

ZSSUEKA



Luty 2021

WEDANIE SPECJALNE



Dzień
Bezpiecznego
Internetu

2021 | Wtorek
9 lutego



GDZIE SZUKAĆ POMOCY W PRZYPADKU ZAGROZEŃ W INTERNECIE?

PIERWSZYM WAŻNYM KROKIEM JEST ZAWIADOMIENIE OSOBY DOROSŁEJ, MOŻE TO BYĆ RODZIC, ZAUFANA I BLISKA CI OSOBA, PEDAGOG SZKOLNY LUB NAUCZYCIEL.

SPOKOJNA ROZMOWA I OPISANIE OSOBIE SYTUACJI, W KTÓREJ SIĘ ZNALEŻLIŚMY JEST NIEZBĘDNĄ RZECZĄ W WYJAŚNIWIU SPRAWY.

JEŚLI BOISZ LUB WSTYDZISZ SIĘ POROZMAWIAĆ ZE ZNAJOMĄ CI OSOBĄ MOŻESZ ZADZWONIĆ NA:

Telefon Zaufania dla Dzieci i Młodzieży:

116 111 - *Bezpłatna i anonimowa rozmowa dla dzieci i młodzieży*

Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka:

800 12 12 12 - *Bezpłatna rozmowa*

112 – Jednolity numer alarmowy obowiązujący na terenie całej Unii Europejskiej

Jeżeli uważasz, że doszło do przestępstwa należy zawiadomić policję! - 997

Magda Szczepanik kl. VIIb

Zapraszamy do współpracy z naszą redakcją! Wszelkie zapytania i sugestie prosimy kierować na naszą skrzynkę e-mail: gazetka@zssso-skierniewice.pl

NASZ ULUBIONY INTERNET—CZYLI JAKI?

Internet, czyli niewątpliwie największy wynalazek w historii ludzkości, jest także nieodzownym i nieodłącznym elementem życia każdego nastolatka. Bo chociaż mamy różne zainteresowania, pasje, talenty, to wszystkich nas – młodych ludzi – łączy (w sensie przenośnym, ale i dosłownym też!) Internet.



Dlatego opowiadanie nastolatkom, do czego służy Internet, jest zadaniem łatwym i trudnym jednocześnie. Łatwym, bo wszyscy korzystamy z sieci: używamy komunikatorów (np. Messenger, WhatsApp), przeglądamy portale społecznościowe (m.in. Facebook, TikTok, Instagram), słuchamy muzyki (np. Tidal lub Spotify), oglądamy filmy i programy (YouTube, Netflix, Amazon Prime Video i inne), wysyłamy do siebie e-maile (czyli tzw. „pocztę elektroniczną” - kto dziś tak jeszcze mówi, prawda?), a z powodu pandemii koronawirusa, od blisko roku uczestniczymy w lekcjach online (platforma Microsoft Teams). Jeżeli dodamy do tego zakupy w sieci, dostęp do konta w banku oraz możliwość wyszukiwania przepisów kulinarnych (polecam blog tocoinnego.pl), miejsc na wakacje (Booking.com, AIRBNB), czy rezerwację biletów na imprezy sportowe i koncerty oraz do kin i teatrów (eBilet, Ticketmaster), to okazuje się, że większość codziennych spraw jesteśmy w stanie załatwić przy pomocy Internetu!

Ale Internet to jednocześnie wielka i nie do końca zbadana przestrzeń. Dlaczego? Przede wszystkim ze względu na to, że utrzymywanie kontroli nad tym, co nazywamy „globalną siecią” jest niezwykle trudnym zadaniem. Wyobraźcie sobie, że nie ma sposobu, by wyłączyć Internet! Nie chodzi mi tutaj o irytujący brak dostępu, związany z przerwami lub usterkami technicznymi. Po prostu, gdyby zdarzyło się, że Internet zostaje opanowany przez wirusa, który niszczy urządzenia: komputery, tablety, telefony komórkowe, to nie istnieje żadna agencja, urząd lub firma, która ma możliwość wyłączenia sieci, by infekcja się nie rozprzestrzeniła.

