Dzień Otwartej Szkoły – 7.11.2019r.

**Rozszerzona prelekcja e-learningowa dla Rodziców uczniów klas I-VIII na temat:**

**„Europejski Miesiąc Cyberbezpieczeństwa 2019: Cyberhigiena i cyberbezpieczeństwo.
Patostreamy – jak uchronić najmłodszych i nastoletnich Internautów
przed wpływem szkodliwych nagrań w Sieci”**

Przełom października i listopada w naszej szkole tradycyjnie (już po raz siódmy) obchodzony jest jako Europejski Miesiąc Cyberbezpieczeństwa (European Cyber Security Month). Ogólnoeuropejska kampania ECSM organizowana jest przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) z inicjatywy Komisji Europejskiej, natomiast w Polsce kampanię mającą podnieść świadomość bezpieczeństwa w Internecie koordynuje Naukowa Akademicka Sieć Komputerowa. W 2019 roku Europejski Miesiąc Cyberbezpieczeństwa ma dwa tematy przewodnie: cyberhigienę oraz cyberbezpieczeństwo w kontekście nowych technologii.

## Cyberhigiena

### Cyberhigiena to zwykłe, codzienne działania, które podnoszą nasze bezpieczeństwo on-line. Regularne mycie rąk zabezpiecza nas przed infekcjami, a przeglądy techniczne samochodu przed groźnymi awariami. Tak samo aktualizowanie oprogramowania i zmiana haseł dostępu do kont i profili, powinny stać się naszymi zdrowymi, odpowiedzialnymi nawykami. W ten sposób i dzieci i dorośli zwiększają swoje bezpieczeństwo w sieci.

### Jeśli chcemy efektywnie zadbać o naszą cyberhigienę, konieczne jest zapoznanie się z pakietem dobrych praktyk w ramach kampanii [STÓJ.POMYŚL.POŁĄCZ](https://stojpomyslpolacz.pl/stp/dobre-praktyki):

## 1: ZADBAJ O AKTUALIZACJE I BEZPIECZEŃSTWO URZĄDZEŃ

* **Korzystaj z aktualnego oprogramowania:** Regularnie aktualizuj system operacyjny, program antywirusowy, przeglądarkę internetową. Dzięki aktualizacjom łatwiej ustrzeżesz się przed szkodliwym oprogramowaniem i innymi zagrożeniami obecnymi w sieci.
* **Włącz aktualizacje automatyczne:** Wiele aplikacji oferuje możliwość automatycznego pobierania aktualizacji, w celu ochrony przed nowymi zagrożeniami. Skorzystaj z tego rozwiązania wszędzie tam, gdzie to możliwe.
* **Chroń urządzenia podłączane do sieci:** Nie tylko komputery, ale także smartfony, tablety i inne podłączane do Internetu urządzenia, potrzebują ochrony przed wirusami i złośliwym oprogramowaniem.
* **Skanuj przed użyciem:** Nie podłączaj do komputera nośników, których pochodzenie nie jest Ci znane. Dyski zewnętrzne, pendrive’y, czy inne nośniki danych mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość skorzystaj ze skanera antywirusowego.

