FUNDACJA SILVER ECONOMY

PomocToMoc

Publikacja sfinansowana z funduszu prewencyjnego

PZU

Bezpieczni w sieci!

Poradnik dla rodziców

Fundacja Silver Economy

Redakcja: Łukasz Gomółka
Sylwia Kulczyk

Opracowanie pt. „Bezpieczni w sieci” to poradnik, dedykowany nie tylko rodzicom, ale również wszystkim czytelnikom, którzy chcą zadbać o bezpieczeństwo swoje i rodziny bez względu na stopień zaawansowania informatycznego.

Czytelnik niniejszego poradnika będzie mógł poznać zagadnienia dotyczące zasad bezpieczeństwa w sieci ze szczególnym uwzględnieniem bezpieczeństwa najmłodszego pokolenia, a także uświadomić sobie, jak poważne w skutkach może być bagatelizowanie rzeczonego bezpieczeństwa, w tym brak zabezpieczeń w komputerze, tablecie lub smartfonie.

W poradniku zostały omówione również zagadnienia cyberprzemocy, plagiatu i praw autorskich, a także temat uzależnienia od Internetu, rozwiązań technologicznych oraz netykiety.

Celem niniejszego opracowania jest przede wszystkim podniesienie świadomości Czytelnika w zakresie czyhających zagrożeń w sieci oraz sposobów zabezpieczenia przed nimi siebie oraz swoich dzieci.

Redakcja i skład: mgr inż. Łukasz Gomółka
mgr Sylwia Kulczyk

Wydawca: Fundacja Silver Economy
ul. Stanisława Żółkiewskiego 4/1
33 - 300 Nowy Sącz

Oprawa graficzna została wykonana z wykorzystaniem zakupionych zasobów Canva.

Poradnik pt. "Bezpieczni w sieci!" został opracowany w ramach projektu "Dzieci, rodzice, dziadkowie - razem bezpieczni w sieci!, sfinansowanego z funduszu prewencyjnego PZU SA.

FUNDACJA SILVER ECONOMY

PomocToMoc

Publikacja sfinansowana z funduszu prewencyjnego

PZU

Projektowi pt. "Dzieci, rodzice, dziadkowie - razem bezpieczni w sieci!" towarzyszył:

Honorowy Patronat Wójt Gminy Łabowa Marty Słaby

Patronat Honorowy Wójta Gminy Korzenna

Patronat Honorowy Burmistrza Miasta Grybów

Patronat Honorowy Wójta Gminy Kamionka Wielka

SPIS TREŚCI

1. Cyberprzemoc

Cyberprzemoc to rodzaj przemocy względem innych użytkowników, która jest realizowana przez Internet. Użytkownik przykładowo straszy/poniża/obraża ofiarę poprzez, np.:

- agresja słowna, np. wyzywanie na czatach internetowych, zamieszczanie obraźliwych, przykrych komentarzy na forum internetowym, portalach społecznościowych;
- upublicznianie upokarzających, przerobionych zdjęć oraz filmów;
- włamanie na konto i podszywanie się pod kogoś w celu zamieszczania w jego imieniu obraźliwych, upokarzających, często nieprawdziwych postów i zdjęć u siebie lub na profilach innych użytkowników;
- robienie jej zdjęć i filmów bez jej zgody;
- szantażowanie, ujawnianie sekretów;
- wykluczanie z grona „znajomych" w Internecie, czy też celowe ignorowanie czyjejś działalności w sieci.

Materiały umieszczone na ogólnodostępnych witrynach odwiedzanych przez wiele osób zapewniają „widownię" przyłączającą się i oglądającą wyśmiewanie / szydzenie. Nie bez znaczenia jest tu tzw. „pozorna anonimowość" – brak bezpośredniej konfrontacji i poczucie „działania w grupie", co ośmiela jeszcze bardziej do działań związanych cyberprzemocą – także komentujących.

Zatem cyberprzemoc to seria agresywnych zachowań, celowo i regularnie skierowanych przeciwko danej osobie.

Do realizacji agresywnych działań sprawcy wykorzystują także pocztę elektroniczną, czaty, strony internetowe, blogi, grupy dyskusyjne, serwisy, SMS i MMS.

Według badań (Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów, NASK, 2019), nastolatki najczęściej doświadczają agresji w sieci ze względu na:

- poglądy (14,9%)
- wygląd (13,5%)
- upodobania (11,6%)
- narodowość (8,1%)
- ubiór (8,0%)
- orientacja seksualna (4,6%)
- religia (4,5%)
- kolor skóry (4,3%)
- płeć (4,2%)
- zła sytuacja finansowa (3,8%)

1.1 Profilaktyka i sygnały ostrzegawcze

Nie ma idealnych form ochrony przed cyberprzemocą, która może spotkać Twoje dziecko lub Ciebie w dowolnym miejscu w sieci. Dlatego przede wszystkim należy jej przeciwdziałać i natychmiast reagować na sygnały świadczące o tym zjawisku.
Należy przede wszystkim uświadomić dziecku, że istnieje w Internecie problem agresji i uwrażliwić go na innych ludzi - każdy wymaga szacunku w sieci tak samo, jak w kontaktach osobistych.
Zapoznaj także dziecko z zasadami netykiety (osobny rozdział w niniejszej publikacji), jeśli korzysta już z sieci, porozmawiaj z nim o ewentualnych doświadczeniach cyberprzemocy. Może zna takie sytuacje z grupy znajomych, może napotkało je w sieci, a może samo jest sprawcą takiego ataku?

1.1.1 Jakie zachowania dziecka powinny zaniepokoić rodzica?

Objawy świadczące, że dziecko padło ofiarą cyberprzemocy można podzielić na emocjonalne i psychiczne:

- spadek poczucia kompetencji oraz agresja;
- stają się nieufne;
- mają trudności z nawiązywaniem kontaktów i tworzeniem więzi;
- pojawia się skłonność do działań autodestrukcyjnych;
- w skrajnych przypadkach mogą próbować targnąć się na swoje życie;
- nagły spadek samooceny;
- wzrost napięcia emocjonalnego, zmienny nastrój, skrywany płacz i chroniczny smutek;
- izolacja od innych, wycofanie z życia towarzyskiego;
- objawy depresji.

Ważne też jest, aby mieć dobry kontakt z dziećmi, gdyż łatwiej będzie zauważyć ww. objawy i szybko odpowiednio zareagować.

1.1.2 Właściwa reakcja rodzica na zauważoną cyberprzemoc

Należy porozmawiać z dzieckiem i dać mu sygnał, że może polegać na rodzicach. Najczęściej sprawcami są znajomi ze szkoły, toteż można spróbować wyciągnąć informacje związane ze źródłem niepokoju – określić zasady, zabezpieczyć ewentualne dowody tego działania.
Kolejnym krokiem powinna być stanowcza reakcja u opiekunów sprawców polegająca na przedstawieniu całej sytuacji i wyciągnięcia konsekwencji
(w zależności od danego przypadku – od udzielenia upomnienia po nawet kroki prawne).
Zatem, gdy Twoje dziecko doświadczy cyberprzemocy, należy:

- udzielić mu osobistego wsparcia, zapewnić dużo uwagi;
- zabezpieczyć wszystkie dowody cyberprzemocy;
- zwrócić się do administratora serwisu/strony z prośbą o usunięcie nienawistnych treści i zablokowanie osoby atakującej (większość serwisów oferuje taką możliwość);
- jeśli możesz porozmawiać ze sprawcą lub jego rodzicami, żądaj od niego zakończenia przemocy i usunięcia z sieci wszystkich jej śladów;
- poinformuj o tej sytuacji szkołę, wychowawcę i ewentualnie inne, istotne osoby (np. pedagog, nauczyciele);
- jeśli popełniono przestępstwo, poinformuj o nim policję.

1.2 Hejt i trolling

Pozornie „delikatniejszą" formą cyberprzemocy jest hejt. Może polegać na umieszczeniu nienawistnego komentarza, obrazka, filmu czy udostępnieniu takiej treści. Hejtu i negatywnych komentarzy jest w sieci tak wiele, że czasem może się wydawać, że tworzy go większość osób korzystających z sieci. Tymczasem z badań wynika, że to zaledwie 5-10% użytkowników go tworzy.

Trollowanie (ang. trolling) to antyspołeczne zachowanie charakterystyczne dla internetowych forów dyskusyjnych i mediów społecznościowych. Polega na zamieszczaniu kontrowersyjnych, napastliwych, często nieprawdziwych treści w celu zwrócenia na siebie uwagi albo sprowokowania, ośmieszenia lub obrażenia innych użytkowników. Osobę odpowiedzialną za publikowanie takich przekazów określa się jako „troll".

Zjawiska te nie dotyczą tylko i wyłącznie dzieci, według badań (badanie dla serwisu ciekaweliczby.pl na ogólnopolskim panelu badawczym Ariadna):

- 15% dorosłych Polaków w ciągu ostatniego roku osobiście doświadczyło hejtu w Internecie;
- Hejtu doświadczyła prawie aż co czwarta osoba (24%) w wieku 18-24 lata;
- Prawie co siódmy dorosły Polak (15%) twierdzi, że osobiście doświadczył hejtu w Internecie, czyli obrażania, wyzywania, poniżania, wyśmiewania lub zniesławiania. Stosunkowo częściej są to mężczyźni (19%) niż kobiety (11%).

Ważne: 800 100 100 to bezpłatna i anonimowa pomoc telefoniczna i online dla rodziców i nauczycieli, którzy potrzebują wsparcia i informacji w zakresie przeciwdziałania i pomocy psychologicznej dzieciom przeżywającym kłopoty i trudności takie jak:

- agresja i przemoc w szkole,
- cybeprzemoc i zagrożenia związane z nowymi technologiami,
- wykorzystanie seksualne,
- kontakt z substancjami psychoaktywnymi,
- depresja i obniżony nastrój,
- myśli samobójcze,
- zaburzenia odżywiania.