Drugim problemem, jaki trzeba brać pod uwagę jest istnienie fałszywych stron, podszywających się pod znane i bezpieczne portale internetowe. Podobnie jak w przypadku tzw. „fake newsów”, czyli nieprawdziwych informacji zamieszczanych w mediach społecznościowych, które „udają” wiadomości pochodzące z wiarygodnych źródeł, istnieje wiele serwisów internetowych, które oferują fałszywe programy, np. darmowe wersje poszukiwanych gier.

Takie strony internetowe nie różnią się często od sprawdzonych serwisów, a skorzystanie z ich oferty w najlepszym razie kończy się „zhakowaniem” naszych kont pocztowych lub tych w social mediach i zasypywania nas niechcianymi ofertami handlowymi lub innym „spamem”. W gorszym scenariuszu może prowadzić do wykradzenia listy kontaktów lub zniszczenia plików i dokumentów, zapisanych w naszych komputerach.

Mniej dokuczliwe, ale dość ryzykowne może być używanie znanych portali, które mogą nam pomagać (a czasem wyręczać nas) w nauce. Jest ich stosunkowo dużo i nie wymienię ich nazw, bo większość z nas zna je doskonale i często z nich korzysta. Ale... po pierwsze: skoro my je znamy – znają je również nauczyciele i łatwo mogą sprawdzić, skąd pochodzą np. nasze prace domowe, a po drugie: to, że ktoś zamieszcza rozwiązanie zadania albo opracowanie lektury, nie oznacza wcale, że nie popełnił tam błędu. Dlatego lepiej sprawdzać i porównywać swoje rozwiązania, niż polegać w 100% na propozycjach znalezionych w Internecie.

Warto również pamiętać, że zawartość Internetu – pomimo iż jest on siecią globalną – różni się w zależności od kraju oraz kontynentu, w którym jest używany. Dlatego korzystając z przeglądarek (np. Google), opartych na sieci serwerów zarejestrowanych jako polskie, otrzymamy inne wyniki wyszukiwania, niż kiedy będziemy używać tych samych portali za granicą. O ile nie stanowi to problemu przy przeglądaniu stron z informacjami, o tyle np. robienie zakupów z wykorzystaniem stron dedykowanych dla internatów zagranicznych, może prowadzić do sytuacji, w której będziemy chcieli skorzystać z promocji, która albo nie działa dla klientów z Polski albo działa wyłącznie na naszym, krajowym rynku, ale nie jest możliwa do zrealizowania przez np. niemiecką czy francuską stronę wybranego sklepu lub sieci handlowej. Przy okazji warto wspomnieć, że katalog filmów Netflix'a również może się zmienić, gdy będziemy używać Internetu za granicą, więc jest możliwe, że nie znajdziemy tam swoich ulubionych pozycji. Natomiast jeżeli mamy możliwość połączenia poprzez tzw. VPN, czyli wirtualną sieć prywatną, która jest specjalnym „tunelem”, przez który odbywa się komunikacja pomiędzy nadawcą i odbiorcą w Internecie, po zmianie lokalizacji na amerykańską, możemy uzyskać dostęp do oferty DisneyPlus, która nie jest jeszcze obecna w Polsce.

NASZ ULUBIONY INTERNET—CZYLI JAKI?

Chciałabym na koniec przedstawić Wam kilka zasad, jakie mogą być przydatne, by korzystanie z Internetu było nie tylko przyjemne, ale i bezpieczne dla nas – użytkowników i dla urządzeń, których używamy. Korzystam tutaj z pomocy serwisu Sieciaki.pl, który promuje najlepsze praktyki związane z pracą i zabawą w sieci.



Po pierwsze: chrońmy swoją prywatność! Nigdy nie należy podawać swoich danych osobowych, takich jak: imię, nazwisko, numer telefonu czy adres domowy. Najlepiej omijać strony internetowe, które wymagają podania adresu e-mail lub innej formy rejestracji, by umożliwić skorzystanie z plików lub programów.