## 2: ZABEZPIECZ DOSTĘP DO POSIADANYCH INFORMACJI

* **Dwuskładnikowe uwierzytelnianie:** Zadbaj o swoje konta w sieci. Logowanie oparte wyłącznie o nazwę użytkownika i hasło nie jest wystarczająco bezpieczne (szczególnie w przypadku konta e-mail, portalu społecznościowego czy bankowości internetowej). Aktywuj weryfikację tożsamości opartą o dodatkowy składnik, np. kod SMS, token, czy klucz sprzętowy.
* **Stwórz mocne hasło:** Dobre hasło składa się przynajmniej z 12 znaków. Skup się na pozytywnych zdaniach lub zwrotach o których lubisz myśleć i które łatwo zapamiętasz (np. „Kocham miasto muzyki”). Na wielu stronach internetowych, możesz przy wprowadzaniu hasła używać spacji.
* **Jedno hasło, jedno konto:** Jeżeli chcesz utrudnić działania przestępcom, dla każdego konta przypisz oddzielne hasło. Niezbędne minimum, to rozdzielenie kont używanych do pracy i celów prywatnych. Zadbaj o silne hasło do najistotniejszych serwisów (bankowość, poczta elektroniczna, portale społecznościowe).
* **Przechowuj bezpiecznie:** Każdy może zapomnieć swojego hasła. W celu ułatwienia nam życia stworzono aplikacje zwane menadżerami haseł. Służą do bezpiecznego przechowywania danych dostępowych. Możesz z nich korzystać. Jeżeli zapisałeś hasło na kartce (lepiej tego nie rób), postaraj się umieścić ją
w bezpiecznym miejscu, z dala od komputera.

## 3: KORZYSTAJ ROZWAŻNIE

* **Zatrzymaj się, jeśli masz wątpliwości:** Linki i załączniki w wiadomościach e-mail, spreparowane posty
w mediach społecznościowych oraz reklamy - to częste metody używane przez przestępców w celu kradzieży danych. Jeżeli wydają Ci się podejrzane, po prostu je zignoruj. Nawet, jeżeli źródło wygląda na zaufane.
* **Uważaj na hotspoty Wi-Fi:** Ogranicz aktywność w publicznie dostępnych sieciach Wi-Fi. Używając poza domem kluczowych serwisów (poczta e-mail, bankowość internetowa, portale społecznościowe) bezpieczniej będzie użyć własnego modemu LTE lub połączenia VPN. Pamiętaj o wyłączaniu transmisji Wi-Fi i Bluetooth, kiedy z niej nie korzystasz.
* **Chroń swoje finanse:** Korzystając z bankowości internetowej i sklepów online, upewnij się, że połączenie jest objęte szyfrowaniem (zielona kłódka oraz prefiks „https://” w pasku adresu). Odczytując kod SMS uwierzytelniający transakcję, zweryfikuj kwotę przelewu i numer rachunku odbiorcy!

## 4: BĄDŹ ŚWIADOMYM UŻYTKOWNIKIEM

* **Pozostań na bieżąco:** Nie lekceważ informacji ze świata bezpieczeństwa IT. Jeśli coś podawane jest do publicznej wiadomości, najczęściej dotyczy także Ciebie.
* **Pomyśl, zanim zadziałasz:** Bądź ostrożny wobec korespondencji zachęcającej do natychmiastowych działań. Szczególnie, jeśli ktoś oferuje Ci łatwy zysk lub próbuje nakłonić do podania prywatnych danych. Robiąc zakupy w sieci, weryfikuj reputacje sklepów. Dziel się wiedzą z rodziną i znajomymi.
* **Zadbaj o kopie zapasowe:** Zabezpiecz efekty swojej pracy, muzykę, zdjęcia, cenne dokumenty. Twórz kopie zapasowe i przechowuj je w bezpiecznym miejscu.

## 5: CHROŃ SWOJĄ PRYWATNOŚĆ

* **Informacje mają wartość:** dane na Twój temat, takie jak historia zakupów czy historia lokalizacji są cenne. Zwracaj uwagę kto i co (aplikacje, strony internetowe) próbuje uzyskać do nich dostęp.
* **Dostosuj ustawienia prywatności w serwisach online i na urządzeniach:** Dzięki nim, możesz lepiej chronić Twoje dane. Sam decyduj, jak wiele informacji na swój temat chcesz udostępnić innym.
* **Pomyśl, zanim udostępnisz:** Zwracaj uwagę na przesyłaną do sieci treść, zasięg komunikatu, a także sposób, w jaki może zostać odebrany.

