Bezpieczne media

poradnik dla rodziców

Spis treści

Wstęp

Oddajemy w Państwa ręce poradnik poświęcony bezpieczeństwu dzieci i młodzieży korzystających z mediów elektronicznych. Znajdą w nim Państwo m.in. informacje dotyczące zabezpieczeń technicznych, które warto wykorzystać oddając w ręce dziecka komputer, telefon lub tablet. Jesteśmy jednak przekonani, że wszelkie programy opieki rodzicielskiej, filtry i oprogramowanie antywirusowe to jedynie niezbędne minimum i dobry początek, a wyrazem prawdziwej troski o bezpieczeństwo dzieci w internecie jest ich edukacja i wychowanie. Wierzymy również, że tak jak i w realnym świecie, to zadaniem rodzica jest bezpieczne wprowadzenie dziecka w świat nowoczesnych mediów. Dlatego też dużą część tej broszury poświęciliśmy na porady dotyczące tego, jak razem z dzieckiem odkrywać świat gier, portali społecznościowych, transakcji online i całego bogactwa informacji, jakie oferuje światowa sieć.

Fundacja Dajemy Dzieciom Siłę oraz Fundacja Orange już od kilkunastu lat wspólnie działają na rzecz bezpieczeństwa młodych internautów. Chcemy, by świat nowoczesnych mediów był przyjazny dla dzieci i młodzieży. Po to, by w pełni mogły wykorzystać jego potencjał. Jesteśmy przekonani, że najlepszą ku temu drogą jest właśnie edukacja. W tak dynamicznie zmieniającym się środowisku, w którym z dnia na dzień pojawiają się nowe usługi, nowe serwisy, a więc i nowe zagrożenia, jedynym sposobem na ich uniknięcie lub zminimalizowanie ich skutków jest wiedza, najlepiej – jak najbardziej aktualna. Śledzimy dynamiczne zmiany cyfrowego świata, reagujemy na pojawiające się w nim trendy, staramy się działać kompleksowo, przygotowując nasze materiały z myślą zarówno o dzieciach i młodzieży, przedszkolach i szkołach, jak i rodzicach, których roli w kształtowaniu właściwych postaw dziecka, również w cyfrowym świecie, nie sposób przecenić.

Mamy nadzieję, że we wspólnym, razem z dzieckiem, odkrywaniu świata nowoczesnych technologii pomoże Państwu ten poradnik.

Fundacja Dajemy Dzieciom Siłę i Fundacja Orange

To tylko statystyka, ale...

To tylko statystyka. Na pewno nie odzwierciedla w pełni tego, jak z sieci korzysta twoje dziecko. Ale opisuje ogólne trendy, a dzięki wynikom badań łatwiej zrozumieć perspektywę dziecka, presję otoczenia, pod jaką się znajduje i wybory, z jakimi ma do czynienia.

Dla dziecka internet znaczy więcej

O ile dla osoby dorosłej sieć jest źródłem informacji lub narzędziem pracy, o tyle dla dziecka ma ona dużo większe znaczenie. Oprócz dostarczania wiedzy i rozrywki internet jest dla dziecka miejscem, w którym rozgrywa się poważna część jego życia społecznego i towarzyskiego, gdzie kreuje swój wizerunek i obserwuje innych. Treści i osoby popularne w sieci („youtuberzy" – osoby publikujące filmy w serwisie YouTube, „szafiarki" – autorki blogów nt. mody) w coraz większym stopniu modelują postawy i zachowania dzieci. Ważne, żeby dorośli zdawali sobie sprawę z popularności internetowych trendów, błyskawicznie rozpowszechniających się np. w serwisach społecznościowych i treści, do jakich ich dzieci mają dostęp.

Nie należy jednak wierzyć w mit, że dzieci od urodzenia otoczone tabletami, smartfonami, konsolami do gier i laptopami naturalnie stają się komputerowymi ekspertami i same doskonale radzą sobie w sieci. Nawet jeśli potrafią modyfikować zaawansowane ustawienia aplikacji, nie oznacza to, że w równie naturalny sposób opanowały techniczne i społeczne aspekty bezpieczeństwa online. Warto pamiętać, że nawet jeśli dziecko spędza dużo czasu w internecie, nie zawsze wie, ani jak się zachować w potencjalnie zagrażającej sytuacji, ani co zrobić, gdy natknie się na problem. Ogranicza je w tym m.in. niedojrzałość psychospołeczna, niezdolność do dostrzegania odległych konsekwencji swoich działań. Zadaniem dorosłych jest bezpieczne wprowadzenie dziecka w ten świat.

WAŻNE!

Nie przeceniaj wiedzy swojego dziecka i jego umiejętności technicznych, a tym bardziej umiejętności dostrzeżenia niebezpiecznych sytuacji i poradzenia sobie z problemami. Jako dorosły jesteś odpowiedzialny za jego bezpieczeństwo w internecie, zadbaj o to, by wiedziało, że może się do ciebie zwrócić z problemami.