Po drugie: dbajmy o swój wizerunek. Jeśli mamy zamiar publikować w sieci swoje zdjęcia, zadbajmy, by widzieli je tylko nasi znajomi. Nie umieszczajmy w Internecie zdjęć, które mogą nam zaszkodzić – nawet jeżeli dziś nie wydają się niestosowne.

Po trzecie: zgłaszajmy rodzicom i opiekunom niepokojące sytuacje związane z używaniem Internetu. W trudnej sytuacji możemy kontaktować się z Telefonem Zaufania dla Dzieci i Młodzieży, dzwoniąc pod bezpłatny numer 116 111.

Po czwarte: nie należy na 100% ufać osobom poznanym w sieci, ani spotykać się z nimi! O propozycjach spotkania od internetowych znajomych informuj rodziców.

Po piąte: szanujmy innych użytkowników sieci! Traktujmy ich z szacunkiem, a swoje opinie o innych osobach wyrażajmy tak, by nikogo nie obrazić.

Po szóste: dbajmy o higienę naszych urządzeń. Nie ściągajmy plików ze stron, które nie są zabezpieczone certyfikatem bezpieczeństwa (czyli nie posiadają znaczka zamkniętej kłódki przy adresie w przeglądarce). W każdym przypadku, kiedy pobieramy plik z programem, dokumentem, plikiem dźwiękowym lub filmem, sprawdzajmy go programem antywirusowym.

Po siódme: bądźmy bezpieczni! Nie łączmy się z bankiem ani nie dokonujemy zakupów w sieci, kiedy korzystamy z otwartych sieci WiFi – np. w restauracjach, centrach handlowych lub tzw. sieci miejskich. Są one bardzo podatne na działania hackerów, którzy w takiej sytuacji bez wysiłku mogą przejąć nasze dane logowania i dostać się do naszych kont i urządzeń.

Najkrócej mówiąc – stosujmy zasadę złotego środka:
nie bagatelizujemy zagrożeń i starajmy się jak najpełniej wykorzystać bogactwo skarbcza naszego ulubionego Internetu.

Hania Wojciechowska, klasa VII B

ZAGROŻENIA ZWIĄZANE Z KORZYSTANIEM Z INTERNETU

Każdy z nas codziennie korzysta z Internetu czy mediów społecznościowych. Zwłaszcza teraz w dobie pandemii, kiedy dorośli pracują zdalnie a dzieci mają szkołę online. Natomiast mało kto zastanawia się nad zagrożeniami z tym związanymi.



Uzależnienie

Tak to też jest zagrożenie. Jeśli ktoś siedzi w Internecie całe dni, uzależnia się od tego. Nieleczone uzależnienie prowadzi do wielu chorób a nawet śmierci. Dlatego lepiej ograniczać czas spędzony na mediach społecznościowych. Zamiast tego lepiej pobawić się z psem lub poczytać książkę.

Utrata danych

Wielu ludzi dostaje maile z banku, pracy itp. miejsc. Ale czy wszystkie są prawdziwe? Nie zawsze. Czasami hakerzy wysyłają takie maile imitujące te z banków czy sklepów. Proszą by wchodzić w jakieś linki. Wchodząc w nie możemy ściągnąć na nasz komputer aplikacje śledzące lub go zawirusować. Dlatego lepiej nie wchodzić we wszystkie linki. Ale jest nadzieja: często hakerzy popełniają błędy ortograficzne lub wpisują złe nazwy. Dlatego trzeba być czujnym.

Zawirusowanie komputera

Niektóre gry, aplikacje posiadają złośliwe oprogramowania, które po ich pobraniu mogą spowodować utratę danych, utratę pieniędzy z kont bankowych czy uszkodzenie komputera. Posiadać je mogą także maile, wiadomości i różnego rodzaju pliki.