## 6: TWÓRZ KULTURĘ BEZPIECZNEJ SIECI

* **Twoje zachowanie w sieci ma znaczenie:** Stosowanie dobrych praktyk buduje kulturę bezpiecznej sieci. To, co robisz, ma znaczenie (w domu, w pracy, gdziekolwiek jesteś).
* **Traktuj innych tak, jak sam chciałbyś być traktowany.**
* **Wspieraj walkę z cyberprzestępczością:** Jeżeli zaobserwujesz niepokojące zjawiska, nie wahaj się o tym poinformować: [*https://incydent.cert.pl*](http://incydent.cert.pl/) (zgłaszanie incydentów naruszających bezpieczeństwo w sieci) [*https://dyzurnet.pl*](http://dyzurnet.pl/)(przyjmowanie zgłoszeń dotyczących nielegalnych treści w Internecie).

**W kontekście cyberbezpieczeństwa oraz wspierania walki z cyberprzestrzępczością chcielibyśmy zwrócić uwagę wszystkich Rodziców na problem zwiększającej się wśród najmłodszych Internautów popularności patostreamów.**

**Patostreamy – co to takiego?**

Patostreamy to jeden z najbardziej negatywnych przykładów korzystania z Internetu. Według definicji opracowanej przez Fundację "Dajemy Dzieciom Siłę", tzw. patostreaming to treści prezentowane w sieci
w postaci transmisji internetowej (stream), fragmentów transmisji (shoty), filmów, zdjęć i innych form przekazu, w których nadawca lub grupa nadawców prezentują zachowania sprzeczne z normami społecznymi, niosące demoralizujący przekaz, obejmujący zachowania takie, jak przemoc fizyczna, psychiczna i seksualna. Promują zażywanie substancji psychoaktywnych, gloryfikują poniżanie, lekceważenie innych. . Najsmutniejsze w modzie na patostreamy jest to, że nagrania te cieszą się dużą popularnością, zwłaszcza wśród nastoletnich użytkowników Internetu. O skali zjawiska alarmują organizacje pozarządowe, wychowawcy, psychologowie
i badacze społeczni. Zwracają uwagę, że treści te mogą oglądać dzieci, czego rodzice często nie są świadomi.

**Popularność wśród najmłodszych Polaków – wyniki badań**

Patotreści ogląda 37 % dzieci w wieku od 13 do 15 lat, a prawie 30 % robi to częściej niż raz
w tygodniu - takie niepokojące dane płyną z raportu Fundacji Dajemy Dzieciom Siłę, który powstał we współpracy z biurem Rzecznika Praw Obywatelskich w 2019 roku.

Wyniki badania pokazują, że patotreści w Internecie ogląda 37 % dzieci w wieku 13-15 lat: 15 % badanych ogląda je codziennie lub prawie codziennie, 28 % raz lub dwa razy w tygodniu. Nawet 10-latki, a może nawet młodsze dzieci, też trafiają na tego typu treści.

Jak wynika z raportu, głównym źródłem wiedzy nastolatków na ten temat jest informacja ustna od osoby znajomej (53 % wskazań), 30 % badanych trafiło na patotreści przypadkiem, bo na przykład wyświetliły się one jako polecane przez strony lub aplikacje z filmami, 29 % usłyszało o tym w mediach, dla 27 % respondentów źródłem informacji był link od znajomych.

Jeśli chodzi o podjęcie jakiejkolwiek aktywności po oglądaniu "patotreści", zadeklarowało ją 65 % badanych. Najczęściej oznaczali oni filmy jako nielubiane (47%). Trzy kolejne aktywności o porównywalnym odsetku wskazań (około 30%), to: udostępnianie treści znajomym, polubienie filmu oraz komentowanie shotów
na YouTube. Aż 18 % udziela się podczas patostreamów na czacie, z kolei 5 % nastolatków wpłaca patostreamerom darowizny!!!

