ZAGROŻENIA PŁYNĄCE Z INTERNETU

MARTYNA DUŻYŃSKA

KL VII A

Jakie mogą być zagrożenia w Internecie dla dzieci, młodzieży, a jakie dla dorosłych?

Najczęstsze zagrożenia w Internecie, które dotyczą wszystkich użytkowników sieci to wirusy. Można zarazić komputer lub smartfon zupełnie nieświadomie, klikając w nieznany link lub nawet otwierając e-maila od nieznajomej osoby. Ale to niestety nie wszystkie niebezpieczeństwa.

NAJCZĘSTSZE ZAGROŻENIA W INTERNECIE – TO WIRUSY

Wirusy, czyli złośliwe oprogramowanie atakujące komputery i telefony, dostają się do naszych urządzeń najczęściej właśnie przez Internet.

Nie pojawiają się znikąd najczęściej przychodzą do nas jako załączniki spamowych e-maili.

Mogą zainfekować nasz komputer, jeśli wejdziemy na podejrzaną stronę, klikniemy niepewny link albo będziemy chcieli zainstalować oprogramowanie z Internetu nie sprawdzając, czy strona, która je oferuje jest autentyczna.

Wirusy mogą infekować także pamięci zewnętrzne , czyli „zarazić” się może także komputer czy telefon bez podłączenia do Internetu. Wystarczy podłączyć np. wymienny dysk z wirusem czy nawet odtwarzacz mp3.

DLACZEGO WIRUSY SĄ NIEBEZPIECZNE ?

- Mogą wyrządzić przeróżne szkody na komputerze i telefonie, m.in.:

- ❖ wykraść nasze poufne informacje,
- ❖ zniszczyć dane, jakie mamy na dysku,
- ❖ za pomocą naszego adresu e-mail wysyłać spam do naszych kontaktów,
- ❖ zaszyfrować nasze dane i wymuszać okup za ich odszyfrowanie,
- ❖ sprawdzić historię naszego przeglądania i wymuszać okup, jeśli np. mamy w historii serwisy pornograficzne,
- ❖ wysyłać smsy typu premium z naszego telefonu,
- ❖ przekazywać informacje o naszym położeniu hakerom.

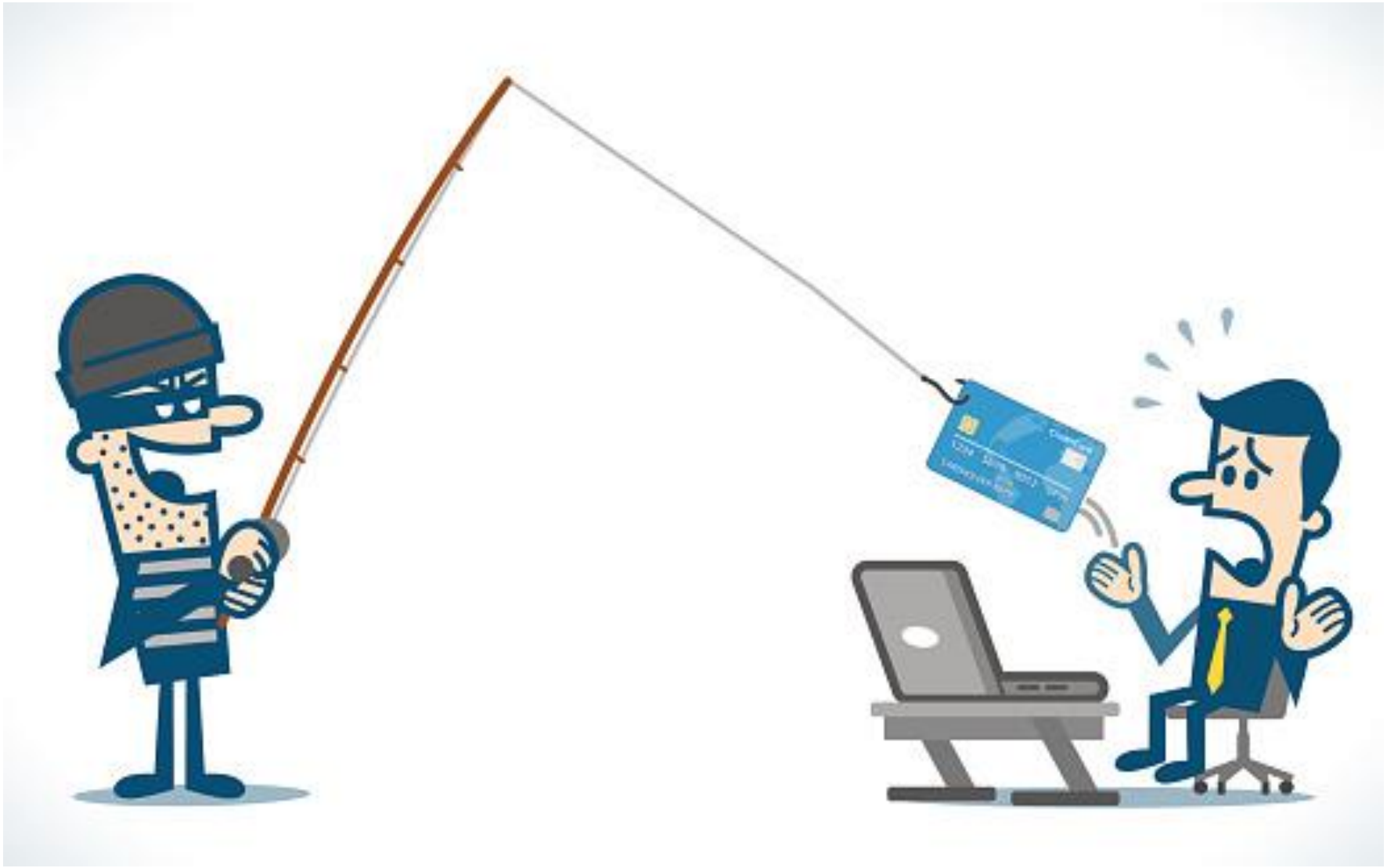
Zagrożenia w sieci Internet – phishing.

