**

Jest to w szczególności ważne, gdy korzystamy ze stron, na których podajemy swoje dane osobowe.

Strony nieszyfrowane posiadają **protokoły http.**

5. 4. SIŁA HASŁA



Bezpieczne hasła powinny zawierać ok. **15 znaków, małe, duże litery, znaki specjalne („@”, „$”, „!”…) i cyfry.**

Istnieje także możliwość skorzystania z automatycznych generatorów haseł.

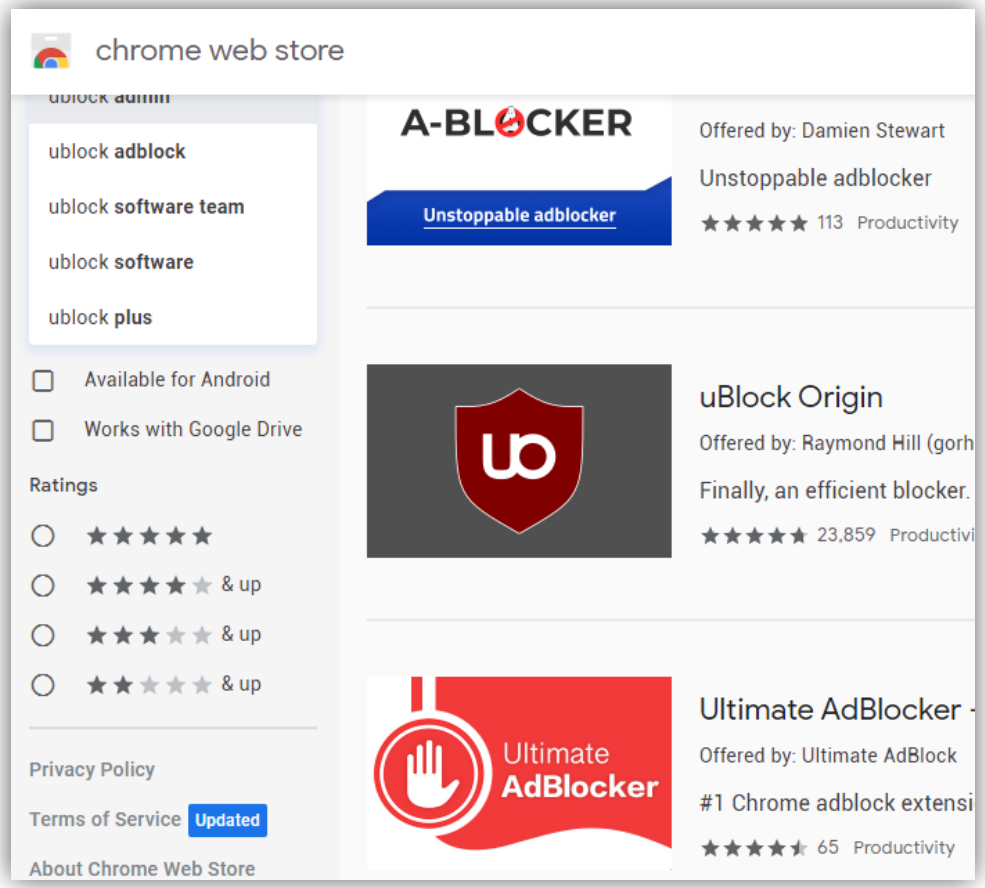
Hasła powinny być często zmieniane.

Nie należy:

- zapamiętywać haseł w przeglądarce;
- używać słów popularnych i uniwersalnych;
- stosować imion, znaczących dat i nazw;
- używać takiego samego hasła do różnych serwisów.

[5]

5. 5. ROZSZERZENIA DO PRZEGLĄDARKI



Aby pozbyć się reklam czy też wyskakujących okienek podczas przeglądania stron internetowych warto zainstalować rozszerzenia blokujące.

Do najbardziej popularnych należą: AdBlock, uBlock.

Dla dodatkowej ochrony możemy zaopatrzyć się we wspomagające rozszerzenie Nano Defender (dla użytkowników Firefox).

Aby zainstalować wyżej wymienione dodatki, musimy skorzystać ze strony **Chrome Web Store** lub **Firefox Add-ons**

5. 6. KOPIE ZAPASOWE

Tworzenie kopii zapasowej jest istotnym elementem w zapobieganiu utraty ważnych plików, dokumentów i innych informacji.

Ponadto warto wykonywać kopię systemu naszego komputera lub smartfona.

Kopie zapasowe możemy zapisywać na dyskach przenośnych, płytach, pamięciach flash (np. pendrive).

Trzeba być świadomym też tego, że żadna z powyższych metod nie gwarantuje stuprocentowego bezpieczeństwa, a jedynie jest dodatkowym zabezpieczeniem.

5. 7. SIECI PUBLICZNE

Nie zaleca się korzystania z nieznanych, ogólnodostępnych sieci Wi-Fi takich jak np. Hotspoty w centrach handlowych, w pociągach, itp.

Takie działanie może skutkować kontrolowaniem naszych poczynań w Internecie.

Jeżeli już zdecydujemy się na połączenie z taką siecią, pamiętajmy o tym aby nie podawać żadnych poufnych danych.

Źródło: https://plblog.kaspersky.com/8-zasad-bezpieczenstwa-dla-uzytkownikow-publicznych-sieci-wi-fi/4067/ , dostęp: 08.02.2021

6. PODSUMOWANIE I WNIOSKI

W dzisiejszych czasach funkcjonowanie bez dostępu do Internetu jest w zasadzie niemożliwe. Jest to największe medium przesyłu informacji, które bez wątpienia ułatwia nam życie.

Jednak Internet nie jest wynalazkiem idealnym i ma też swoje wady. Ze względu na to, że jest szeroko dostępny nikt nie jest w stanie go w pełni kontrolować i może być używany do celów niemoralnych i nielegalnych.

Dlatego zachowujmy ostrożność, zwracając uwagę na wskazówki dotyczące bezpiecznego użytkowania Internetu.

7. BIBLIOGRAFIA

1. materiały dydaktyczne pozyskane z zajęć w szkole wyższej;

2. http://www.sp3.jozefow.pl/zalety.html;

3. https://marken.com.pl/2020/12/12/rodzaje-wirusow-komputerowych/

4. https://trybawaryjny.pl/rodzaje-wirusow/

5. http://www.zikom.com.pl/bezpieczne-hasla/