Hejt ze strony innych osób

Jest to jakieś zagrożenie. Kiedy wrzucamy do sieci jakieś wyzywające, nieprzemysłane zdjęcia ktoś może nas zhejtować. Wyzwać nas i ośmieszyć. Musimy też pamiętać, że w Internecie **nie jesteśmy anonimowi!**

Wyłudzenie pieniędzy

Niektórzy hakerzy potrafią włamać się do naszego komputera i zablokować nam dane, a potem kazać płacić okup za ich odzyskanie.

Treści nie odpowiednie dla naszego wieku

Większość ludzi tworzących strony nie oznacza od ilu lat można wejść w jakąś stronę. Choć nieliczny odsetek ludzi to robi. Niestety można powiedzieć, że bezcelowo. Młodzi internauci widząc oznaczenie, że coś jest od 18+ lub jest wymagane potwierdzenie wieku, jeszcze chętniej wchodzi na tę stronę.

Hakerzy

To osoby świetnie znające się na komputerach. Potrafią utworzyć wirusa czy złośliwe oprogramowania. Swoje umiejętności wykorzystują do wyłudzenia pieniędzy, kradzieży danych osobowych i innych niecnych planów. Przysparzają policji coraz więcej problemów.

Naruszenie prywatności

Tyle teraz wszyscy walczą o nienaruszenie swojej prywatności, ale też wrzucają do sieci swoje zdjęcia, nie myśląc o tym, że każdy może je ukraść i wykorzystać by np. nas ośmieszyć. Jeszcze chciałam przypomnieć **w Internecie nie jesteśmy anonimowi!** Jeśli ktoś nas zhejtuje lub naruszy naszą prywatność to będzie możliwość ustalenia, kto to zrobił.

Spam

Czyli wysyłanie niepotrzebnych wiadomości, które zaśmiecają nam telefon, komputer itp. Wiadomości te mogą być nośnikami wirusów, złośliwych oprogramowań, aplikacji śledzących urządzenie, a także aplikacji kradnących dane.

Hasła zapamiętywane przez przeglądarkę

Wielu ludzi dla wygody zapisuje w przeglądarce hasła do wielu aplikacji, kont itp. Takie hasła mogą zostać skradzione przez hakera lub jeśli zgubimy urządzenie, to osoba, która je znajdzie może je wykorzystać i użyć naszych kont. Np. wypłacić w naszym imieniu pieniądze.

Pedofilia

Dorośli ludzie na mediach społecznościowych podają się za młodzież, rówieśników osób, z którymi piszą. Stają się wzorem dla tych dzieci. Często namawiają je do robienia złych rzeczy, spotkań z nimi.

Falszywe „cookies„

Czasem zdarza nam się kliknąć OK w pytaniu o przetwarzanie plików cookie bez czytania. Później może się okazać, że zgodziliśmy się na pobranie czegoś, udostępnienie czegoś czy śledzenie naszego urządzenia, a o tym nie wiemy. Dlatego lepiej czytać takie pytania i dobrze sprawdzić, na co się zgadzamy.

Korzystanie z udostępnionej sieci WI-FI.

Zagrożeniem jest to, że nie wiemy, kto udostępnił Internet. Czasem może się zdarzyć, że stracimy dane.

Kradzież danych osobowych

Hakerzy dostają się na nasze konto i kradną nam nasze dane osobowe: imię, nazwisko, adres, konta np.. bankowe, numer telefonu itd. A potem się nimi posługują np. by podając się za nas, wypłacić nasze pieniądze z banku.

Skrócone adresy

Mają ułatwiać ludziom wchodzenie na strony, ale nie zawsze wiadomo do jakiej strony nas przekierują.

Błędy w adresach WWW

Kiedy ktoś szybko pisze na klawiaturze może pomylić się wpisując adres. I czasem wchodzi na złą stronę, która może nawet zablokować komputer.

Jest oczywiście wiele więcej innych zagrożeń, ale wymieniłam najważniejsze.

Musimy pamiętać, by zawsze uważać w sieci!