Nie tylko w domu

Internet w Polsce rzeczywiście trafił pod strzechy – według danych GUS w 2016 roku już 80 proc. gospodarstw domowych miało dostęp do sieci, a tam, gdzie są dzieci, wskaźnik ten wzrasta aż do 98 proc. Wśród dzieci i młodzieży w wieku szkolnym praktycznie nie ma osób niekorzystających z internetu. Już w 2010 roku (badania *EU Kids Online*) 98 proc. dzieci w wieku 9-16 lat deklarowało, że korzysta z internetu przynajmniej raz w tygodniu. A według europejskiego raportu *Zero to Eight: Young children and their internet use* z 2013 roku, z sieci korzysta już ponad połowa dzieci w wieku przedszkolnym.

Najnowsze dane dotyczące polskich dzieci w wieku 10-18 lat pochodzą z badania *Bezpieczeństwo dzieci w internecie,* zrealizowanego w 2016 roku na zlecenie Orange Polska przy współpracy Fundacji Orange i Fundacji Dajemy Dzieciom Siłę. Wszystkie dzieci biorące udział w badaniu miały dostęp do sieci w domu, 55 proc. z nich korzystało z internetu w szkole, a 25 proc. u znajomych. 26 proc. badanych zadeklarowało korzystanie z internetu cały czas i wszędzie, dzięki dostępowi do sieci przy użyciu telefonu i korzystaniu z pakietów internetowych.

Chociaż komputer pozostaje najpopularniejszym urządzeniem, dzięki któremu dzieci korzystają z internetu, coraz więcej młodych osób korzysta z sieci używając telefonów – wykorzystuje je aż 68 proc. dzieci w wieku 10-18 lat. 40 proc. dzieci do przeglądania sieci używa także tabletów.

Większość dzieci w ciągu tygodnia korzysta z internetu (posługując się różnymi urządzeniami: komputerem stacjonarnym, laptopem, tabletem, smartfonem) najczęściej od godziny do dwóch dziennie. Tylko 13 proc. przekracza 4 godziny dziennie. W weekendy i dni wolne od zajęć ponad dwie godziny dziennie online jest już 53 proc. dzieci.

Już w 2012 roku polskie dzieci znalazły się w czołówce użytkowników telefonów komórkowych. Według badania firmy The Marketing Store przeprowadzonego w 12 krajach, to Polska odnotowała wówczas najwyższy odsetek 10-latków deklarujących posiadanie własnego telefonu komórkowego (83 proc.). Na kolejnych pozycjach znalazły się: Wielka Brytania (73 proc.), Brazylia (73 proc.) i Niemcy (69 proc.).

WAŻNE!

Dzieci coraz częściej korzystają z internetu używając innych urządzeń niż domowy komputer. Warto więc rozważyć uruchomienie blokady niebezpiecznych treści w telefonie dziecka.
W przypadku komputera i używanego przez dziecko tabletu, uruchomiony na stałe filtr *SafeSearch* wyszukiwarki Google pozwala ograniczyć dostęp do treści przeznaczonych wyłącznie dla dorosłych.

Najpopularniejsze serwisy

Google, Facebook i YouTube – te serwisy niepodzielnie rządzą w światowym internecie. Zajmują najwyższe pozycje wśród stron odwiedzanych zarówno przez dorosłych, jak i przez dzieci. Ale już kolejne pozycje tego rankingu (ustalonego na podstawie realnego zachowania internautów, a nie ich deklaracji, źródło: Megapanel PBI) różnią się w zależności od wieku:

Odsetek internautów, którzy odwiedzili daną stronę		
serwis	**7-14 lat**	**15-24 lata**
Google	94%	98%
YouTube	88%	85%
Facebook	77%	88%
Onet	57%	70%
Allegro	47%	69%

Aż 88% internautów w wieku 7-14 lat odwiedzało YouTube – serwis wideo, w którym od przeznaczonych dla dzieci kreskówek łatwo przejść do materiałów zupełnie dla nich nieodpowiednich. Na kolejnym miejscu znalazł się Facebook. Według regulaminu tego serwisu korzystać mogą z niego osoby powyżej 13. roku życia, jednakże ze względu na nieproporcjonalnie duży odsetek użytkowników Facebooka w grupie 7-14 lat należy przypuszczać, że wiele dzieci musiało podawać nieprawdziwy wiek, by zarejestrować się na FB. Warto zauważyć również popularność wśród dzieci serwisu zakupowego Allegro, co może być źródłem dodatkowych zagrożeń związanych z transakcjami w sieci.

Najpopularniejszą wśród dzieci i młodzieży formą aktywności w sieci są komunikatory i serwisy społecznościowe (obydwie usługi są coraz bardziej zintegrowane). Korzysta z nich

4 na 5 internautów z tych grup wiekowych. Bardzo popularne jest także oglądanie filmów i wideoklipów online – na YouTube zagląda aż 84 proc. młodych internautów. Co ciekawe, z popularnej wśród dorosłych poczty elektronicznej korzysta tylko 61 proc. nastolatków, jeszcze mniej – z portali szkolnych i serwisów z wiedzą naukową (odpowiednio 58 i 54 proc. nastolatków).