2. Analiza i przeciwdziałanie ryzykownym zachowaniom on-line

W sieci, tak jak w życiu realnym można także napotkać wiele zagrożeń. Jeżeli użytkownik nie potrafi odpowiednio zachować środków ostrożności, to może ponieść spore k**onsekwencje.**

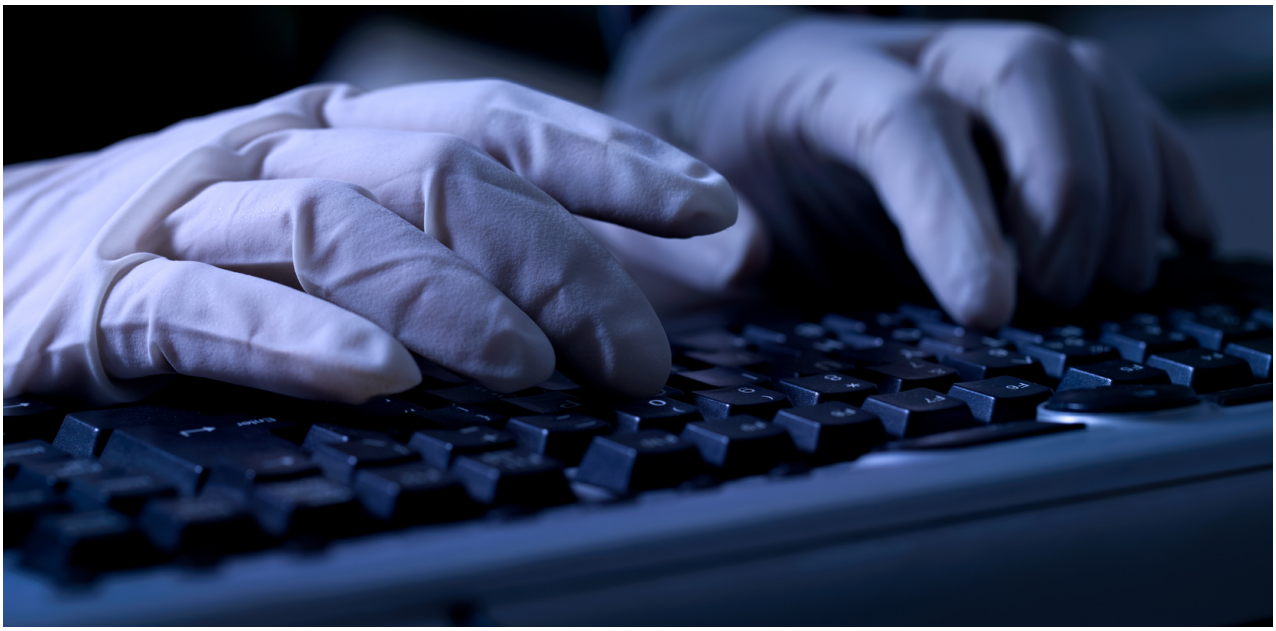
2.1 Uwodzenie w sieci

W tej grupie zagrożeń wskazać trzeba zwłaszcza zagrożenia płynące z nawiązywania znajomości poprzez Internet. Brak bezpośredniego kontaktu pomiędzy użytkownikami i związana z tym anonimowość (w stosunku do drugiej osoby) powoduje, że nawiązując za pomocą Internetu kontakt z nieznanym nam użytkownikiem, wiemy o nim tylko tyle, ile on sam nam o sobie ujawni.

Jednocześnie należy nadmienić, iż trudno oczekiwać od razu całej prawdy od swojego rozmówcy. Taki kontakt poprzez Internet stwarza możliwość ukrycia rzeczywistej tożsamości użytkownika. Może on podszywać się pod kogoś zupełnie innego. Co więcej – może on mieć zamiary, których nie jesteśmy w stanie przewidzieć. W oczywisty sposób opisywana sytuacja stwarza największe zagrożenie dla dzieci i młodzieży.

Sytuację taką wykorzystują często osoby o skłonnościach pedofilskich. Osoby takie próbują nawiązać kontakt z młodym, niedoświadczonym użytkownikiem, zdobyć stopniowo jego zaufanie, by następnie, stosując rozmaite socjotechniczne metody, skłonić go do oczekiwanych przez siebie zachowań. W najlepszym razie może chodzić o skłonienie dziecka do przesłania fotografii. Może też chodzić o nakłonienie go do bezpośredniego spotkania w świecie rzeczywistym, celem wykorzystania seksualnego.

Celem ataków bywają także inne grupy społeczne, w tym osoby starsze. Realnie dzieci/ młodzież oraz seniorzy są częstym celem tego typu „ataków", ponieważ łączy te grupy stosunkowo duża ufność, poszukiwanie towarzystwa oraz ograniczona świadomość bezpieczeństwa. Głównym celem dla oszustów w przypadku osób starszych są malwersacje na tle finansowym.



2.2 Wyłudzenia danych osobowych i środków pieniężnych

Drugą grupą zagrożeń wymagającą szczególnej uwagi jest przekazywanie danych na skutek ich wyłudzenia od użytkownika. Można tu znów wykorzystać łatwowierność i brak doświadczenia dzieci i młodzieży, choć częściej próby wyłudzenia danych są skierowane przeciwko dorosłym, w szczególności osobom starszym. Oni są bowiem, zazwyczaj w posiadaniu informacji będących w polu zainteresowania wyłudzającego (oszustwa na tle finansowym – dzieci zatem tu nie są głównym celem). Wyłudzenie informacji może przybrać postać prób uzyskania pożądanych informacji w bezpośrednim internetowym kontakcie bądź też metodami pośrednimi, z wykorzystaniem technik komputerowych z zastosowaniem fałszywych stron internetowych, na których nieświadomy użytkownik pozostawia swoje dane, które będą potem wykorzystane przez przestępcę.

Pod pojęciem wyłudzenia danych osobowych rozumie się sytuację, w której użytkownik Internetu sam, z własnej woli udostępnia innym jego użytkownikom rozmaite dane za pomocą Internetu (online). Często zdarza się to na skutek wprowadzenia w błąd ofiary, ale nie zmienia to faktu samodzielnego udostępnienia.

Zagrożeniem jest nie samo udostępnienie, a to, że wprowadzenie danych do Internetu, grozi utratą kontroli nad nimi i stwarza możliwość wykorzystania tych danych przez innych użytkowników w niepożądany sposób (np. wzięcie kredytu, podszywanie się pod tożsamość ofiary, itd.)

Bardzo ciekawe jest też to, że osoba dopuszczająca się nieuprawnionego wykorzystania pozyskanych danych nie musi wcale posiadać specjalistycznych umiejętności, które charakteryzują cyberprzestępców. Przy czym trzeba też zauważyć, że zagrożenie takie może pochodzić zarówno ze strony tych osób, którym dane zostały bezpośrednio udostępnione, jak i ze strony osób trzecich. Ta druga możliwość pojawia się zwłaszcza wtedy, kiedy dane są udostępniane bliżej nieokreślonemu gronu odbiorców (upubliczniane).

Dane, które użytkownik zamieścił w Internecie mogą, po odpowiednim wyselekcjonowaniu, a ewentualnie także odpowiednim ich przetworzeniu, posłużyć do jego szantażowania bądź ośmieszania. Mogą to być formy tzw. przemocy w Internecie, której skutki potrafią być dla użytkownika bardzo dotkliwe.

3. Ochrona dzieci i młodzieży przed szkodliwymi treściami w Internecie

Coraz więcej obszarów życia społecznego i prywatnego jest upublicznianych, a ludzie mogą dzięki temu uczestniczyć w zdarzeniach, które wcześniej były dla nich niedostępne. Oczywiście Internet rodzi nieograniczone możliwości dostępu do różnego typu wydarzeń.
Tym samym pojęcie ochrony małoletnich w kontekście mediów dotyczy właśnie zapewnienia, że szkodliwe treści w mediach, w tym w Internecie nie zaszkodzą fizycznemu i psychicznemu rozwojowi dzieci.

Typy zagrożeń:

- związane z agresją, w tym z przemocą, okrucieństwem i drastycznymi scenami dostępnymi w grach, relacjach, filmach, itd.,
- związane z seksem – pornografią i napastowaniem seksualnym;
- związane z rasizmem i nienawiścią, czyli tzw. hejtem;
- związane z marketingiem i perswazją, ale także nadużyciem prywatności, wykorzystaniem danych osobowych (wyłudzanie tożsamości);
- naruszeniem praw autorskich;
- hazardem online.

Według raportu z badania UE „Kids Online 2018" dzieci i młodzież spotykają się w Internecie z informacjami dotyczącymi brania narkotyków, krwawymi lub brutalnymi obrazami, hejtem, propagowaniem anoreksji lub bulimii, a także ze sposobami na popełnienie samobójstwa czy zrobienie sobie krzywdy fizycznej.

3.1 Blokowanie na komputerze dostępu do szkodliwych treści

Istnieją na rynku programy służące do blokowania treści w Internecie. Kilka najciekawszych omówiono poniżej.

Program Cenzor

Producent oferuje 3 wersje programu:

- dla indywidualnych odbiorców;
- dla placówek oświatowych;
- biznesowa dla firm.

Program blokuje dostęp do stron szkodliwych takich jak: pornografia, przemoc oraz narkomania. Posiada prosty, funkcjonalny i czytelny interfejs, przez co użytkownik w intuicyjny sposób może dowolnie go konfigurować wg własnych preferencji. Baza blokowanych stron jest automatycznie aktualizowana. Dzięki zakładce Blokady użytkownika można utworzyć własną listę stron zakazanych oraz poprzez zakładkę Wyjątki blokady można zdefiniować strony, jakie – mimo że normalnie program by je zablokował – mają się wyświetlać.