Większość osób (88%), które oglądały patotreści, twierdzi, że było to dla nich niepokojące doświadczenie.
Z raportu wynika, że patotreści postrzegane są przez młodzież przede wszystkim jako szkodliwe, zachęcające innych do naśladowania patologicznych zachowań (87 %), a co za tym idzie powinny być zakazane
w internecie (82 %). Bardziej krytyczne w stosunku do tych materiałów są osoby, które ich nie oglądały,
a tylko o nich słyszały. Krytycznie częściej wypowiadają się dziewczęta. Młodsze dzieci (10-12 lat) są bardziej skłonne do oglądania tych treści. 38 % badanych uważa, że patotreści pokazują prawdziwe życie. Co piąty widz deklaruje, że lubi je oglądać. 59 % badanych wskazało, że ktoś dorosły rozmawiał z nimi na temat patotreści.

## Skąd się bierze popularność patostreamów?

To, co szokujące, co wykracza poza normy moralne i społeczne, co jest tematem tabu, jest również atrakcyjne i popularne. Zwłaszcza wśród młodych ludzi, którzy chcą się wyróżniać i imponować innym. Właśnie na takim mechanizmie opiera się popularność patostreamów.

Ich autorzy lubią szokować [przemocą](https://www.mjakmama24.pl/dziecko/edukacja/przemoc-w-szkole-jak-reagowac-i-jak-rozmawiac-z-dzieckiem-o-jego-problemach-film%2C563_6482.html), brutalnością, lekceważeniem wszelkich zasad, a osoby subskrybujące ich kanały zachwycają się ich „odwagą” i zamiłowaniem do ryzyka. Podoba im się możliwość oglądania ich życia za pomocą kamery, ale szansa współtworzenia filmów – często decydują oni o przebiegu akcji, porozumiewając się z youtuberem w trakcie relacji live.

Warto dodać, że autorzy patostreamów, popularność swoich kanałów mierzą nie tylko liczbą subskrypcji (najpopularniejsi tzw. patonadawcy mają nawet setki tysiące odsłon), ale również pieniędzmi. Zdarza się bowiem, że zbierają „zamówienia” na szokujące filmiki i realizują je po wpłaceniu przez fanów określonej kwoty na ich konto – to tzw. donejty. To znaczy każdy, kto ogląda taki materiał, taki stream może przekazać małą kwotę zachęcając nadawców do przekraczania kolejnych granic, do podejmowania kolejnych, często przemocowych zachowań (podobno miesięcznie patoyoutuberzy mogą zarobić w ten sposób od kilku do kilkudziesięciu tysięcy zł).

## Czy patostreamy to przestępstwo?

Patostreamy są niestety domeną polskiego Internetu - zjawisko ich powstawania w naszym kraju znacznie wzrosło w latach 2017–2018. Oczywiście na całym świecie spotkać można ludzi, którzy umieszczają w sieci głupie, wulgarne czy nawet pełne przemocy filmy, jednak w naszym kraju tendencja ta jest wyjątkowo silna. Na tyle, że zyskała własną nazwę oraz zainteresowanie policji, która interesuje się [bezpieczeństwem w sieci](https://www.mjakmama24.pl/rodzice/dom-prawo-finanse/jak-zadbac-o-bezpieczenstwo-dziecka-w-internecie-poradnik%2C569_6381.html). Niektóre filmiki rejestrujące pobicia czy inne przestępstwa trafiły w ręce odpowiednich służb, co pozwoliło na skazanie autorów kilku takich patostreamów. Sama publikacja patostreamów nie jest zabroniona, chociaż coraz częściej bywa cenzurowana przez Youtuba. Jednak utrwalona relacja z przestępstwa może być dowodem
w trakcie śledztwa. Niestety, nie jest to proste, ponieważ filmy zazwyczaj znikają z sieci po zakończeniu transmisji live, a wraz z nimi dowody na popełnienie przestępstwa.

**Dlaczego dzieci i nastolatki oglądają patostreamy?**

To, że dzieci i młodzież interesują się patostreamingiem, można uznawać za niedorzeczne – w końcu oglądanie przemocy fizycznej czy kierowanych ku innym ludziom wulgaryzmów ciężko uznać za rozrywkę. Warto jednak pamiętać, że najmłodsi nie kierują swoich oczu ku takim programom bez powodu.