WAŻNE!

Twoje wyobrażenia o tym, co dziecko robi w internecie, mogą mijać się z rzeczywistością. Postaraj się znaleźć wspólne tematy, interesujące zarówno ciebie, jak i twoje dziecko. Wspólne korzystanie z internetu to również okazja do budowania bliskości.

Co zagraża dziecku?

Dzieci i młodzież intensywnie korzystają z sieci i możliwości, jakie oferuje. Pamiętajmy jednak, że wciąż są dziećmi – nie zawsze potrafią właściwie ocenić zagrożenia i się przed nimi obronić.

Jedną z metod usystematyzowania niebezpieczeństw, które mogą dotyczyć dzieci, jest typologia nazywana 5C, od anglojęzycznych określeń zagrożeń:

1. **Content:** niebezpieczne treści, na jakie dzieci i młodzież mogą natrafić w internecie.
2. **Conduct:** niebezpieczne zachowania, w jakie mogą się angażować młodzi ludzie w internecie.
3. **Contact:** niebezpieczne kontakty, jakie dzieci i młodzież mogą nawiązać w sieci.
4. **Confidentiality:** naruszenie prywatności i danych osobowych.
5. **Commercialisation:** zagrożenia związane z aktywnością komercyjną firm online.

Content – niebezpieczne treści

Młodzi internauci mogą się zetknąć w sieci z materiałami, które są dla nich nieodpowiednie – przeznaczone wyłącznie dla dorosłych lub wręcz nielegalne. Przede wszystkim dotyczy to pornografii. Do treści szkodliwych należą także m.in.: materiały rasistowskie i ksenofobiczne, strony zachęcające do zachowań autodestrukcyjnych: zażywania narkotyków, skrajnego odchudzania, samookaleczeń i samobójstwa. Do materiałów nieodpowiednich dla dzieci i młodzieży zalicza się również serwisy i strony związane z hazardem. Treści uznawane za nieodpowiednie dla młodych ludzi są w internecie bardzo rozpowszechnione – kontakt z nimi miało łącznie 54 proc. gimnazjalistów.

Odsetek młodzieży w wieku 14-17 lat deklarującej kontakt z treściami niebezpiecznymi w internecie	
Pornografia	67%
Przekazy rasistowskie i pełne nienawiści	40%
Skrajne odchudzanie	28%
Informacje promujące zażywanie narkotyków	24%
Samookaleczanie się	22%
Popełnienie samobójstwa	15%
Hazard	6%

Źródło: EU-NET-ADB

Conduct – niebezpieczne zachowania
Kategoria ta obejmuje różne zjawiska, najważniejsze z nich to: cyberprzemoc, seksting oraz nadużywanie internetu lub uzależnienie od niego.

- Cyberprzemoc – to przemoc psychiczna z wykorzystaniem internetu i telefonu. Może przyjmować bardzo różne formy: od obraźliwych SMS-ów, złośliwych komentarzy w serwisach społecznościowch, poprzez publikację w sieci zdjęć ukazujących konkretną osobę w niekorzystnym świetle, aż po tworzenie specjalnych, szykanujących stron lub profili. Cyberprzemoc często jest związana z tradycyjną przemocą rówieśniczą, zarówno fizyczną, jak i psychiczną. Według badań EU-NET-ADB, ofiarą cyberprzemocy padło w Polsce 22 proc. gimnazjalistów.
- Seksting – termin ten powstał z połączenia angielskich słów „sex" i „texting" (sms-owanie, czatowanie). Polega na przesyłaniu osobistych zdjęć i filmów o charakterze seksualnym za pośrednictwem telefonu komórkowego (MMS) lub sieci (pocztą elektroniczną, poprzez komunikatory internetowe, pozowanie nago przed kamerą online). Odbywa się to często pomiędzy osobami, które są w relacji intymnej lub dopiero chcą zwrócić na siebie uwagę drugiej osoby. Przeprowadzone w 2014 r. badania Fundacji Dajemy Dzieciom Siłę pokazały, że w Polsce 33 proc. młodych ludzi w wieku 15-19 lat otrzymywało tego typu wiadomości, zaś 11 proc. przyznało się do ich wysyłania.
- Nadużywanie internetu – chociaż zjawisko to nie zostało jeszcze do końca rozpoznane przez psychologów i psychiatrów, na pewno można o nim mówić, gdy korzystanie z internetu wymyka się użytkownikowi spod kontroli i wpływa negatywnie na inne aspekty jego życia. Badania wykazały, że problem ten dotyczy w znacznym stopniu 1,3 proc. gimnazjalistów, a w grupie osób zagrożonych (u których stwierdza się część symptomów) znalazło się 12 proc. gimnazjalistów. Chociaż wydawać się może, że problem ten dotyka stosunkowo wąskiej grupy młodzieży, często są to sytuacje bardzo poważne. Wraz ze wzrostem zarówno skali, jak i świadomości problemu, coraz więcej instytucji oferuje profesjonalną diagnozę i pomoc.