Program Emilek

Zdaniem producenta Emilek to łatwy w obsłudze program, dzięki któremu rodzice mogą przede wszystkim blokować dostęp do stron o tematyce erotycznej i pornograficznej. Ponadto opiekunowie mogą definiować własne słowa kluczowe. Aplikacja jest przeznaczona dla użytkowników systemu Windows. Posiada intuicyjny interfejs np. duże ikonki odpowiadają symbolizowanym przez nie funkcjom. Panel administracyjny składa się z 9 zakładek: Ustawienia, Dodatkowe, Statystyki, Czarna Lista, Biała Lista, Czas, Własne Definicje, System, Rejestracja.

P**rogram Motyl**

W panelu konfiguracyjnym użytkownik może zdefiniować opcje filtrowania w zależności od własnych preferencji. Program umożliwia blokowanie stron pornograficznych, czatów, bramek sms, komunikatorów oraz popularnych przeglądarek Opera, Firefox, Internet Explorer. Za pomocą specjalnego suwaka można zmieniać czułość programu. Producent nie opisuje jednak, co dają kolejne ustawienia suwaka i jakie są różnice w ustawieniach tej opcji. Motyl blokuje niestosowną stronę zamykając przeglądarkę i nie wyświetlając żadnego graficznego komunikatu.

W przypadku gdy przeglądarka jest skonfigurowana tak, aby rozpoczynać z tymi samymi stronami co w chwili ostatniego jej zamknięcia, mogą wystąpić problemy z jej otworzeniem. Dopiero w zakładce Raporty można odkryć, iż dana strona nie została wyświetlona ze względu na jej nieodpowiedni charakter. Istnieje także możliwość definiowana słów czy stron dozwolonych. Służą temu zakładki: Lista stron dozwolonych oraz Lista stron zakazanych czy też Słowa kluczowe.

Program Opiekun Dziecka w Internecie

Producent oferuje trzy wersje programu:
- dla użytkownika domowego;
- wersję jednostanowiskową przeznaczoną dla szkół;
- wersję sieciową.

Opiekun Dziecka charakteryzuje się ciekawym, kolorowym i przejrzystym interfejsem. Aplikacja zawiera opcje ograniczenia czasowego. W związku z tym rodzic ma możliwość wpływu na czas surfowania dziecka w Sieci. Program blokuje strony według kategorii: pornografia, sekty i satanizm, przemoc, narkotyki.

4. Ochrona komputera przed potencjalnie niechcianymi aplikacjami

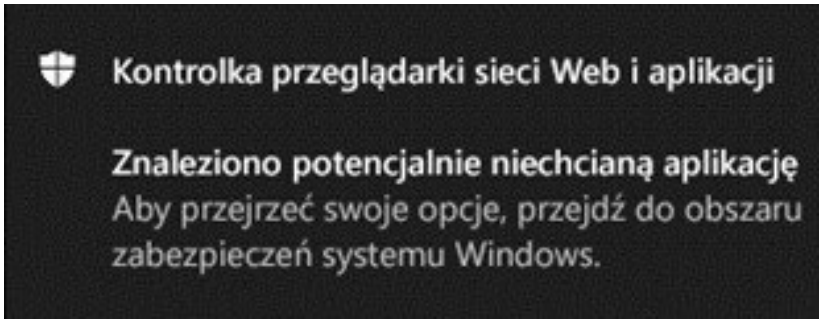
W ramach różnorodności oprogramowania z jednej strony istnieją aplikacje działające bez zakłóceń, a z drugiej złośliwe oprogramowanie, natomiast pomiędzy nimi istnieją aplikacje, którym nie do końca ufamy, oraz takie, które wyróżniają się działaniem budzącym niepokój. Nazywamy to „Potencjalnie niechciane aplikacje" lub „PUA".
Potencjalnie niechciane aplikacje (PUA) nie są złośliwym oprogramowaniem, ale mogą wyświetlać niechciane reklamy, potajemnie używać komputera do wydobywania kryptowalut, oferować inne nieoczekiwane aplikacje lub wykonywać inne niepożądane czynności.

W przypadku potencjalnie niechcianych aplikacji system Windows 10 informuje o obawach i pozwala zdecydować, czy chcemy kontynuować ich instalację.
Potencjalnie niechciane aplikacje to kategoria oprogramowania, która może powodować:
- spowolnienie działania komputera
- wyświetlać niespodziewane reklamy
- instalować inne oprogramowanie, które może być bardziej szkodliwe lub drażniące.

Oprogramowanie tego typu z reguły pozwala wyłączyć blokowanie potencjalnie niechcianych aplikacji i wybrać, czy chcesz zablokować zainstalowane aplikacje, czy pobrane aplikacje.

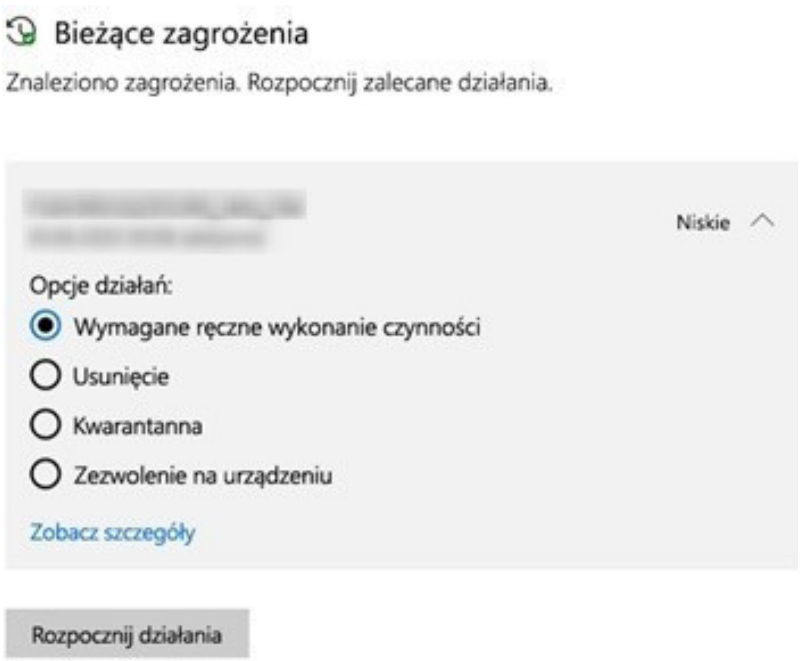
- Blokowanie aplikacji wykrywa potencjalnie niechcianą aplikację (PUA), która została już pobrana lub zainstalowana.
- Blokowanie pobierania wyszukuje potencjalnie niechcianą aplikację, gdy jest ona pobierania.

Przykładem może tu być aplikacja Zabezpieczenia Windows – gdy wykryje potencjalnie niechcianą aplikację, otrzymujemy powiadomienie z prośbą o podjęcie działania.



Rysunek 1 - Kontrolka Windows

Klikając powiadomienie, przechodzimy do obszaru Ochrona przed wirusami i zagrożeniami aplikacji Zabezpieczenia Windows. Wtedy można kliknąć nazwę potencjalnie niechcianej aplikacji i wybrać działanie.



Rysunek 2 - Bieżące zagrożenia - aplikacja Windows

Dopóki nie wybierze się działania, które ma być wykonane, wykryta potencjalnie niechciana aplikacja zostanie zablokowana tylko na komputerze użytkownika — nie zostanie usunięta. W trakcie wykonywania kolejnych skanów, ta potencjalnie niechciana aplikacja może być nadal wykrywana, dopóki nie podejmiemy stosownego działania. Po dokonaniu wyboru, wybieramy pozycję Rozpocznij działania.

Jeżeli chcemy zmniejszyć szanse uzyskania niechcianego oprogramowania, to powinniśmy:

- Pobierać aplikacje tylko z zaufanych źródeł.
- Używać regularnie aktualizowanego produktu antywirusowego, takiego jak program antywirusowy Microsoft Defender wbudowany w system Windows 10.
- Posiadać najnowszą wersję przeglądarki.
- Zadbać o aktualność swojego urządzenia dzięki najnowszym aktualizacjom dla systemu Windows, przeglądarki oraz Twoich aplikacji.

Jeśli podejrzewamy, że masz już na komputerze niechciane oprogramowanie:

- Przeglądnij i odinstaluj niepotrzebne oprogramowanie
- Uruchom pełne skanowanie za pomocą dowolnego programu antywirusowego

4.1 Programy filtrujące treści

Dziecko w sieci, to temat, którego popularność jest projekcją tego, jak bardzo ważne jest właściwe podejście do korzystania przez dzieci z Internetu. Nie od dziś wiadomo, że rozmowa z dzieckiem jest najważniejsza. Zanim Internet powstał i stał się zagrożeniem, dzieci były narażone na szereg innych sytuacji i od pokoleń wiadomo, że przede wszystkim trzeba je uświadamiać i uczyć, jak nie należy się zachowywać. Młodość i dzieciństwo rządzą się swoimi prawami, a to oznacza, iż mały użytkownik komputera, może nie dojrzeć zagrożenia, zbagatelizować je lub po prostu nie zrozumieć. Dlatego ważne jest zachowanie czujności ze strony rodzica i podejmowanie działań kontrolnych. Mowa oczywiście o programach do kontroli rodzicielskiej, które zaprezentowano poniżej.