Współczesne tempo życia nie sprzyja budowaniu w pełni poprawnych relacji rodzinnych – zaganiani rodzice, wracający z pracy każdego dnia późnym wieczorem, nierzadko nie są autorytetem dla swojej pociechy.

Takim może się za to stać jeden z patostreamerów – nastolatek może traktować osobę, która produkuje tego rodzaju filmiki, za kogoś, kto coś w życiu osiągnął (tym czymś mogą być np. pieniądze lub duża ilość subskrybentów – nie od dziś wiadomo, że świat internetowy dla współczesnej młodzieży jest niezwykle ważny). Takie „autorytety” w życiu młodego człowieka niczego dobrego nie przynoszą, co gorsza – może się on jeszcze zacząć inspirować ich działaniami i sam zaczynać je powielać.

Czasami zainteresowanie patostreamingiem można uznawać za swego rodzaju objaw – zdarza się, że treści tego typu oglądają osoby, które **nie do końca radzą sobie ze swoją własną psychiką**. Poczucie osamotnienia
i odrzucenia (przez rówieśników, ale i rodziców), brak wiary w siebie czy kompleksy bywają przyczyną zainteresowania patostreamingiem – kiedy młody człowiek widzi, że komuś jest mimo wszystko gorzej niż jemu, dochodzić może wtedy do chwilowej poprawy jego własnego nastroju. Zdecydowanie nie tędy droga
– oglądanie patostreamingu prowadzi do wykształcania się u nastolatka niewłaściwych postaw moralnych.

## Dlaczego patostreamy są groźne?

Najważniejszą kwestią, którą poruszają wszyscy badający sprawę patostreamów jest kwestia bezpieczeństwa. Chodzi zarówno o ofiary filmików, jak i o odbiorców relacji, którymi często są małe dzieci i młodzież. Śledzenie relacji z pobicia czy gwałtu może być potężna traumą, może nieprawidłowo kształtować osobowość dziecka.

Wielu subskrybujących kanały nastolatków nie zdaje sobie sprawy z tego, że oglądając filmy bierze udział
w wyrządzaniu komuś krzywdy, a płacąc za streaming jest współsprawcą czynu – pobicia, kradzieży, przemocy psychicznej. Dla nich jest to zabawa, często pomysł do naśladowania, rzadko natomiast powód do refleksji.

Badacze twierdzą, że skutki patostreamu u widzów mogą w dłuższej perspektywie polegać na: przyswojeniu sobie przez obserwatora nieznanych dotąd zachowań, osłabieniu hamulców powstrzymujących przed agresją, przejęciu emocji i motywacji obserwowanego patostreamera.

## Jak ochronić dzieci przed patostreamami?

Jak podkreślają specjaliści, walkę z patostreamingiem trzeba zacząć od walki z ich popularnością. Im mniej osób będzie zainteresowanych oglądaniem relacji, tym rzadziej będą one powstawały. Konieczne jest też wprowadzenie takich przepisów, które nie pozwolą youtuberom na czerpanie zysków z publikacji relacji.  Dlatego trzeba zrobić wszystko, aby dzieci i nastolatki nie miały styczności z patostreamingiem. Rodzice małych i dorastających dzieci powinni orientować się w nowych trendach w sieci, aby móc odpowiednio reagować. Wielu dorosłych nie ma pojęcia, że istnieje coś takiego jak patostreaming, dlatego nie kontroluje zachowań swoich dzieci w Internecie pod tym kątem.