Contact – niebezpieczne kontakty
Fakt, że w kontakcie wyłącznie online łatwo zafałszować swoją prawdziwą tożsamość, stwarza ryzyko, że z dziećmi mogą się kontaktować osoby o niekoniecznie uczciwych zamiarach. Kontakty z osobami znanymi wyłącznie z internetu są powszechne wśród gimnazjalistów – aż 69 proc. z nich poznało przez internet kogoś, kogo nie znało wcześniej, a aż 31 proc. spotkało się na żywo z kimś, kogo poznało po raz pierwszy w internecie.

Confidentiality – naruszenie prywatności
Do sieci trafia coraz więcej prywatnych informacji o użytkownikach – w przypadku dzieci dotyczy to zarówno danych osobowych (miejsce zamieszkania, wiek, szkoła), jak również zdjęć, które nie powinny być dostępne publicznie. Zagrożeniem są również usługi geolokalizacyjne. Nierzadkie są także przypadki, w których dzieci udostępniają znajomym bądź nawet nieznanym sobie osobom hasła do serwisów online. W badaniach *EU Kids Online*, 7 proc. polskich nastolatków w wieku 11-16 lat zadeklarowało, że doświadczyło naruszenia swojej prywatności.

Commercialisation – zagrożenia związane z działalnością komercyjną
Dzieci i młodzież często postrzegają internet jako źródło darmowych w większości usług, nie rozumiejąc modelu biznesowego przyjętego przez firmy, chcące zarabiać także na młodych użytkownikach. Młodsze dzieci często mają problem z rozróżnieniem informacji od reklamy, zagrożeniem może być również wyłudzanie danych osobowych (wykorzystywanych później marketingowo), np. pod pozorem udziału w konkursie. Problemem są także ukryte bądź odroczone opłaty za usługi i aplikacje online. Na przykład w przypadku gier *freemium* (ich używanie jest zasadniczo bezpłatne, płacić trzeba za dodatkowe funkcje lub kolejne etapy) opłaty te mogą być pobierane w systemie *in-app purchases* – dzięki zapisaniu w urządzeniu danych karty kredytowej dziecko może dokonywać opłat, nie mając świadomości wydawania pieniędzy rodzica.

WAŻNE!

Nie warto demonizować internetu, upatrując w nim siedliska wszelkiego zła. Jednocześnie warto świadomie podchodzić do internetowych zagrożeń. Przyjęcie założenia „mojego dziecka to nie dotyczy" może się okazać złudne.

Mowa nienawiści

Powszechnym problemem internetu jest tzw. **mowa nienawiści** (język nienawiści). To – według definicji Rady Europy – „wszelkie formy wypowiedzi, które szerzą, propagują czy usprawiedliwiają nienawiść rasową, ksenofobię, antysemityzm oraz inne formy nienawiści bazujące na nietolerancji". Pozory anonimowości jakie daje internet sprzyjają radykalnym opiniom i powodują, że mowa nienawiści często pojawia się w komentarzach i opiniach na temat innych osób i grup społecznych. Zwróć uwagę dziecka na język, jakim się posługuje w internecie, naucz je szanować innych ludzi,

przekonaj je, by nie publikowało treści, których nie potrafiłoby powiedzieć drugiej osobie twarzą w twarz.

Problemem mowy nienawiści zajmuje się **Koalicja Przeciwko Mowie Nienawiści**, wspierana przez firmę Orange. To nieformalne zrzeszenie organizacji, instytucji i osób, którym bliska jest problematyka praw człowieka w internecie.

Więcej informacji: beznienawisci.pl

Darknet

Oprócz ogólnodostępnego, „zwykłego" internetu funkcjonuje tzw. Darknet, swoiste „podziemie" sieci. Do Darknetu nie trafia się przypadkiem, jego zawartość nie jest indeksowana przez zwykłe wyszukiwarki, korzystanie z niego wymaga właściwego oprogramowania obsługującego sieć TOR (ang. *The Onion Router*), wykorzystującą „trasowanie cebulowe", pozwalające na ukrycie lokalizacji użytkownika i ograniczające możliwość śledzenia zaszyfrowanych pakietów danych. Instalacja i konfiguracja oprogramowania niezbędnego do korzystania z Darknetu leży w zasięgu możliwości zdeterminowanego nastolatka. Istotą Darknetu jest anonimowość – zarówno osób zamieszczających treści, jak i je wykorzystujących. Swobodny przepływ informacji to z jednej strony zaleta – materiały umieszczone w Darknecie nie są objęte kontrolą ani rządów, ani dostawców internetu. Jednocześnie powszechność nielegalnych i szkodliwych treści (przemoc, agresja, pornografia dziecięca), łatwy dostęp do nielegalnych towarów (broń palna, narkotyki) stanowią dla młodych internautów poważne zagrożenie. Cechą charakterystyczną Darknetu są strony internetowe, których adres jest zakończony domeną .onion. Jeśli dostrzeżemy, że nastolatek z nich korzysta, będzie to dobra okazja do rozmowy z nim o odpowiedzialności w internecie.

