CYBER BEZPIECZNI

PFR Fundacja

BEZPIECZNE DZIECKO W SIECI

praktyczny przewodnik
po cyberbezpieczeństwie
dla rodziców i opiekunów

Centralny Dom Technologii

Fundacja Cyber

Dostęp do Internetu jest obecnie nieodłącznym elementem życia każdego człowieka. Chociaż sieć oferuje nieograniczone możliwości nauki, komunikacji i rozrywki, można w niej znaleźć także **zagrożenia** – związane z kwestiami bezpieczeństwa, prywatności, ale też mogące mieć wpływ na dobre samopoczucie najmłodszych użytkowników Internetu. Broszura, którą przygotowaliśmy dla Państwa przedstawia wybrane najważniejsze zagadnienia związane z cyberbezpieczeństwem i najprostsze kroki, które każdy z nas może podjąć, by zapewnić swojemu dziecku bezpieczeństwo w sieci. Jesteśmy pewni, że ta dawka praktycznej wiedzy będzie dobrym punktem startu do rozmowy z dziećmi o tym, jak odpowiedzialnie i świadomie korzystać z zasobów internetowych.

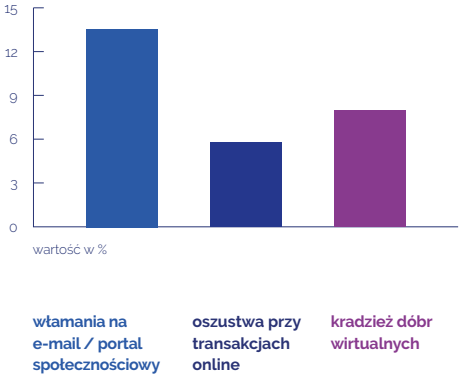
Zadbajmy wspólnie o bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni.

PORADA 1.

ZABEZPIECZ KOMPUTER, SMARTFON I TABLET SWOJEGO DZIECKA.

Najczęstszymi formami przestępczości internetowej, których ofiarami padają nastolatki i nastolatkowie są: włamania na konto e-mail lub na portalu społecznościowym (ok. 13,6% respondentów) oraz oszustwa przy transakcjach online (5,8%). Blisko 8% badanych padło ofiarą kradzieży dóbr wirtualnych takich jak przedmioty czy punkty w grach*.

NAJCZĘSTRZE FORMY PRZESTĘPCZOŚCI INTERNETOWEJ:



Rządowy laptop dla IV klasy, gamingowy komputer i smartfon, to urządzenia wymagające **ochrony i konfiguracji**, bez względu na właściciela. Ważne, by ustawiać silne i unikatowe hasła logowania, zwłaszcza na urządzeniach mobilnych. Po stworzeniu hasła logowania, zadbaj o **hasła** w internetowych kontach – powinny być one **długie, pozbawione schematów oraz unikatowe** (patrz punkt 4.). Dane, hasła i konta internetowe są narażone na kradzież lub przejęcie kontroli z niezabezpieczonego i zalogowanego sprzętu. Pamiętaj też o nawyku **blokowania swojego urządzenia.**

PORADA 2.

WSPÓLNIE DBAJCIE O KONDYCJĘ SPRZĘTU ELEKTRONICZNEGO.

Mniej, niż połowa uczestników warsztatów o cyberbezpieczeństwie (43%) odpowiedziała prawidłowo na pytanie: co może ochronić ich przed Keyloggerem (prawidłowa odpowiedź: oprogramowanie antywirusowe)*.**

Hasło na komputerze i smartfonie to podstawa. Dla bezpieczeństwa dzieci, zainstaluj lub włącz **wbudowane oprogramowanie antywirusowe** oraz upewnij się, że włączone są **domyślne opcje zabezpieczeń** (np. zapora Microsoft Defender oraz kontrola aplikacji i przeglądarki – menu „zabezpieczenia Windows" dla systemów od Microsoftu).
Nie mniej ważne są **aktualizacje oprogramowania**, które zapewniają poprawki bezpieczeństwa. Dbaj zatem o regularną aktualizację komputera i smartfonu swojego oraz dziecka.