Beniamin

Bardzo ciekawy program, z którego korzystają zarówno użytkownicy domowi, jak i szkoły i inne placówki, w których dzieci mają dostęp do Internetu. Program jest płatny. Interfejs jest relatywnie prosty w obsłudze. Nawet rodzic kompletnie niemający informatycznego zacięcia powinien móc bez problemu go skonfigurować oraz raz na jakiś czas aktualizować, czy zmienić ustawienia. Panel zabezpieczony hasłem sprawi, że nawet najbystrzejszy maluch nie poradzi sobie ze zmianą ustawień.

Program ten świetnie radzi sobie z blokowaniem dostępu do niepożądanych treści, nadmiernego lub samowolnego używania komunikatorów, korzystania z portali społecznościowych, poczty e-mail itd. Ponadto można monitorować czas, jaki dziecko spędza w Internecie lub na wirtualnych rozrywkach oraz otrzymywać raport z jego aktywności.

Visual Porn Blocker Free

Jest to darmowy program blokujący strony z niepożądanymi, erotycznymi treściami. Pozwala on na zablokowanie takowych w całym systemie, można go więc używać jako program do filtrowania stron nawet, jeżeli z komputera nie korzysta dziecko.
Ustawienia programu zabezpieczone są hasłem, bez którego dziecko nie będzie w stanie zdjąć blokady. Program w tej chwili nie posiada polskiej wersji językowej, ale jego obsługa jest relatywnie prosta, więc nie należy się zniechęcać do jego zainstalowania.

Mini Monitoring

Program występujący w dwóch wersjach. Jednej w pełni widocznej dla użytkownika i w drugiej, która jest ukryta w systemie i ciężko ją odinstalować. Jest to program inwigilujący pracę na komputerze, robiący zrzuty ekranu i raportujący każdą możliwą akcję, od przeglądania stron przez uruchamianie aplikacji, a nawet monitoruje wciśnięte na klawiaturze znaki.

Sam program jest relatywnie prosty do konfiguracji, posiada polski interfejs, a jego obsługa, jak i odbieranie raportów aktywności użytkowania nie powinny być problematyczne nawet dla średnio zaawansowanych obserwatorów.

Opiekun Dziecka w Internecie

Polski program do kontroli rodzicielskiej, posiadający szereg funkcji zarówno chroniących dziecko przed niepożądanymi treściami, jak i pozwalający na monitorowanie jego aktywności przy komputerze.
Program posiada bazę ponad 500 tysięcy stron www z nieodpowiednimi dla dziecka treściami. Ponadto rozróżnia niepożądane hasła w 7 językach na bieżąco skanując pod ich kątem otwartą stronę. Może również zapisywać zrzuty ekranu i przechowuje pełną historię włączanych witryn. Ponadto, tak jak wiele programów do kontroli rodzicielskiej ma także opcję ograniczania czasu przy komputerze. Całość w intuicyjnym i prostym w obsłudze interfejsie, który bez problemu powinien zrozumieć każdy rodzic.

Visikid

Aplikacja monitorująca czas i działania dziecka przy komputerze, jednakże w przeciwieństwie do innych nie blokuje stron o niepożądanej treści. Program monitoruje aktywności i przesyła raporty e-mail do rodzica. Jest to rozwiązanie raczej dla starszych dzieci, uczące je odpowiedzialności za to, co robią i czego szukają w Internecie.

Panel do obsługi programu jest prosty i czytelny, posiada opcję ustawień w języku polskim. Program pozwala na monitorowanie aktywności nawet trójki dzieci jednocześnie.

Kurupira Web Filter

Kolejny darmowy program do kontroli rodzicielskiej. Podobnie jak inne tego typu oprogramowania jego głównym zadaniem jest blokowanie stron, które zawierają nieodpowiednią dla dzieci treść. Posiada on swoją własna bazę jak i pozwala na dodanie stron, których my nie życzymy sobie, aby nasz maluch uruchamiał.

Standardowo już program daje możliwość ustawień ograniczania czasu dziecka przy komputerze oraz umożliwia opcje przechwytywania zrzutów ekranu w czasie aktywności malucha.

Motyl

Znany program do kontroli rodzicielskiej, kolejny rok utrzymuje się na rynku. Program blokuje standardowo strony o charakterze erotycznym, ale także pozwala na ograniczenie dostępu do bramek sms czy komunikatorów. Standardowo posiada opcję ustawień czasu jaki dziecko może spędzić przed ekranem. Ciekawostką jest zablokowanie wpisywania pewnych słów już z poziomu klawiatury. Program jest dość intuicyjny i przyjazny dla użytkownika.

5. Klasyfikacja PEGI

PEGI pomaga rodzicom w podejmowaniu świadomych decyzji podczas zakupu gier wideo.

PEGI oferuje klasyfikacje wiekowe gier wideo w 38 krajach europejskich. Rating wiekowy stanowi potwierdzenie, że gra jest odpowiednia dla gracza w danym wieku. PEGI ocenia, czy gra jest odpowiednia dla danego wieku, nie ocenia natomiast poziomu trudności.

Ratingi wiekowe to systemy używane nie tylko do oznaczania treści rozrywkowych, na przykład gier, lecz również filmów, telewizyjnych programów rozrywkowych lub aplikacji mobilnych znakiem stanowiącym rekomendację wiekową na podstawie treści. Ratingi wiekowe stanowią dla konsumentów, a zwłaszcza rodziców, wskazówki, które pomagają w dokonaniu wyboru podczas zakupu konkretnego produktu dla dziecka.

Ograniczenie	Informacje
 Od lat 3	Treść gier oznaczonych w ten sposób uznawana jest za odpowiednią dla wszystkich grup wiekowych. Dopuszczalna jest pewna ilość przemocy w komicznym kontekście (typu bajka „Tom i Jerry"). Postaci powinny być wytworem fantazji. Gra nie powinna zawierać dźwięków ani obrazów, mogących przestraszyć dziecko. Nie powinny w niej występować wulgaryzmy, sceny zawierające nagość ani nawiązujące do życia seksualnego.
 Od lat 7	Gry są podobne do gier z grupy od 3 lat, ale zawierają dźwięki lub sceny, które potencjalnie mogłyby przerazić najmłodszych. W grach tych dopuszczalne są sceny obejmujące częściową nagość, ale nigdy odnoszącą się do życia seksualnego.
 Od lat 12	Gry komputerowe dla tej kategorii wiekowej ukazują przemoc skierowaną przeciwko postaciom fantastycznym lub o ludzkim wyglądzie. Mogą pojawić się nawiązania do życia seksualnego, ale muszą mieć one łagodny charakter. Podobnie jak pojawiające się w grze wulgaryzmy. Do tego rodzaju gier mogą należeć gry hazardowe, które w rzeczywistości rozgrywają się w kasynach czy punktach gier.
 Od lat 16	Ten symbol jest nadawany, jeżeli przemoc czy czynność seksualna wyglądają tak jak w rzeczywistości. Gry dla tej grupy wiekowej mogą zawierać ostrzejsze wulgaryzmy, a także mogą pojawić się treści o paleniu tytoniu, piciu alkoholu czy zażywaniu narkotyków. Ponadto mogą zawierać treści o grach losowych.
 Od lat 18	Ten symbol oznacza gry dla osób dorosłych. Mogą one zawierać daleko posuniętą przemoc, w tym realistyczne zabijanie. W tej kategorii znajdują się również gry, w których bohaterowie zażywają narkotyki i spożywają inne niebezpieczne używki. W grach pojawiają się realistyczne sceny i zachowania związane z życiem seksualnym.

Obrazek	Treść	Informacje	Dopuszczalne oznaczenia
	Przemoc	Gra zawiera elementy przemocy	7 12 16 18
	Seks	W grze pojawiają się nagość lub zachowania seksualne lub nawiązania do zachowań o charakterze seksualnym	16 18
	Dyskryminacja	Gra pokazuje przypadki dyskryminacji lub zawiera materiały, które mogą do niej zachęcać osoby nieletnie	18
	Narkotyki	W grze pojawiają się nawiązania do używek lub przedstawiono ich zażywanie	16 18
	Strach	Gra może przestraszyć młodsze dzieci	7 12 16 18
	Wulgarny język	W grze jest używany wulgarny język	12 16 18
	Hazard	Gry, które zachęcają do uprawiania hazardu lub go uczą	12 16 18
	Gra online	Gry, w które można grać przez Internet	3 7 12 16 18

5.1 Jak kontrolować w jakie gry gra dziecko?

Nielimitowany dostęp do informacji, możliwość kontaktu z ludźmi z całego świata, cudowne gry i aplikacje – to wspaniałe cechy nowoczesnego telefonu/sprzętu, ale też niebezpiecznie uzależniające dla dziecka.

Pamiętać należy, że nic nie zastąpi edukacji, rozmowy i osobistego nadzoru nad dzieckiem, któremu wręczamy smartfon lub tablet. Są jednak aplikacje, które pomogą nam ustrzec dzieci przed niebezpieczeństwami Internetu.

Programy takie, jak Kids Place, pozwalają ograniczać funkcjonalność telefonu wedle naszego życzenia, jak również podglądać to czym zajmuje się nasze dziecko, bez przesadnej ingerencji w jego prywatność. Inne pozwolą zlokalizować pociechę lub poinformują, kiedy będzie potrzebowała pomocy.

To w jaki sposób będziemy prowadzić nadzór zależeć będzie od nas samych i możliwości aplikacji. Możemy blokować dostęp do wybranych stron internetowych. Możemy zablokować możliwość instalowania gier i aplikacji. Możemy kontrolować ile dziecko spędza czasu przy telefonie. Możemy też sprawdzać czy nie wpadło w tarapaty przeglądając raporty z wybranego przez nas programu.