Kontrolowanie tego, co oglądają dzieci w komputerze czy na smartfonie to w dzisiejszych czasach obowiązek każdego rodzica. Nie wolno zostawiać dzieci – młodszych i starszych – sam na sam z Internetem. Pomocne mogą tu być [blokady rodzicielskie](https://www.mjakmama24.pl/rodzice/dom-prawo-finanse/blokady-i-filtry-rodzicielskie%2C569_490.html), które ograniczają dostęp do niektórych treści. Trzeba też koniecznie tłumaczyć dzieciom, że patostreaming jest zły, bo wyrządza innym krzywdę i często ociera się o przestępstwo.

Eksperci Fundacji Dajemy Dzieciom Siłę radzą, aby rodzice dużo i szczerze ze swoimi pociechami rozmawiali.

**Szczera rozmowa na temat wartości i czas poświęcony dziecku to swoista szczepionka, która skutecznie pomaga chronić najmłodszych przed podejmowaniem ryzykownych zachowań, zarówno w Internecie,
jak i świecie realnym.**

*Opracowanie i kolportaż prelekcji:*

*Patrycja Karykowska, Marta Więckowska*

**Bibliografia:**

* Europejski Miesiąc Cyberbezpieczeństwa, [on-line], [dostęp 1 listopada 2019], dostępny w Internecie: [*https://bezpiecznymiesiac.pl/*](https://bezpiecznymiesiac.pl/)
* *Patotreści w Internecie. Raport o problemie*, Fundacja Dajemy Dzieciom Siłę we współpracy
z Rzecznikiem Praw Obywatelskich, Warszawa 2019
* FDDS, *Patotreści w Internecie. Raport o problemie*, [on-line], [dostęp 1 listopada 2019], dostępny
w Internecie: [*https://www.rpo.gov.pl/sites/default/files/Raport%20z%20bada%C5%84%20nastolatk%C3%B3w%20nt.%20*](https://www.rpo.gov.pl/sites/default/files/Raport%20z%20bada%C5%84%20nastolatk%C3%B3w%20nt.) *patotre%C5%9Bci.pdf*
* Patostreaming - co robimy? Deklaracja uczestników Okrągłego Stołu RPO do walki z patotreściami w Internecie, [on-line], [dostęp 1 listopada 2019], dostępny w Internecie*:* [*https://www.rpo.gov.pl/pl/content/deklaracja-uczestnikow-okraglego-stolu-rpo-do-walki-z-patotresciami-w-internecie*](https://www.rpo.gov.pl/pl/content/deklaracja-uczestnikow-okraglego-stolu-rpo-do-walki-z-patotresciami-w-internecie)
* KB/adso, [Wielogodzinne transmisje, przemoc, wulgaryzmy. Coraz więcej dzieci ogląda patotreści](https://www.tvn24.pl/wiadomosci-z-kraju%2C3/patostreamy-w-internecie-zagrozeniem-dla-dzieci-czym-jest-patostreaming%2C940671.html),
[on-line], [dostęp 1 listopada 2019], dostępny w Internecie: [*https://www.tvn24.pl/wiadomosci-z-kraju,3/patostreamy-w-internecie-zagrozeniem-dla-dzieci-czym-jest-patostreaming,940671.html*](https://www.tvn24.pl/wiadomosci-z-kraju%2C3/patostreamy-w-internecie-zagrozeniem-dla-dzieci-czym-jest-patostreaming%2C940671.html)
* Redakcja Dzień Dobry TVN, Patostreamy – patologiczne treści w Internecie, [on-line], [dostęp 1 listopada 2019], dostępny w Internecie: [*https://dziendobry.tvn.pl/a/patostreamy-patologiczne-tresci-w-internecie*](https://dziendobry.tvn.pl/a/patostreamy-patologiczne-tresci-w-internecie)
* Wójcik Małgorzata, Patostreamy – czym są i jak chronić przed nimi dzieci?, [on-line], [dostęp:
1 listopada 2019], dostępny w Internecie: *https://www.mjakmama24.pl/nastolatek/zagrozenia/ patostreamy-czym-sa-i-jak-chronic-przed-nimi-dzieci-aa-kLe5-ThxW-wUDd.html*