Ochrona prawna

Anonimowość online jest jedynie pozorem. W większości przypadków policja jest w stanie ustalić kto stoi za nielegalnymi działaniami. To ważna informacja zarówno dla potencjalnych sprawców, ale i ofiar przemocy lub przestępstw w sieci. Ofiara przemocy lub przestępstwa w sieci ma prawo oczekiwać skutecznej ochrony w oparciu o obowiązujące przepisy.

W przypadku przemocy rówieśniczej w sieci, prawa ofiar chronią: art. 216 kk (znieważenie), art. 212 kk (zniesławienie), art. 267 i 268a kk (włamanie), art. 190 i 191 kk (groźby), art. 190a kk (nękanie), art. 23 i 24 kc (naruszenie wizerunku dziecka). Kwestie mowy nienawiści regulują art. 257 kk (znieważanie na tle rasowym, wyznaniowym, etnicznym), oraz 256 kk (propagowanie faszyzmu, totalitaryzmu, nawoływanie do nienawiści), jak i wspomniane wcześniej art. 212 i 216 kk. Osoby zaangażowane w sekstyng mogą w określonych przypadkach podlegać przepisom prawa regulującym kwestie produkowania, prezentowania lub rozpowszechniania pornografii dziecięcej (art. 202 kk). Konsekwencje prawne grożą również za dosyć powszechne wśród młodych ludzi wykorzystywanie cudzej własności intelektualnej, choćby w formie plagiatów prac szkolnych lub ściąganie plików (programów, filmów, muzyki) z nielegalnych źródeł (art. 78, 79, 115 Ustawy o prawach autorskich).

Naucz dziecko bezpieczeństwa

Kiedy udostępnić dziecku internet, telefon, laptop, tablet?

Po tablet lub smartfon sięgają coraz młodsze dzieci. Zadecydowała o tym wygoda posługiwania się urządzeniami z ekranami dotykowymi, bardziej poręcznymi dla maluchów niż myszka i klawiatura. Ze smartfona lub tabletu korzysta ponad 80 proc. dzieci w wieku przedszkolnym. Wśród dzieci rocznych i dwuletnich odsetek ten przekracza 40 proc. Niemal co trzecie dziecko w tym wieku korzysta z urządzeń mobilnych codziennie lub prawie codziennie, 13 proc. dzieci w tym wieku ma już własny tablet lub smartfon (Badanie Millward Brown Poland dla FDN, 2015).

Według rekomendacji Fundacji Dajemy Dzieciom Siłę, dzieciom do drugiego roku życia nie zaleca się kontaktu z tabletami i smartfonami.

W przypadku dzieci w wieku od 3 do 6 lat udostępnianie im urządzeń dotykowych powinno być decyzją przemyślaną i obwarowaną szeregiem zasad. Najważniejsze z nich to:

- Należy zapewnić dzieciom dostęp jedynie do bezpiecznych i pożytecznych treści, dostosowanych do ich wieku, za pośrednictwem odpowiednio zabezpieczonych urządzeń (oprogramowanie antywirusowe i aplikacje kontroli rodzicielskiej).
- Dzieci nie powinny korzystać z urządzeń mobilnych codziennie. Dobrym pomysłem jest ustalenie dnia lub dni (np. weekendu) bez tabletu/smartfonu.

- Warto, żeby jednorazowo dzieci nie korzystały z urządzeń mobilnych dłużej niż 15-20 minut.
- Dzienny kontakt dzieci z wszelkimi urządzeniami ekranowymi nie powinien przekraczać 30 minut w przypadku dzieci młodszych, a 2 godzin w przypadku dzieci starszych.
- Rodzice powinni towarzyszyć dzieciom w korzystaniu z urządzeń mobilnych, tłumaczyć im to, co widzą na ekranie, wykorzystywać czas spędzony przed ekranem do budowania relacji z dziećmi.
- Nie należy udostępniać urządzeń mobilnych dzieciom przed snem. Korzystanie wtedy z tabletu/smartfonu przyczynia się do problemów z zasypianiem i wpływa na jakość snu dziecka.
- Nie należy traktować urządzeń mobilnych jako nagrody, a zakazu ich używania jako kary. Podnosi to w oczach dzieci atrakcyjność tych urządzeń i wzmacnia przywiązanie do nich.
- Nie należy również używać urządzeń mobilnych do motywowania dziecka np. do jedzenia, treningu czystości.

WAŻNE!

To rodzic decyduje, kiedy przekazać dziecku pierwszy telefon komórkowy lub tablet. Sam musisz rozstrzygnąć, czy to już właściwy moment. Upewnij się, że dziecko rozumie podstawowe zasady korzystania z telefonu, ale wcześniej – jasno je określ. Upewnij się, że dziecko nie widzi w telefonie przede wszystkim zabawki, która będzie je np. rozpraszała w szkole.