PORADA 3.

POMÓŻ DZIECKU STWORZYĆ WIELE TOŻSAMOŚCI ONLINE.

Jedynie 23% uczestników warsztatów Cyberbezpieczni rozpoznało wszystkie elementy wskazujące na wiadomość phishingową*.**

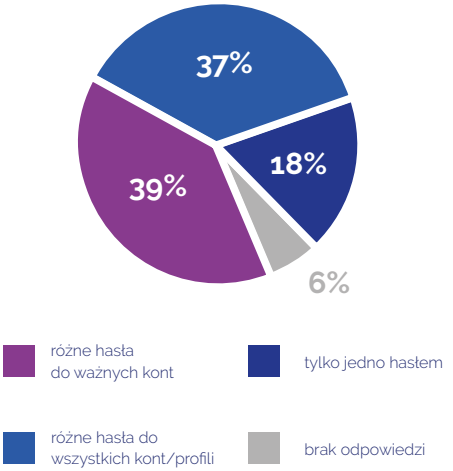
Adres mailowy JanKowalski@gmail.com to przykład profesjonalnie wyglądającego adresu, idealnego do wysyłania CV, ale młodzi wykorzystują internet na wiele sposobów, nie tylko do procesów rekrutacyjnych.

Dlatego **warto mieć kilka adresów** i, co za tym idzie, kilka tożsamości w sieci dla różnych działań. Zachęcaj swoje dziecko do tworzenia **oddzielnych adresów mailowych** do szkoły, do pracy, newsletterów oraz kontaktów z bliskimi. Dla zachowania bezpieczeństwa swojego dziecka, unikaj informacji osobistych w adresie, który dla niego tworzysz: „gruszka777@protonmail.com „ to dobry adres mailowy, który nie ujawnia nazwiska ani wieku. „Gruszka777" może również pełnić funkcję pseudonimu w grach oraz nazwy użytkownika na forach.

PORADA 4.

TWÓRZ SILNE HASŁA I ZABEZPIECZ KONTA INTERNETOWE.

39% badanych ma różne hasła do ważnych kont (np. bank, media społecznościowe czy platformy eCommerce), 37% ma różne hasła do wszystkich kont/profili, a 18% posługuje się w Internecie tylko jednym hasłem.**



W sieci mamy wiele kont – od maili po media społecznościowe. Ważne, by dzieci potrafiły tworzyć mocne, unikalne hasła. **Silne hasło to kombinacja liter, cyfr i znaków specjalnych**. Im dłuższa kombinacja znaków, tym ochrona konta jest lepsza! Hasło powinno być długie (minimum 14 znaków, np. w formie abstrakcyjnej frazy lub zdania), pozbawione schematów (np. nazw miesięcy lub szlaczków typu „qwerty" na klawiaturze) oraz unikatowe (inne do każdego serwisu). Ostatni warunek jest szczególnie trudny, ale może pomóc nam w nim menedżer haseł – program służący tworzeniu i przechowywaniu silnych haseł w „wirtualnym sejfie" chronionym hasłem głównym.

Równie ważnym elementem, co silne hasło i menedżer haseł, jest **uwierzytelnianie dwuskładnikowe** chroniące nasze konta w przypadku wycieku hasła do sieci. Uwierzytelnianie dwuskładnikowe może mieć formę klucza U2F czy potwierdzeń i kodów w aplikacji typu authenticator. Są to podstawowe i najważniejsze kroki zwiększające bezpieczeństwo naszych kont i danych w sieci! Jeśli któreś z tych narzędzi i programów jest dla Ciebie nowe, pamiętaj o zerknięciu do **PORADY 10!**

PORADA 5.

OKREŚL WIEK, W KTÓRYM ROZPOCZYNACIE KORZYSTANIE Z URZĄDZEŃ EKRANOWYCH I INTERNETU.