Termin phishing pochodzi od angielskiego password harvesting fishing , co oznacza **„łowienie haseł”.**

Do phishingu niekoniecznie są wykorzystywane wirusy. Wystarczy wiadomość e-mail z linkiem i strona wyglądająca na autentyczną – czy to będzie strona banku, czy aukcji internetowych.

Przestępcy wysyłają wiadomości e-mail do wielu osób, podszywając się pod bank lub serwis aukcyjny i przekierowują użytkowników na swoją stronę, wyglądającą dokładnie tak, jak autentyczna (może różnić się np. tylko jedną literą w adresie).

Kiedy internauta wpisze swoje dane logowania – przestępca może je wykorzystać do swoich celów.



ZAGROŻENIA W SIECI DLA DZIECI I MŁODZIEŻY

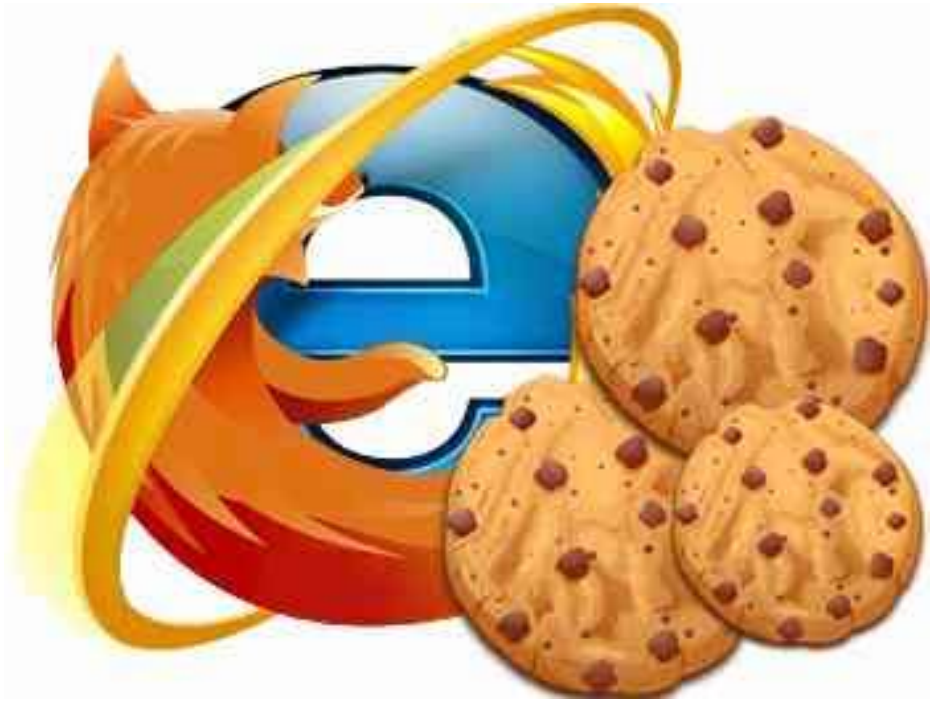
Zagrożenia w sieci dla dzieci i młodzieży wiążą się z dostępem do nielegalnych i szkodliwych dla nich treści. Chodzi o strony pornograficzne, neonazistowskie, ksenofobiczne, rasistowskie, promujące różnego rodzaju sekty, a także zdjęcia i filmy przedstawiające przemoc, materiały zachęcające do korzystania z używek czy eksperymentowania na własnym zdrowiu.