6. Selekcja informacji prezentowanych w Internecie

6.1 Wyszukiwanie i weryfikowanie treści

Fake news to z angielskiego po prostu fałszywa informacja. To treści, które są nieprawdziwe lub nie do końca prawdziwe, ale mimo to są publikowane w serwisach informacyjnych czy na portalach społecznościowych. Często fake newsy mają być traktowane bardzo poważnie i przekonać użytkowników, że opisują prawdę. Czasem są tworzone w charakterze satyrycznym, ale interpretowane przez ludzi jako prawda i rozprzestrzeniane już nie jako żart, a prawda. Nie zawsze mają one formę tekstową – wykorzystywane są grafiki, zdjęcia, a nawet filmy, w których poprzez obróbkę zmanipulowana jest treść.

Pojęcie to zostało słowem roku 2017 w Stanach Zjednoczonych i w Belgii. Dziś spotykamy się z nim coraz częściej – fake newsy stają się codziennością.

MISTYFIKACJA - kłamstwo, fikcja, łgarstwo, nieprawda, półprawda, oszustwo, przemilczenie, zatajenie, fałszerstwo, zafałszowanie, zmyślenie, koloryzowanie, konfabulacja, fantazjowanie, blaga, bujda, bajer (słownik synonimów).

W ogólnoeuropejskim badaniu Eurobarometr, przeprowadzanym regularnie przez Kantar TNS na zlecenie Komisji Europejskiej, w 2018 roku poruszone zostały tematy związane z obecnością w mediach nieprawdziwych informacji. Z raportu z badania „Czy żyjemy w rzeczywistości fake newsów?" wynika, że w Polsce z fake newsami spotyka się prawie codziennie aż 75% z nas. 79% traktuje je jako zagrożenie dla demokracji – choć jednocześnie niemal tyle samo (71%) uważa, że umie odróżnić prawdziwą wiadomość od fałszywej.

Warto jest zastanowić się nad treściami, które czytamy i traktujemy jako prawdę. Naukowcy mówią, że żyjemy w społeczeństwie post prawdy – a zatem sytuacji, w których fakty nie są już aż tak istotne. Dużo ważniejsze są emocje, osobiste przekonania i wiążąca się z nimi siła przebicia.

Istnieją grupy osób, dla których celem staje się przedstawianie kłamstwa – fake newsa, post prawdy – w takiej formie, żeby jak najwięcej osób do takich „informacji" dotarło, uwierzyło w nie i je rozpowszechniało, po to, aby osiągać własne cele – niezależnie od tego, czy są one polityczne, ekonomiczne, społeczne, czy jakiekolwiek inne. Ponieważ gra toczy się o wpływanie na poglądy innych, sposoby na docieranie z fake newsami również muszą być coraz bardziej wysublimowane, aby ludzie wciąż się na nie nabierali.

Gdzie możemy spotkać fake newsy?

Przede wszystkim w portalach społecznościowych, od Facebooka, Instagrama, po fora internetowe i mailing. Zatem w dużej mierze tam, gdzie przeciętny człowiek może tworzyć treści i je udostępniać. Poza „zwykłymi" osobami nie można też zapomnieć o kontach trolli internetowych czy botów (automatycznych kont użytkowników w mediach społecznościowych, które mogą masowo publikować treści), których wciąż są niezliczone ilości w mediach społecznościowych.

6.2 Konsekwencje i zagrożenia płynące z fake newsów

Pisaliśmy wcześniej o znaczeniu informacji w społeczeństwach informacyjnych, o postprawdzie, która wpływa na otaczającą nas rzeczywistość.

Fake newsy w „łagodnym" wariancie pokazują nieprawdziwą historię dotyczącą jakiegoś miejsca, jakiejś osoby, co po prostu chwyta za emocje i chętnie ją udostępniana.

W wariancie „średnim" fake newsy mogą oczerniać konkretne osoby – np. poprzez edycję ich zdjęć, aby pokazać coś innego.

Zaś w skrajnych przypadkach fake newsy bywają również źródłem działań agresywnych lub autoagresywnych – poprzez wykorzystanie skrajnych emocji powodują działania, które mogą zakończyć się kalectwem a nawet śmiercią.

Jak rozpoznać fake newsy?

Z pomocą przychodzi nam Międzynarodowa Federacja Stowarzyszeń i Instytucji Bibliotekarskich. Przygotowała ona specjalny instruktaż, jak w ośmiu krokach zweryfikować informację. Otóż należy:

- rozważyć źródło (rozumieć jego cele i intencje) - jaka redakcja odpowiada za to źródło, kto jest jej właścicielem itp.
- czytać całość artykułu, nie tylko nagłówek (aby zrozumieć cały materiał)
- sprawdzić autorów, by zweryfikować, czy są oni wiarygodni. Nie zawsze jest to możliwe, ponieważ nie wszystkie artykuły są podpisane z nazwiska oraz nie wszyscy autorzy – nawet w wiarygodnych treściach – są podpisani. Jeśli jest taka możliwość dobrze jest wyszukać nazwisko autorki czy autora i zobaczyć inne treści, które ta osoba tworzy.
- sprawdzić informację w innych źródłach (upewnić się, że podają te same informacje).
- znaleźć datę publikacji (aby zobaczyć, czy informacje są aktualne).
- upewnić się, czy nie jest to żart lub satyra.
- przemyśleć własne uprzedzenia (by zobaczyć, czy nie wpływają one na nasz osąd).
- zapytać ekspertów (uzyskać potwierdzenie od niezależnych ludzi dysponujących wiedzą na dany temat).

Warto też przyjrzeć się samemu sposobowi publikacji wiadomości:

- Czy znajduje się na znanej nam stronie internetowej?
- Czy adres tej strony nie budzi naszych wątpliwości?
- Czy język newsa jest poprawny, czy zachowana jest ortografia i interpunkcja?
- Jeśli nie, może to być słabej jakości tłumaczenie fake newsa, który ma za zadanie dotrzeć do jak największej liczby odbiorców.
- Jakie emocje wzbudza w nas dana treść?
- Czy jest przygotowana tak, by wywołać w nas gniew, złość, pogardę? Jeżeli tak, to jest w najwyższym stopniu podejrzana i lepiej jej nie ufać.

J**ak uwrażliwić dziecko na zjawisko fake newsów?**

Dzieci na co dzień zdobywają wiele informacji i są ciekawe świata. Nie wszystkie źródła, z których czerpią wiedzę, są wiarygodne i rzetelne. Warto, aby wiedziały, że nie wszystko co podają media elektroniczne, musi być prawdą. Krytycznego myślenia, refleksji i ograniczonego zaufania do treści publikowanych w Internecie warto uczyć dziecko od najmłodszych lat.

6.3 Wybrane przykłady fake newsów i innych mistyfikacji

Koniec świata planowany na 1 kwietnia

Prognozy końca świata to częsty wątek, jaki już wielokrotnie okazywał się nieprawdziwy. Jednym z ciekawszych jest wydarzenie z dnia 31 marca 1940 roku, kiedy to Instytut Franklina oświadczył dla prasy, iż dnia następnego nastąpi koniec świata. Nie zwlekając rzeczone oświadczenie przechwyciła stacja radiowa KYW, nadając wiadomość o treści:

"Nasze najgorsze obawy o rychłym nadejściu końca świata zostały potwierdzone przez astronomów z Instytutu Franklina w Filadelfii. Naukowcy oceniają, że nastąpi to jutro o 15.00 czasu wschodniego. To nie jest primaaprilisowy żart. Potwierdzenie można uzyskać u Wagnera Schlesingera, dyrektora Fels Planetarium w Filadelfii."

Ta złowroga wiadomość sprawiła, iż rozdzwoniły się telefony w urzędach i zapanowała panika, która została opanowana dopiero po wydaniu kolejnego oświadczenia przez Instytut Franklina, iż nie wydawał i nie potwierdza takich prognoz. Okazało się również, iż to rzecznik prasowy Instytutu William Castellini, chciał za pomocą tego drobnego oszustwa nagłośnić wykład pt. "Jak skończy się świat", który był zaplanowany właśnie na 1 kwietnia w Instytucie. Konsekwencje jednak zostały wyciągnięte wobec żartownisia i władze Instytutu podjęły decyzję o zwolnieniu Castelliniego z pracy.

Rój os na Nowej Zelandii

W 1949 roku Phil Shone, didżej w stacji radiowej 1ZB, przekazał z samego rana słuchaczom, że w kierunku Auckland zmierza szeroki na 1,5 kilometra rój os. Radził im jednocześnie, aby dobrze zabezpieczyli siebie i swoje domy przez skrzydlatym niebezpieczeństwem, m.in. aby idąc do pracy, wpuszczali spodnie w skarpetki, a na zewnątrz domów rozwieszali nasmarowane miodem pułapki. Tysiące ludzi uwierzyło w podaną im informację i wyszli na ulicę w spodniach obciśniętych skarpetkami. Dopiero koło południa Shone przyznał, że jego komunikat o osach był żartem. Dyrekcja rozgłośni wyciągnęła konsekwencje z zaistniałej sytuacji. Raz, że orzeczono, iż takie mistyfikacje niszczą wiarygodność ich Instytucji, a dwa od tego czasu przed każdym 1 kwietnia wysyłano do radia notatkę nakazującą podawać tylko prawdziwe informacje.

Fotomontaże

W 1839 roku gazety donosiły o odkryciu przez Louisa Daguerre`a sposobu obróbki zdjęć fotograficznych. Dla wielu czytelników informacja ta wydawała się nieprawdopodobna i uznali ją jako mistyfikację. W XIX wieku fotografia symbolizowała naukowy obraz natury, niespaczony ludzkim działaniem. Powszechnie przyjęło się, że "obiektyw nie kłamie", że to co jest na zdjęciu to najczystsza prawda. Tymczasem odkrycie tej nowej techniki fotograficznej było faktem. Jednakże utożsamianie fotografii z prawdą i obiektywizmem paradoksalnie uczyniło z niej idealne narzędzie mistyfikacji i dzieje się to aż do dnia dzisiejszego.