Porozmawiaj z dzieckiem

Pokolenie obecnych dzieci i nastolatków jest pierwszym, dla którego internet „był od zawsze" – urodzili się w czasie, kiedy dostęp do sieci był już rozpowszechniony. Pomimo rozwoju zabezpieczeń technicznych, wiele problemów związanych z bezpieczeństwem w internecie wciąż pozostaje nierozwiązanych. Dzieci nadal są narażone na kontakt z niebezpiecznymi treściami, próby uwodzenia, przemoc rówieśniczą. Co więcej – nowe technologie, nowe serwisy, nowe usługi tworzą nowe zagrożenia. Dlatego zabezpieczenia techniczne mogą być jedynie wsparciem dla rodziców i nigdy nie zastąpią ich uwagi lub rozsądku. Dziecko, a z czasem nastolatek, chce być coraz bardziej niezależne, niechętnie poddaje się kontroli rodziców. Jedynym sposobem by potrafiło samodzielnie poradzić sobie z problemami w sieci, jest jego edukacja. To rolą rodziców jest nauczenie dziecka jak bezpiecznie poruszać się w sieci – tak, jak i nauczenie bezpiecznego przechodzenia przez ulicę. Nikt nie jest w stanie przewidzieć, na co i na kogo dziecko natrafi w internecie. Warto więc uczyć je samodzielności i zadbać, by wiedziało, jak unikać internetowych zagrożeń, a przede wszystkim – przekonać je, że zawsze może się do ciebie zwrócić w przypadku problemów.

WAŻNE!

Nie musisz być ekspertem w zakresie nowych technologii lub bezpieczeństwa sieciowego. Zasady, które powinno poznać dziecko są uniwersalne, dotyczą zarówno tego, co dzieje się w internecie, ale i tego, na co natrafiamy w codziennym życiu. Powinieneś być jednak zaangażowany w życie dziecka. O to, byś na bieżąco znał internetowe trendy, zadba już twoje dziecko.

Podstawowe wskazówki dla rodzica dziecka rozpoczynającego przygodę z internetem

- Rozmawiaj z dzieckiem, mów mu o zagrożeniach, na które może natrafić w internecie. Naucz je, jak może sobie poradzić, jeśli będzie miało kontakt ze szkodliwymi treściami lub nieprzyjemnym zachowaniem innego internauty. Zainteresowanie dorosłego daje dziecku poczucie bezpieczeństwa i wykształca dobre nawyki korzystania z sieci i sprzętu elektronicznego.
- Bardzo duże znaczenie ma to, w jaki sposób sam używasz internetu i urządzeń elektronicznych. Jesteś dla swojego dziecka przykładem. Dobre przyzwyczajenia i nawyki mają ogromne znaczenie dla rozwoju dziecka i wykorzystywania nowych technologii.
- Ustal z dzieckiem z jakich serwisów, usług internetowych i innych aktywności online może korzystać. Ustal zasady, powiedz mu, czego od niego oczekujesz. Ważne, by zasady te były adekwatne do wieku dziecka.
- Ustal czas, który wolno dziecku spędzić w sieci, przy komputerze, tablecie lub konsoli gier i konsekwentnie pilnuj przestrzegania tych ustaleń.
- Stosuj programy filtrujące treści, zabezpieczenia w przeglądarkach, oprogramowanie kontroli rodzicielskiej we wszystkich urządzeniach, które na to pozwalają (komputer, tablet, smartfon, smartTV). Pamiętaj również o odpowiednim zabezpieczeniu urządzeń przed złośliwym oprogramowaniem.
- Korzystajcie wspólnie z komputera lub tabletu – zawsze dziecko razem z rodzicem. Sprzęt elektroniczny nie może dziecku niczego zastępować: nie może być nagrodą, uspokajać, być sposobem na nudę lub brak kontaktu z rodzicami.
- Warto przeglądać strony, z których może korzystać dziecko i sprawdzać, w jakie miejsca w sieci prowadzą.
- Nie traktuj sprzętu elektronicznego i internetu jako jedynego sposobu spędzania wolnego czasu przez twoje dziecko. Pomyśl o innych zajęciach, również ruchowych, w które warto angażować dziecko. Zadbaj, by miało znajomych i spotykało się z nimi w realnym świecie.
- Rozmawiaj z dzieckiem o grach i stronach, z których korzysta. Wspólnie z nim odkrywaj możliwości nauki i zabawy, jakie oferuje internet. Na bieżąco oceniaj, co jest dla dziecka dobre, a co nie.