Średnia wieku inicjacji internetowej dla szkół podstawowych, według deklaracji uczniów, wynosi: 6 lat i 8 miesięcy*.

Większość popularnych aplikacji takich, jak Google, Facebook, TikTok, Instagram i innych jest przeznaczona dla 13-latków i starszej młodzieży. Przy wprowadzaniu dziecka do świata cyfrowego, ustaw jego wiek w sposób przemyślany. Konta dla użytkowników od 13-stego do 18-stego roku życia, mają inne ustawienia ochrony prywatności – domyślnie chronią one

użytkownika ograniczając wiadomości od nieznajomych, udostępnianie treści i streaming. Unikaj zatem sytuacji, w których Twoje dziecko otrzymuje konto niedostosowane do jego wieku i potrzeb.

PORADA 6.

OKREŚL ZASADY ZWIĄZANE Z UŻYCIEM URZĄDZEŃ EKRANOWYCH I INTERNETU.

Zaledwie 8,7% nastolatków uważa, że rodzice stosują systemy kontroli ryzykownych treści w Internecie. Większość (69,0%) twierdzi, że w ich domu/mieszkaniu nie jest zainstalowany filtr rodzinny, ani inna technologia ograniczająca dostęp do niebezpiecznych treści w Internecie*.

Nastolatki deklarują najczęściej, że w ich domach nie wprowadza się zasad ograniczających czas korzystania z Internetu czy reguł dotyczących selekcji treści **(39,9%)***.

Aplikacje do „kontroli rodzicielskiej" – ta nazwa może brzmieć strasznie, ale są to bardzo praktyczne i pomocne narzędzia do egzekwowania ustalonych z dzieckiem zasad korzystania z urządzeń ekranowych i Internetu. Dlaczego warto z nich korzystać? Można w nich ustawić ograniczony czas ekranowy, określić dozwolone aplikacje i filmy oraz ustawić przedział wiekowy ograniczający treści dla osób pełnoletnich. Pozwolą również na zlokalizowanie danego urządzenia i użytkownika, czyniąc Twoje dziecko bezpieczniejszym również w świecie offline. Pamiętaj jednak, że dzieci i młodzież potrafią być niezwykle kreatywne w obchodzeniu różnego rodzaju ograniczeń – mogą mieć inne telefony, karty SIM lub wchodzić do sieci za pośrednictwem telewizorów, konsol do gier czy smartwatchy. Wprowadzone przez Ciebie zasady powinny zatem uwzględniać wszystkie sprzęty, ale również szersze zasady i reguły, ustalone z dzieckiem w ramach wspólnego kontraktu.

Kontrakt i kontrola rodzicielska powinny być bowiem narzędziami budowy samodzielnej i długotrwałej motywacji dziecka do korzystania z urządzeń ekranowych i Internetu w sposób bezpieczny i zrównoważony.

PORADA 7.

POZWALAJĄC KORZYSTAĆ Z MEDIÓW SPOŁECZNOŚCIOWYCH, NIE POZWÓL, BY MEDIA WYKORZYSTAŁY CIEBIE I TWOJE DZIECKO.

Dzielenie się zdjęciami, filmami czy informacjami osobistymi w mediach społecznościowych jest przez uczniów oceniane jako zagrożenie dla prywatności rzadziej niż przez ich rodziców i opiekunów (nastolatki – 40,3% vs. rodzice – 69,5%). Jedynie co dwunasty (8,5%) nastolatek dostrzega zagrożenie w przyjmowaniu zaproszeń od osób nieznajomych, a 14% młodych respondentów przyznało, że spotkało się na żywo z osobą dorosłą poznaną w Internecie*.