Złoto i wojna secesyjna

To był maj 1864 roku kiedy to generałowi Lee w Wirginii deptał po piętach Grant, a żołnierze Północy mieli nadzieję, iż wojna wkrótce się zakończy. I wówczas 18 maja nowojorczycy przeczytali w dwóch porannych gazetach, że prezydent Lincoln ogłosił proklamację, nakazując powołanie pod broń dodatkowych 400 000 mężczyzn Unii, mając na względzie *"sytuację w Wirginii, klęskę nad Czerwoną Rzeką, opóźnienie w Charlestonie i ogólny stan państwa"*. Informacja ta niosła ze sobą dość jasne przesłanie, iż wojna może trwać jeszcze przez długie lata. W takim stanie informacji ceny akcji na nowojorskiej giełdzie natychmiast gwałtownie spadły, zaś złoto, prawie od zawsze uważane za dość bezpieczną lokatę odporną na inflację, skoczyło w górę. Kilka godzin później prawda wyszła na jaw, kiedy to przyszła depesza z Departamentu Stanu w Waszyngtonie, stwierdzająca, że "proklamacja jest od początku do końca fałszerstwem". Detektywi szybko odkryli, kto stoi za całym zamieszaniem. Okazało się, że winowajcą był wydawca pewnej gazety Joseph Howard Jr., który miał dostęp do informacji o stanie gospodarki i zainwestował dużą gotówkę w złoto, a potem przez wynajętych posłańców rozesłał sfałszowaną depeszę do gazet. Kiedy otwarto giełdę czekał po prostu na jej reakcję na niepokojącą wiadomość i sprzedał swoje akcje zarabiając na tym spory zysk. Kiedy został aresztowany w Brooklynie, od razu przyznał się do wszystkiego. Jednak w areszcie odsiedział raptem zaledwie niespełna trzy miesiące, po czym został zwolniony na polecenie Lincolna. Najprawdopodobniej prezydenta poruszyła prośba przyjaciela zamożnego ojca Howarda, który dowodził, iż młody mężczyzna "chciał tylko trochę zarobić pieniędzy".

Mistyfikacje w telewizji

W latach 50. XX wieku jednym z najpopularniejszych teleturniejów telewizyjnych w Stanach Zjednoczonych był program *"Dwadzieścia jeden"*, a oglądalność wzrosła jeszcze bardziej, kiedy to w 1956 roku wziął w nim udział Charles van Doren, syn laureata nagrody Pulitzera, poety Marka van Dorena. Młody uczestnik teleturnieju wydawał się niepokonany. Odpowiadał prawidłowo na wszystkie pytania, zdobywając w sumie 129 000 dolarów (ponad 500 000 złotych). Niestety rok później jego poprzednik Herbert Stempel ujawnił, iż wyniki teleturnieju są z góry ustalone. Okazało się, że van Dorenowi dostarczano odpowiedzi na pytania, w konsekwencji czego Kongres powołał specjalną komisję dochodzeniową, a NBC - producent widowiska, musiał się przyznać do manipulacji.

7 Plagiat i prawa autorskie

7.1 Prawo autorskie

Prawo autorskie – nazywane również prawem własności intelektualnej – reguluje Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, która wskazuje, że każdemu twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim oraz że ma on prawo do wynagrodzenia za korzystanie z utworu. Prawo autorskie chroni utwory, a więc każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia.

Każde artystyczne wykonanie utworu jest chronione zupełnie niezależnie od jego wartości, przeznaczenia, czy sposobu wyrażenia. Z naruszeniem praw autorskich mamy do czynienia za każdym razem, gdy korzystamy z utworu poza zakresem dozwolonego użytku, nie posiadając odpowiedniego zezwolenia. Naruszenie tych praw może skutkować odpowiedzialnością cywilną lub karną.

Rozwój Internetu w ostatnich latach spowodował ogromny wzrost liczby użytkowników doprowadzając do tego, że naruszanie praw autorskich jest bardzo powszechne i co więcej niezwykle proste.

Zgodnie z art. 1 ust. 1 wspomnianej wyżej ustawy, autorsko - prawna ochrona materiału prasowego obejmuje wszelkie formy jego wyrażenia, w tym m.in. w formie wydruku papierowego, przekazu internetowego, zapisu na zewnętrznym nośniku (np. pendrive), wprowadzenia do pamięci stałej komputera itp.

7.2 Co to jest plagiat?

W polskim systemie prawnym nie istnieje legalna definicja pojęcia „plagiat".

Można posłużyć się językiem łacińskim, gdzie słowo plagiatus oznacza skradziony. Zatem przyjęto powszechnie, że plagiat to przywłaszczenie autorstwa cudzego wytworu lub jego części. Encyklopedia PWN podaje, że plagiat to naruszenie osobistych praw autorskich polegające na przywłaszczeniu całości lub części cudzego utworu, pracy, nauk, itp., a także zapożyczenie treści z cudzych dzieł (bez względu na nośnik), podane jako własne i opublikowane pod własnym nazwiskiem.

7.3 Tworzenie bibliografii, przypisów

Są to krótkie notki i objaśnienia autora odnoszące się do wskazanych wyrazów, zwrotów lub fragmentów tekstu. Wskazują źródło pochodzenia określonych danych, poglądów, cytatów. Mogą także spełniać funkcję polemiczną, objaśniającą, ilustrującą lub uzasadniającą szczegółowo (poza tekstem właściwym) postawioną w pracy tezę. Przywoływanie cudzych myśli w oryginalnym brzmieniu lub parafrazowanie ich bez udokumentowania tego w formie przypisu stanowi naruszenie prawa i traktuje się jako plagiat.

- Przypisy bibliograficzne – to notki wskazujące wykorzystane źródła
- i opracowania; zawierają opisy bibliograficzne dokumentów, z których pochodzą informacje lub cytaty zawarte w tekście.
- Opis bibliograficzny – to uporządkowany zespół danych o dokumencie (książce, artykule itp.), służący do jego identyfikacji.
- Bibliografia – uporządkowany spis dokumentów (książek, artykułów
- z czasopism itp.) wybranych według pewnych kryteriów, sporządzony według określonych zasad oraz spełniający określone zadania informacyjne.
- Bibliografia załącznikowa – to wykaz dokumentów (drukowanych i elektronicznych) wykorzystanych przez autora przy pisaniu pracy. Zawiera opisy bibliograficzne cytowanych lub związanych z tematem publikacji uszeregowane w określonej kolejności.

7.4 Plagiat - konsekwencje

Dopuszczając się plagiatu, narażamy się na odpowiedzialność cywilną, jak i karną. Odpowiedzialność cywilna będzie prowadziła do zaniechania naruszenia czy wydania osiągniętych nielegalnie korzyści. Prawdziwy autor ukradzionego utworu może również domagać się opublikowania przeprosin, wycofania plagiatu z obrotu, a często również zadośćuczynienia finansowego.

Warto podkreślić, że plagiaty, które nie stanowią naruszenia prawa autorskiego mogą wiązać się z odpowiedzialnością prawną, ale jej podstawą nie będzie w tym przypadku prawo autorskie. Takie plagiaty wówczas mogą być np. naruszeniem cudzych dóbr osobistych, które są chronione na podstawie kodeksu cywilnego.

7.5 Legalne źródła filmów/muzyki/gier

Internet zawiera sporą gamę utworów muzycznych. Znaczna część osób pobiera pliki muzyczne nie zastanawiając się, czy jest to legalne. Wszystko zależy od celu korzystania z tych zasobów. Jeśli bowiem pobieramy muzykę za darmo wyłącznie na użytek własny lub najbliższego otoczenia, nie łamiemy prawa. Jeżeli jednak wykorzystujemy ją do celów komercyjnych, jest to nielegalne (chyba że autor na to zezwolił).

Gdy chcemy wykorzystywać darmową muzykę w celach komercyjnych np. jako ścieżkę dźwiękową na naszym kanale You Tube, powinniśmy zainteresować się odpowiednią licencją, która zezwala na udostępnianie treści szerszemu gronu użytkowników.

Licencje Creative Commons

Warto zwrócić tu uwagę zwłaszcza na zestaw licencji Creative Commons (CC), dzięki którym zachowane zostają prawa autorskie i równocześnie jest możliwość dzielenia się własną twórczością z innymi. Szczególnie przydatna jest licencja CC0 opatrzona domeną publiczną.

Jako ciekawostkę prezentujemy poniżej najlepsze strony z darmową muzyką:

- Soundcloud
- ReverbNation
- Free Music Archive
- Jamendo
- Live Music Archive
- Musopen
- Audionautix
- Bandcamp
- SoundClick
- NoiseTrade

8 Objawy i przeciwdziałanie dysfunkcyjnemu korzystaniu z sieci

8.1 Uzależnienie od Internetu – objawy

Uzależnienie od Internetu to stosunkowo nowe zjawisko, przybiera jednak na sile wraz z upowszechnianiem się dostępu do globalnej sieci oraz stałym wzrostem liczby jej użytkowników. Jest to zaburzenie psychiczne i ma wiele cech wspólnych z innymi rodzajami uzależnień.

8.2 Jak reagować na objawy u dziecka?

Uzależnienie od Internetu to zespół zależności mających swoje źródła w nadużywaniu dostępu do Internetu, które skutkują negatywnym wpływem na funkcjonowanie jednostki w sferze:

- psychicznej,
- społecznej,
- rodzinnej,
- relacji międzyludzkich,
- ekonomicznej.

Wielogodzinne, niekontrolowane korzystanie z Internetu wywołuje u człowieka szereg nieprzyjemnych uczuć (ból/lęk/cierpienie), które mogą z kolei prowadzić do znacznego pogorszenia jakości życia.