- Rozmawiaj o tym, co się dzieje online. Dziecko poznaje świat przez bezpośredni kontakt, towarzyszące temu słowa nadają mu znaczenie. Młodym ludziom często brakuje umiejętności oceny i selekcjonowania informacji znalezionych w sieci. Dzięki obecności rodziców i rozmowie z nimi dzieci mają możliwość uczenia się tego, co jest wiarygodne i sprawnego korzystania z zasobów online.
- Naucz dziecko zasady ograniczonego zaufania do osób, które spotykają w sieci. Jeśli zgadzasz się na kontakty dziecka z osobami poznanymi w internecie, monitoruj te znajomości. Reaguj na wszelkie podejrzane sytuacje. Zapewnij dziecko, że w sytuacji zagrożenia zawsze może liczyć na twoją pomoc.
- Jeśli jesteś świadkiem podejrzanej sytuacji, w której bierze udział twoje dziecko, rozmawiaj z nim, daj mu poczucie, że ma w tobie oparcie. Razem szukajcie najlepszego wyjścia. Nie zostawiaj dziecka sam na sam z jego problemami. Nawet tymi, które wydają ci się niepoważne, bo istnieją wyłącznie w internetowym świecie. Pamiętaj, że to tylko dziecko – może mu brakować dystansu nawet do tak błahych spraw, jak natrętne wpisy internetowego trolla.
- Umieść komputer w ogólnodostępnym miejscu, by wiedzieć, co robi twoje dziecko w internecie.

BEZPIECZNIE TU I TAM – KURS INTERNETOWY DLA RODZICÓW

Fundacja Orange stworzyła dla rodziców bezpłatny kurs internetowy, w którym można znaleźć wiele porad dotyczących bezpieczeństwa w internecie, zagrożeń w sieci, serwisów społecznościowych, ochrony prywatności, cyberprzemocy, zakupów online i nadużywania internetu. fundacja.orange.pl/kurs

Bezpieczny adres, login i hasło

Login i hasło to najczęstsza metoda identyfikacji użytkowników w większości serwisów i usług internetowych. Zazwyczaj w procesie rejestracji do tych serwisów konieczne jest również podanie adresu e-mail. By uniknąć sytuacji, w której inne osoby przejmują dostęp do konta naszego dziecka (pocztowego, w serwisie społecznościowym, usłudze internetowej) lub są w stanie wywnioskować z pozornie błahych informacji sporo faktów związanych z dzieckiem, naucz je zasad tworzenia bezpiecznego adresu mailowego, loginu i hasła.

WAŻNE!

Ani adres mailowy dziecka, ani login do usług sieciowych nie powinny ujawniać informacji na temat dziecka – nie mogą zawierać imienia, nazwiska, informacji o wieku lub roku urodzenia ani innych prywatnych danych, pozwalających na zidentyfikowanie dziecka. W internecie dziecko powinno się posługiwać „nickiem", czyli internetowym pseudonimem. To pod nim będą widoczne efekty jego aktywności w sieci.

Podobne zasady mają zastosowanie w przypadku tworzenia bezpiecznego hasła – nie należy w nim zawierać informacji, które mogą się kojarzyć z jego właścicielem (np. data urodzenia, imię, imię kogoś z rodziny, psa, nazwa ulubionego zespołu itd.). W takim wypadku byłoby ono bowiem łatwe do odgadnięcia przez każdego, kto zna twoje dziecko.

Pomagając dziecku przy wyborze hasła, weź również pod uwagę inne zastrzeżenia:

- Hasło nie powinno być wyrazem słownikowym. Podstawianie wyrazów ze słownika jest jedną z podstawowych metod ataku internetowych włamywaczy.
- Im więcej znaków w haśle, tym lepiej. Minimum to 8 znaków, dodanie każdego kolejnego znacznie wydłuża czas konieczny na jego złamanie. Nie powinny to być tylko litery, warto wykorzystać zarówno cyfry, duże litery, jak i znaki typu: !, @, #, $, %, ^, &, *, (.
- Nie należy używać jednego hasła do różnych serwisów. Jego złamanie otworzy dostęp do całej tożsamości internetowej dziecka.
- Hasło powinno być systematycznie zmieniane, należy jednak unikać stałego schematu zmian, np. dopisywania do stałej części hasła bieżącego miesiąca.

Jednym ze sposobów na skonstruowanie silnego hasła, które będzie łatwo zapamiętać, jest wymyślenie zdania na swój temat i stworzenie skrótu z pierwszych liter każdego z wyrazów, np. *Bardzo lubię chodzić na basen, kiedy jest ciepło.* Uzyskamy wtedy: blcnbkjc. Jeśli zastąpimy część liter podobnymi do nich cyframi, uzyskamy „8lcn6kjc", a jeśli dodamy do niego jeszcze znaki specjalne (np. 8lcn6,kjc) otrzymamy hasło, którego złamanie wymaga wielokrotnie więcej czasu (w tym przypadku ponad 12 dni w porównaniu z 52 sekundami wobec hasła podstawowego, howsecureismypassword.net).

WAŻNE!

Nawet najbardziej złożone hasło nie ochroni konta, jeśli jego użytkownik sam je zdradzi. Przekaż dziecku, że nie powinno hasła nigdzie notować, a przede wszystkim – nie powinno się nim dzielić ze swoimi znajomymi, nawet najbardziej zaufanymi, nawet w dowód przyjaźni.

Zdarza się, że hasło zostanie zapomniane. Pomagając dziecku w rejestracji w danym serwisie, zadbaj o bezpieczne procedury odzyskiwania lub resetowania hasła: podanie aktualnego adresu e-mail, do którego dostęp ma wyłącznie użytkownik hasła, wymyślenie pytania pomocniczego, na które tylko konkretny użytkownik będzie znał odpowiedź.