Media społecznościowe są popularnym miejscem interakcji w Internecie, ale mogą też być źródłem zagrożeń. Zakładając nowe konto w wybranym serwisie, znajdźmy i zajrzyjmy do zakładki "Prywatność". W tym rzadko odwiedzanym przez młodych i rodziców miejscu, kryją się liczne ustawienia pomagające chronić prywatność naszych podopiecznych. Omówmy z młodymi i wprowadźmy podstawowe za-

sady bezpieczeństwa. Zachęćmy nasze dzieci i młodzież do **komunikacji w sieci w sposób odpowiedzialny i bezpieczny.** Wspólnie ustalmy zasady bezpiecznej komunikacji z nieznajomymi poznanymi w Internecie. Rozmawiajmy z nimi na temat potencjalnych zagrożeń, które mogą pojawić się podczas rozmów internetowych, takich jak nękanie, wyłudzanie poufnych informacji czy podszywanie się pod kogoś innego. Wyraźnie mówmy o tym, że nie każda osoba widoczna na zdjęciu profilowym lub wysłanym w wiadomości, okazuje się tą samą osobą w świecie realnym.

PORADA 8.

POROZMAWIAJ O HEJCIE I MOWIE NIENAWIŚCI. BĄDŹ TYM, KOMU TWOJE DZIECKO MOŻE POWIEDZIEĆ O TYM, CO JE SPOTYKA W INTERNECIE

Co piąty nastolatek przyznaje, że doświadczył przemocy w Internecie. Najczęstszymi jej przejawami są: wyzywanie (29,7%), ośmieszanie (22,8%) czy poniżanie (22%). Jedynie co czwarty nastolatek (24,1%) szuka wsparcia u rodziców i opiekunów w sytuacji doświadczania przemocy w sieci. Częściej deklarowany jest brak reakcji (32,4%) oraz szukanie pomocy u przyjaciół i znajomych (31,9%)*.

Warto porozmawiać z młodymi lub poprosić nauczycieli o organizację odpowiednich zajęć w szkole w temacie hejtu i mowy nienawiści w sieci. Bądźmy gotowi służyć wsparciem i radą w przypadku trudnych sytuacji online. Sami cały czas poszerzajmy swoja wiedzę na temat się cyberbezpieczeństwa, aby móc rzetelnie odpowiadać na pytania dzieci.

W sytuacji, gdy ogromna ilość internautów staje się ofiarami mowy nienawiści w sieci, warto mieć świadomość jak reagować i przeciwdziałać hejtowi w sieci.

CO PIĄTY NASTOLATEK PRZYZNAJE, ŻE DOŚWIADCZYŁ PRZEMOCY W INTERNECIE

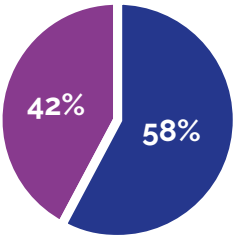
PORADA 9.

POZNAJ LEPIEJ ŚWIAT GIER KOMPUTEROWYCH I MOBILNYCH

W Internecie, dzieci i młodzież najwięcej czasu poświęcają na rozmowy ze znajomymi oraz rodziną za pomocą komunikatorów czy czatów (58% ankietowanych). Druga grupa aktywności to gry online (42%).**

Gra w gry komputerowe i korzystanie z aplikacji rozrywkowych, to częsty sposób spędzania czasu przez dzieci. Jako rodzice, możemy pomóc im zrozumieć znaczenie odpowiedzialnego korzystania z tych usług. Wspólnie ustalmy limity czasu spędzanego przed ekranem, aby zapewnić równowagę między światem wirtualnym, a realnym.

Zwróćmy uwagę na gry mobilne w modelu Pay-To-Win, namawiające do ciągłych zakupów i wydawania pieniędzy. Jeśli dziecko wykorzystuje nasz telefon do gier, koniecznie pamiętajmy o ustawieniu dodatkowego uwierzytelnienia płatności (przy pomocy odcisku kciuka lub hasła). Pozwoli to wyznaczyć młodym osobom granice oraz uchroni nas przed rachunkiem-niespodzianką!