Z raportu 2018 Global Digital przygotowanego przez We Are Social i Hootsuite wynika, że dziś z Internetu korzysta ponad 4 mld ludzi na całym świecie, co stanowi wzrost o 7 proc. w porównaniu z poprzednim rokiem. Ta ogromna masa internautów to osoby potencjalnie narażone na uzależnienie się od korzystania z sieci.

Szacuje się, że globalnie uzależnieniem od Internetu dotkniętych może być 6 proc. internautów. Dane zebrane w 2003 r. przez Center for On-line Addiction na podstawie obserwacji 17 tys. osób wykazały, że właśnie taki odsetek użytkowników sieci wymaga leczenia, a blisko co trzeci internauta traktuje sieć jako sposób na ucieczkę przed problemami, co może łatwo stać się czynnikiem uzależnienia.

Rodzaje uzależnień od Internetu

Według typologii zaproponowanej przez Kimberly Young uzależnienie związane z używaniem komputera można podzielić na pięć rodzajów:

- erotomania internetowa (cybersexual addiction) – czyli kompulsywne korzystanie z serwisów pornograficznych;
- socjomania internetowa (cyber-relationship addiction) – oznacza uzależnienie od chatów i internetowych kontaktów społecznych;
- uzależnienie od sieci internetowej (net compulsions) – w kategorii tej mieszczą się uzależnienia od internetowego hazardu, od gier sieciowych, od obsesyjnego grania na rynkach finansowych, czy zakupów w Internecie, a także od obserwowania mediów społecznościowych;
- przeciążenie informacyjne – (information overload) czyli potrzeba sięgania do dostępnych w Internecie danych;
- uzależnienie od komputera (computer addicion) – obejmuje wszelkie uzależnienia niekoniecznie związane z dostępem do sieci.

Charakterystyczny dla osób uzależnionych jest „głód Internetu" – dostęp do sieci staje się środkiem pozwalającym uniknąć nieprzyjemnych emocji. Pojawia się dyskomfort psychiczny związany z brakiem możliwości dostępu do sieci – niepokój, zmienny nastrój, irytacja, czy wybuchy agresji. Życie i aktywności osoby uzależnionej koncentrują się wokół komputera, wszystko podporządkowane jest sesjom internetowym, co skutkuje trudnościami w wykonywaniu codziennych obowiązków. Uzależnienie od Internetu może skutkować także depresją.

Z uzależnieniem od Internetu wiąże się zjawisko FOMO, czyli silny strach przed tym, że naszej uwadze umknie jakaś ważna informacja, czy wydarzenie (ang. „fear of missing out"). Mechanizm ten może powodować pogłębienie psychicznej zależności od korzystania z sieci.
U dzieci nadużywanie Internetu najczęściej przejawia się:

- apatią,
- agresją,
- bezsennością,
- społecznym wyizolowaniem.

Leczenie osób uzależnionych od Internetu jest trudne ponieważ brakuje państwowych placówek specjalizujących się w pomocy takim osobom, a istniejące ośrodki leczenia uzależnień koncentrują się na alkoholikach i narkomanach. Dodatkowych trudności przysparza fakt, że „siecioholicy" potrafią spędzać w Internecie kilkanaście, a nawet kilkadziesiąt godzin dziennie. W efekcie czego są zbyt zabsorbowani swoim nałogiem, by dostrzec problemy ze zdrowiem, a ponad to często odwykli od kontaktów z ludźmi, a więc także z lekarzami.
Najważniejszym orężem w walce z internetowym uzależnieniem jest psychoterapia, a najskuteczniejszy jest jej nurt poznawczo-behawioralny. Proces leczenia opiera się na zmianie nawyków korzystania z Internetu, co ma stopniowo przywrócić w życiu pacjenta miejsce na inne, niewirtualne rozrywki, aktywności i relacje.
Ponieważ w dzisiejszych czasach nie sposób wyeliminować kontaktu z komputerem stosuje się harmonogram korzystania z sieci, zmierzając do tego, by kontakty z Internetem były raczej krótsze, a częstsze, niż wielogodzinne sesje. Pomocne są także techniki kształtujące nowe zachowania związane z korzystaniem z komputera, takie jak notowanie internetowych aktywności w dzienniku, zmienianie pór korzystania z sieci, czy trening stopniowego wydłużania przerw w dostępie do Internetu.

9 Analiza zagrożeń technologicznych związanych z korzystaniem z sieci

9.1 Szkodliwe oprogramowanie

Złośliwe (szkodliwe) oprogramowanie to ogólny termin określający wszelkiego rodzaju złośliwe oprogramowanie zaprojektowane do uszkadzania lub wykorzystania dowolnego programowalnego urządzenia lub sieci.
Złośliwe oprogramowanie obejmuje wszystkie rodzaje złośliwego oprogramowania, w tym wirusy, które cyberprzestępcy wykorzystują z wielu różnych powodów, m.in. w celu:

- Oszukania ofiary aby dobrowolnie podała swoje dane dane osobowe;
- Kradzieży danych finansowych ofiary;
- Przejęcia kontroli nad wieloma komputerami;
- Zainfekowania komputerów i używania ich do kryptowalut.

Istnieje wiele złośliwych programów np.:

- Wirusy, które wykonują różnego typu szkodliwe działania;
- Oprogramowanie ransomware, które instaluje się na komputerze, szyfruje pliki, a następnie żąda okupu (zwykle w walucie bitcoin) w zamian za zwrot tych danych użytkownikowi.
- Scareware - Cyberprzestępcy, chcąc przekonać do zakupu fałszywej aplikacji informują, że nasze komputery lub smartfony zostały zainfekowane;
- Robaki - mają zdolność kopiowania się z urządzenia na urządzenie, zwykle wykorzystując słabość zabezpieczeń w oprogramowaniu lub systemie operacyjnym;
- Oprogramowanie szpiegujące - program instalowany na komputerze, zwykle bez wyraźnej wiedzy, który przechwytuje i przesyła dane osobowe lub zwyczaje związane z przeglądaniem Internetu do swojego użytkownika. Oprogramowanie szpiegujące umożliwia swoim użytkownikom monitorowanie wszystkich form komunikacji na docelowym urządzeniu.
- Konie trojańskie - podszywają się pod nieszkodliwe aplikacje, nakłaniając użytkowników do ich pobrania i korzystania z nich.
- vAdware - to oprogramowanie z reklamami, które pokazuje użytkownikom niechciane reklamy i zwykle po wykonaniu określonej czynności wyświetla migające reklamy lub wyskakujące okna.

Istnieje wiele sposobów ochrony przed złośliwym oprogramowaniem, stąd koniecznie należy uwzględnić poniższe najważniejsze wskazówki:

- Aktualizuj system operacyjny i aplikacje;
- Nigdy nie klikaj linku w wyskakującym okienku;
- Ograniczaj liczbę aplikacji na urządzeniach. Instaluj tylko te aplikacje, które uważasz za potrzebne i które będziesz regularnie używać;
- Stosuj programy antywirusowe;
- Nie pożyczaj telefonu ani nie pozostawiaj urządzeń bez nadzoru z jakiegokolwiek powodu i koniecznie sprawdź ich ustawienia oraz aplikacje;
- Uważnie wybieraj witryny, które odwiedzasz;
- Uwaga na e-maile z prośbą o podanie danych osobowych.
- Unikaj niebezpiecznych witryn
- Kupuj oprogramowanie zabezpieczające tylko od renomowanej firmy
- Korzystaj z oficjalnych sklepów z aplikacjami

Jak rozpoznawać zainfekowanie komputera?

- Komputer pracuje wolno;
- Komputer zaczyna wyświetlać wyskakujące okna i komunikaty;
- Komputer przekierowuje Cię na strony internetowe, których nie wyszukiwano;
- Komputer nie może połączyć się z Internetem;
- Program antywirusowy zniknął z urządzenia;
- Aplikacje nie uruchamiają się lub komputer zaczyna wyświetlać błędy;
- Na komputerze znajduje się nowy program, którego nie instalowano;
- Pojawiają się komunikaty w innym języku;
- Pliki użytkownika zostały usunięte.

9.2 Popularne i darmowe programy antywirusowe

Program antywirusowy to bardzo przydatny element wyposażenia PC. Nie każdy z nich wymaga opłaty, niektóre są dostępne za darmo.

Dobry darmowy program antywirusowy musi być aktualny i dlatego też należy wybierać programy, nad których rozwojem producenci cały czas czuwają.

Przykładowe, darmowe programy antywirusowe:

- Avast Antywirus
- AVG AntiVirus Free
- Panda Dome
- Comodo AntiVirus
- Avira Free Antivirus
- Bitdefender Antivirus Free Edition
- Ad-Aware Antivirus Free
- 360 Total Security
- SecureAPlus

10. Hasła

Hasło to ciąg znaków, używany zazwyczaj podczas logowania do różnego rodzaju zasobów, m.in. systemów operacyjnych, baz danych, portali, poczty e-mail itp.

Hasło powinno pozostać znane wyłącznie osobie, która je ustala. Nie należy go udostępniać, ani zapisywać w miejscach dostępnych dla innych użytkowników.

Hasła powinny składać się z:

- co najmniej 8 znaków;
- dużych i małych liter;
- cyfr i znaków specjalnych (np. *, &, $ itp.).

Jednocześnie wybierając hasło należy unikać:

- powtórzenia loginu;
- słów, które znajdziemy w słowniku, np. football, mojehaslo, Bydgoszcz;
- haseł będących wyłącznie cyframi lub wyłącznie literami;
- ciągów znaków występujących obok siebie na klawiaturze, np. 123qwerty, zxcvbnm, !@#123.