Innym zagrożeniem dla dzieci i młodzieży w Internecie jest możliwość kontaktu z nieznajomymi osobami, które mogą okazać się niebezpieczne. **Uwodzenie dzieci przez Internet nosi nazwę groomingu .**

SPAM – NIECHCIANA POCZTA

Spam (określany także jako wiadomości śmieci), powinna być jedynie czynnikiem irytującym. Jednak często w tych pozornie nieszkodliwych treściach kryją się niebezpieczne szkodniki.

Cyberwłamywacze liczą, że przez pomyłkę lub z ciekawości otworzymy zainfekowany załącznik, co niestety dość często ma miejsce.



FAŁSZYWE LAJKI I CIASTECZKA

W sieciach społecznościowych często podążamy za nawykami znajomych. To znakomita okazja dla hakerów, którzy umieszczają na stronach kody wymuszające ich polubienie.

My widząc na tablicy, że ktoś znajomy polubił interesujący nas temat, klikamy na link i kłopot gotowy.

Z kolei w przypadku powiadomień o ciasteczkach (cookies) czujemy się zobligowani kliknąć i nawet nie sprawdzamy, czy faktycznie zatwierdzamy politykę ciasteczkową, czy coś całkowicie innego.

A może się zdarzyć, że klikając na niewinnie wyglądające powiadomienie, zaakceptujemy niekorzystny dla nas regulamin jakiejś usługi.

" TWÓJ KOMPUTER JEST ZAINFEKOWANY , SKORZYSTAJ Z NASZEGO OPROGRAMOWANIA''

To jedno z haseł kluczy, które w przypadku naiwnych internautów otwiera drogę cyberprzestępcom do komputerów ofiar.

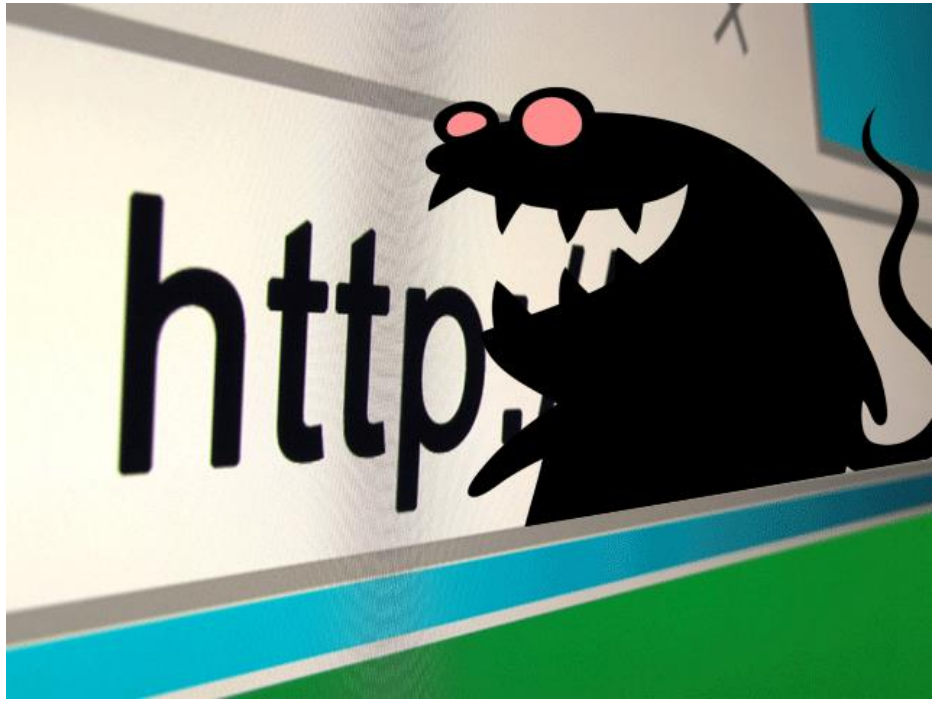
Jednakże i ostrożna osoba może stać się ofiarą, gdy zdecyduje się pobrać z Internetu jedną z aplikacji antywirusowych, która jest chwalona przez innych internautów.

W rzeczywistości taki fałszywy antywirus jedynie udaje działanie prawdziwego programu.