gry online

rozmowy

Rzetelne oceny gier i aplikacji mogą pomóc uniknąć treści nieodpowiednich dla wieku naszych dzieci, a odpowiednie skonfigurowanie kontroli rodzicielskiej uniemożliwi instalację gier bez akceptacji rodzica. Zwróćmy także uwagę na to, z kim nasze dzieci komunikują się w grach online i jak reagują na sytuacje niebezpieczne (hejt i mowa nienawiści). Wreszcie, porozmawiajmy z naszymi podopiecznymi o tym, w co i dlaczego grają. Świat gier, to świat pełen wspaniałych bohaterów, porywających historii, błyskotliwych strategii i wielu wartości edukacyjnych. Warto się w niego zagłębić, pamiętając o bezpieczeństwie o zachowaniu umiaru.

PORADA 10.

ZDOBYWAJ NOWE INFORMACJE

Tylko 7% dzieci i młodzieży zawsze weryfikuje informacje znalezione w sieci, 57% robi to czasami, a 31% w ogóle tego nie robi.**

Zagrożenia w sieci zmieniają się i ewoluują bardzo szybko. W Internecie codziennie pojawiają się nowe próbki złośliwego oprogramowania, nienawistne komentarze czy fałszywe informacje. Aby dbać o bezpieczeństwo swoje i swoich bliskich, warto śledzić instytucjei organizacje dbające o bezpieczeństwo w Internecie takie jak NASK, Niebezpiecznik, Fundacja Szkoła z Klasą, Cyfrowy Dialog, Fundacja Cyber czy Demagog.

Można również zapisać klasę swojego dziecka do udziału w bezpłatnych warsztatach, w ramach naszego programu edukacyjnego Cyberbezpieczni oraz zachęcić młodzież do udziału w ogólnopolskim teście bezpieczeństwa w sieci.

Wszystkich rodziców zapraszamy na bezpłatny webinar prowadzony przez Niebezpiecznik.pl, uzupełniający poniższą broszurę o jeszcze większą dawkę wiedzy i umiejętności. Bezpieczny Internet to przestrzeń, którą musimy tworzyć wspólnie!

WIĘCEJ O PROJEKCIE:
HTTPS://FUNDACJAPFR.PL/CYBERBEZPIECZNI.HTML

* Lange, R., et al., Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów., NASK, Warszawa (2021): https://thinkstat.pl/publikacje/nastolatki-3-0-raport-z-ogolnopolskiego-badania-uczniow-2021-r ** badania EY Polska „Ostrożni w Sieci": https://www.ey.com/pl_pl/ostrozni-w-sieci *** wyniki pretestów realizowanych w ramach programu Cyberbezpieczni w 2022 na grupie ponad 200 uczestników projektu w wieku od 10 do 18 lat (próba niereprezentatywna).

CYBER
BEZPIECZNI

Projekt edukacyjny dla uczniów i nauczycieli

Cyberbezpieczni to ogólnopolski program rozwoju kompetencji uczniów i nauczycieli realizowany przez zespół edukacyjny Centralnego Domu Technologii i Fundację Polskiego Funduszu Rozwoju. Projekt ma na celu promowanie wiedzy z zakresu bezpieczeństwa w sieci. W efekcie działań edukacyjnych już ponad 11 tysięcy osób – uczniów, nauczycieli i rodziców – miało szansę dowiedzieć się, jak być bezpiecznym w sieci i jak rozpoznawać nieprawdziwe treści publikowane w Internecie. Materiały edukacyjne stworzone w ramach projektu są udostępnione bezpłatnie na kanałach YouTube CDT oraz na stronie **www.cdt.pl**

WIĘCEJ INFORMACJI O PROJEKCIE ZNAJDUJE SIĘ NA STRONIE:

HTTPS://FUNDACJAPFR.PL/CYBERBEZPIECZNI.HTML

Projekt jest finansowany ze środków Kancelarii Prezesa Rady Ministrów w ramach ogólnopolskiego programu rozwoju kompetencji uczniów i nauczycieli „Cyberbezpiecznai".

Centralny Dom Technologii

PFR Fundacja