11 Popularne portale społecznościowe i witryny internetowe

11.1 Facebook

Serwis społecznościowy, w ramach którego zarejestrowani użytkownicy mogą tworzyć sieci i grupy, dzielić się wiadomościami i zdjęciami oraz korzystać z aplikacji, będący własnością Meta Platforms z siedzibą w Menlo Park.

11.2 Instagram

Fotograficzny serwis społecznościowy hostingu zdjęć, połączony z aplikacją o tej samej nazwie (dostępną na systemy operacyjne iOS i Android), który umożliwia użytkownikom edycję zdjęć i filmów, stosowanie do nich filtrów[cyfrowych oraz udostępnianie ich w różnych serwisach społecznościowych.

11.3 Snapchat

Snapchat – aplikacja mobilna służąca do wysyłania filmów i zdjęć, które można oglądać przez nieokreślony czas, dostępna na urządzenia z systemami operacyjnymi Android oraz iOS.

11.4 Twitter

Jest to serwis społecznościowy udostępniający usługę mikroblogowania. Zarejestrowany użytkownik może wysyłać i odczytywać tak zwane tweety. Tweet to krótka wiadomość tekstowa (maks. 280 znaków) wyświetlana na profilu autora wpisu oraz pokazywana użytkownikom, którzy obserwują dany profil.

11.5 TikTok

TikTok to aplikacja, dająca dostęp do tworzonych przez użytkowników z całego świata, krótkich materiałów wideo. Oczywiście daje ona również możliwość tworzenia i udostępniania własnych, kilkunastosekundowych klipów z zewnętrznymi ścieżkami dźwiękowymi. Większość dostępnych w TikTok filmików to tzw. „lipsync", w których osoby na filmie udają, że śpiewają.

11.6 YouTube

YouTube – serwis internetowy założony w lutym 2005 roku, który umożliwia bezpłatne umieszczanie, nadawanie na żywo, ocenianie i komentowanie filmów.

11.7 Ask.fm

Askfm (poprzednio Ask.fm) – serwis społecznościowy Questions and Answers (Pytania i Odpowiedzi), w ramach którego zarejestrowani użytkownicy mogą zadawać innym pytania oraz na nie odpowiadać.

Rysunek - Askfm

11. 8 Jak uczyć dziecko odpowiedzialnego korzystania z Internetu

Jak podaje CBOS w raporcie z badania „Korzystanie z internetu" - siedmiu na dziesięciu polskich użytkowników internetu ma konto w jakimś serwisie społecznościowym. Z social mediów korzystają i starsi i młodsi, osoby publiczne, firmy, instytucje, ale przede wszystkim prywatni użytkownicy.

Najważniejsze zasady bezpieczeństwa w mediach społecznościowych:

1. Utwórz silne hasło
2. Ogranicz dostęp do konta - Uaktywnij dwuskładnikowe uwierzytelnianie na wszystkich swoich kontach.
3. Dodawaj do listy znajomych wyłącznie osoby, które rzeczywiście znasz i którym ufasz.
4. Korzystaj tylko z oficjalnych aplikacji sieci społecznościowych
5. Dbaj o prywatność - praktycznie wszystkie serwisy społecznościowe posiadają rozwiązania zwiększające prywatność – aktywuj je! Jednocześnie należy także prześledzić ograniczenia związane z siecią znajomych (w regulaminach powinno to zostać ujęte)
6. Używaj programu antywirusowego na każdym urządzeniu z dostępem do Internetu powinien być dostępny program antywirusowy, także na tablecie i telefonie (o czym często użytkownicy nie pamiętają)
7. Czytaj regulaminy - niestety bardzo rzadko użytkownicy zdają sobie sprawę z konsekwencji jakie niesie za sobą akceptacja regulaminu na portalu społecznościowym.

12 Uprzejmość w sieci

12.1 Netykieta

Netykieta to zasady zachowania, które odpowiadają na pytanie: jak zachowywać się w Internecie.

Celem netykiety jest stworzenie dobrych ram dla działania danej społeczności internetowej oraz przeciwdziałanie takim zjawiskom jak: floodowanie, spamowanie, trollowanie itd. Nie ma jednej ustalonej odgórnie netykiety.

Podstawowe zasady netykiety (wybrane przykłady):

- Sprzeciwiaj się hejtowi - nawet jeśli spotka Cię hejt, nie odpłacaj się tym samym. Nie daj się sprowokować, nie publikuj poniżających komentarzy czy grafik.
- Nie nadużywaj CAPS LOCKA, nie pisz wyłącznie WIELKIMI LITERAMI, co jest traktowane jako krzyk.
- Pisz zgodnie z zasadami język polskiego - ortografia, odmiana, zwroty grzecznościowe – działają w internecie tak samo jak w komunikatach analogowych.
- Nie przesadzaj z emotikonami - pamiętaj, że to dodatek do całej wypowiedzi, a nie odwrotnie.
- Nie trolluj - nie publikuj zaczepnych treści wyłącznie po to, by wywołać reakcję.
- Uważaj na fake newsy – nie przesyłaj wiadomości, jeżeli nie masz absolutnej pewności, co do prawdziwości treści.
- Szanuj prawo do własności w sieci - jeśli publikujesz obrazek czy wypowiedź, podaj autora i źródło.

13 Odpowiedzialne zakupy w sieci

Zakupy za pośrednictwem Internetu rozwijają się dość dynamicznie. Coraz więcej osób korzysta z zakupów online. Niestety ułatwia to również aktywną działalność oszustom, m. in. tym którzy za pośrednictwem ofert kupna/sprzedaży wyłudzają pieniądze.

13.1 Jak uniknąć prób oszustwa

Każdy, kto korzysta ze sklepów internetowych lub portali aukcyjnych, powinien mieć świadomość o działalności oszustów, którzy stale opracowują różne sposoby na nieprawne zdobycie pieniędzy. Najpierw starają się zdobyć zaufanie, a następnie proszą o pieniądze.

Najczęściej do wyłudzenia pieniędzy dochodzi za pośrednictwem ofert kupna/sprzedaży. Na portalu aukcyjnym oszuści zamieszczają bardzo atrakcyjną ofertę kupna, która jest okazją wśród pozostałych. Oszuści bardzo umiejętnie podchodzą do klienta i są w stanie przekonać go do płatności z góry lub wpłaty zaliczki, wykorzystując jego nieświadomość i brak ostrożności w sieci. Istotny jest sposób realizowania płatności za towar.

Zatem aby uniknąć oszustwa powinniśmy:

- Korzystać ze sprawdzonych stron (istniejących na rynku od dłuższego czasu);
- Sprawdzać możliwe metody płatności oraz dane kontaktowe sprzedawcy;
- Unikać płatności z góry, bądź dokonywać ich tylko na sprawdzonych i zaufanych portalach;
- Sprawdzać opinie zarówno o sprzedawcy, jak i o sklepie;
- Nie ufać w super oferty i unikać zakupu przedmiotów o rażąco niskiej cenie;
- Zachować korespondencje ze sprzedawcą;
- Nigdy nie udostępniać żadnych swoich haseł dostępowych;
- W przypadku zamawiania sprzętu elektronicznego, pytać o dołączenie oryginalnego oprogramowania oraz instrukcji obsługi;
- Jeżeli otrzymujemy wiadomość od sprzedawcy, nie wchodzimy na stronę sklepu, bądź firmy za pomocą przysłanego linku;
- Zawsze wchodźmy wpisując samodzielnie adres w przeglądarkę internetową na stronę sklepu lub firmy.

13.2 Jak nauczyć dziecko rozsądnego dokonywania zakupów przez Internet

Podczas zakupów z dziećmi, należy kierować się pewnymi zasadami, które warto ustalić z dzieckiem jeszcze przed zakupami (także tymi stacjonarnymi):

- ***Należy zapoznać dziecko z zasadami bezpieczeństwa podczas płatności***

Każda osoba, także dziecko powinno zdawać sobie sprawę z zasad bezpieczeństwa i potencjalnych zagrożeń, jakie mogą czyhać w sieci.

- ***Należy ustalić plan działania***

Trzeba jasno określić cel i miejsce działania. Dzieci potrzebują konkretnie sprecyzowanych celów.

- ***Należy kupować tylko rzeczy z listy potrzeb***

Przed zaplanowanymi zakupami należy wypisać potrzebne produkty na kartce, a dziecko może brać w tym udział w formie dodatkowej aktywności i zabawy.

- ***Należy wyznaczyć dziecku budżet na jego zakupy***

Przed zakupami należy ustalić kwotę, którą ma do dyspozycji podczas zakupów. Wyznaczoną kwotę dziecko może przeznaczyć na co tylko chce, ale możemy dawać cenne rady, podpowiadać.

- ***Należy porównać ceny tego samego produktu w różnych sklepach***

W przypadku zakupów w internecie, możemy bez problemu poszukać konkurencyjnych ofert danego produktu

- ***Należy prześledzić regulamin zakupów i zwrotu produkt***

Każdy sklep może mieć nieco unikatowe zasady z tym związane i warto je prześledzić przed zakupami.

14 Bibliografia

Publikacje

- Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa, Marek Górka, Difin 2017
- Cyberbezpieczeństwo, Redakcja naukowa: Cezary Banasiński, Marcin Rojszczak, Wolters Kluwer Polska 2020
- Cyberprzemoc włącz blokadę na nękanie, Anna Borkowska, NASK Państwowy Instytut Badawczy 2019
- Ochrona małoletnich przed szkodliwymi treściami w sieci – rekonesans, Dagmara Sidyk, Marlena Sztyber, Dyskurs&Dialog 2019
- Fake newsy i inne fałszerstwa od średniowiecza do XXI wieku, Alex Boese, Amber Sp. z o.o. 2018

Strony internetowe:

- https://niebezpiecznik.pl/
- https://www.cyfrowobezpieczni.pl/