Wyświetla nawet udawane komunikaty o wykryciu i usunięciu wirusów, w tle jednak działając na naszą szkodę.

SKRÓCONE ADRESY URL

Kolejna forma ułatwienia życia w bogatym w treści Internecie, którą chętnie wykorzystują przestępcy. Adresy stanowiące skróconą alternatywę dla długich oryginalnych adresów, są łatwiejsze do zapamiętania, zajmują mniej miejsca w korespondencji. Zarazem jednak nie wskazują jednoznacznie, dokąd prowadzą, a często kierują do szkodliwej witryny.



LITERÓWKI W ADRESACH WWW

Wpisując szybko adres strony na klawiaturze nietrudno o pomyłkę, przestawienie liter lub zapomnienie o wpisaniu danego znaku.

I choć szanujący się operatorzy witryn sieciowych dbają o rejestrację podobnie brzmiących adresów, nie jest to regułą.

Zresztą liczba alternatyw jest tak duża, że trudno przewidzieć jak pomyli się internauta.

Otworzenie witryny o podobnie brzmiącej nazwie czasem prowadzi do nic nieznaczącej strony z reklamami, ale czasem może kompletnie zablokować komputer.

OTWARTE SIECI Wi - Fi

Niebezpieczne są na dwa sposoby.

W pierwszym przypadku dotyczy to konfigurowanych przez nas domowych sieci, które nie są w żaden sposób zabezpieczone i dają dostęp niepowołanym osobom nie tylko do Internetu, ale także do naszych danych.

Drugi scenariusz to korzystanie przez nas z otwartych sieci Wi-Fi, o których kompletnie nic nie wiemy. Choć tworzenie takich sieci ma służyć ułatwieniu dostępu do Internetu, często taka droga na skróty może być opłakana w skutkach, gdyż kompletnie nie wiemy, kto kontroluje przepływ danych przez taki punkt dostępowy.

Inne zagrożenia w Internecie

Gracze w gry MMO (Massive Multiplayer Online) są narażeni na ataki cyberprzestępców, którzy tworzą programy do przejmowania ich postaci.

Robią to po to, by ukraść przedmioty, które w tego typu grach kupuje się za prawdziwe pieniądze lub po żmudnych przygotowaniach i rozwoju postaci.

Samą postać i przedmioty przestępcy mogą wystawić później na sprzedaż i dostać za nie prawdziwe pieniądze.

Ostatnie z niebezpieczeństw, jakie na nas czyhają, mają swoje źródło w przekonaniu, że nasze urządzenie i posiadane oprogramowanie doskonale potrafi sobie poradzić z każdym zagrożeniem.
W praktyce często człowiek nie zdaje sobie sprawy z różnorodności technik cyberprzestępczych. Wiara we własne umiejętności sprawia, że ignorujemy rzeczywiste sygnały o zagrożeniu.
Wciąż nie znamy podstawowych reguł bezpiecznego korzystania z sieci.
Niestety, nawet najbardziej zaawansowan technologie wykorzystywane przez portale, e-sklepy, poczty e-mail czy banki, nie zabezpieczają nas całkowicie przed zagrożeniami, jakie niesie Internet.
Dlatego jednym z najlepszych narzędzi zabezpieczających nasze urządzenia, dane oraz prywatność jest **zdrowy rozsądek**

Aby być bezpiecznym w Internecie i zapewnić bezpieczeństwo sobie i swoim bliskim musimy przestrzegać poniższych zasad:

- Regularnie aktualizujemy oprogramowanie i system operacyjny.
- Instalujemy program antywirusowy z firewallem i pilnujemy, aby zawsze był aktualny.

- Nigdy nie otwieramy e-maili nieznanego pochodzenia, nawet jeśli nadawca ma zbliżony adres np. do naszego banku. Prawdziwe serwisy zwykle nie proszą za pomocą e-maili o ponowne zalogowanie się. Nie klikamy w takie linki.
- Nigdy nie klikamy w linki co do których nie mamy pewności.
- Do każdego serwisu, społecznościowego, bankowego, ale i takiego z grami (szczególnie jeśli wpłacamy tam jakiekolwiek pieniądze) mamy inne hasło – nie brzmiące „12345678”!

- Nigdy nikomu nie podajemy swoich haseł i loginów, nie przesyłamy ich przez Internet.
- Zawsze przed wpisaniem hasła i loginu do strony (szczególnie banku) sprawdzamy w oknie, czy adres strony się zgadza.
- Nie korzystamy w hot-spotów niewiadomego pochodzenia.
- Nie przesyłamy przez Internet swoich intymnych zdjęć czy filmów.