WAŻNE!

Naucz dziecko, by po zakończeniu korzystania z danego serwisu ZAWSZE się z niego wylogowywało i nie zaznaczało opcji zapamiętywania hasła przez przeglądarkę, przede wszystkim na ogólnodostępnych komputerach.

Serwisy społecznościowe

Portale społecznościowe (m.in. Facebook, Instagram, Snapchat, Twitter, Ask.fm) są obecnie jednymi z najbardziej popularnych wśród dzieci i młodzieży serwisów internetowych. Toczy się na nich poważna część życia towarzyskiego rówieśników twojego dziecka, prawdopodobnie również ono w nim uczestniczy. Serwisy te wymagają jednak szczególnej uwagi, gdyż ich specyfika stwarza zagrożenia dla bezpieczeństwa dzieci, chociażby ze względu na łatwość dotarcia do treści niekoniecznie dla nich przeznaczonych.

Jeżeli nie korzystasz z serwisów społecznościowych, poproś dziecko, by pokazało ci, jak działają te, z których korzysta. Łatwiej będzie wam wtedy rozmawiać o związanych z nimi zasadach bezpieczeństwa, a dodatkowo twoje dziecko poczuje się dostrzeżone i docenione.

Popularne serwisy społecznościowe nie są przeznaczone dla najmłodszych dzieci. Obowiązująca np. na Facebooku granica 13 lat wydaje się rozsądnym minimum, mimo to korzystanie z serwisów tego typu deklaruje duża część dzieci nawet z początkowych klas szkoły podstawowej. Jeżeli jest wśród nich i twoje dziecko, spróbuj skierować jego uwagę na inne formy aktywności online, bardziej adekwatne do wieku, np. serwis Sieciaki.pl (więcej o Sieciakach na str. 64). Razem możecie też ustalić, kiedy będzie odpowiedni czas na korzystanie z serwisów społecznościowych.

Zasady bezpieczeństwa dziecka w serwisach społecznościowych

- Jeżeli zgadzasz się na korzystanie przez dziecko z serwisów społecznościowych, zawczasu ustal z nim zasady, na jakich może ich używać.

Profil dziecka nie może być profilem otwartym, dostępnym dla wszystkich. W niektórych serwisach jest to ustawienie domyślne. Zmiany można dokonać w zakładce „ustawienia prywatności", należy wybrać jego widoczność tylko dla bliskich znajomych. Informacje i porady Facebooka dla rodziców, dotyczące bezpieczeństwa dzieci są dostępne pod adresem: **facebook.com/safety**.

- Ustal z dzieckiem, jakie informacje na swój temat może zamieścić na profilu. Nie należy publikować informacji ułatwiających zidentyfikowanie dziecka, w tym adresu domowego, nazwy i adresu szkoły.
- Profil powinien być zabezpieczony silnym hasłem, przypomnij dziecku o konieczności trzymania go w tajemnicy, nawet przed najbliższymi znajomymi. Jego ujawnienie może oznaczać utratę przez twoje dziecko internetowej tożsamości i umożliwić wykorzystanie profilu bez jego wiedzy, np. do podszywania się pod nie i publikowania w jego imieniu złośliwych, wymierzonych w inne osoby wpisów.
- Ostrzeż dziecko przed dodawaniem do grona znajomych osób, których nie zna osobiście. Nie powinno również wysyłać do nich zaproszeń do grona znajomych.
- Porozmawiaj z dzieckiem o zdjęciach i filmach, które publikuje na profilu, powinno unikać zdjęć ośmieszających (siebie i innych), o charakterze intymnym lub erotycznym, wszelkich, które mogą być wykorzystane przeciwko niemu. Naucz dziecko korzystania z funkcji udostępniania zdjęć tylko konkretnym osobom. Zwróć uwagę dziecka na fakt, że zdjęcie, które trafiło do sieci może zostać natychmiast skopiowane lub udostępnione w innych serwisach, a co za tym idzie – usunięcie go może być trudne lub niemożliwe.
- Wiele serwisów społecznościowych lub komunikatorów internetowych umożliwia transmisję obrazu z kamery komputera lub smartfonu na żywo, inne programy – przechwycenie i zapisanie takiego obrazu, a następnie rozpowszechnianie, czasami wbrew woli osoby prowadzącej transmisję. Ostrzeż dziecko o możliwych konsekwencjach – usunięcie takiego filmu z sieci może się okazać niemożliwe.
- Zwróć uwagę dziecka na zamieszczane przez nie komentarze lub statusy. Nie mogą być wulgarne, obrażające lub w inny sposób kogoś krzywdzące.
- Nadmierne korzystanie z serwisów społecznościowych może prowadzić do uzależnienia. Ustal z dzieckiem limit czasu na korzystanie z portali tego typu.
- Przekaż dziecku, że powinno usuwać wszelkie internetowe ataki lub złośliwości pod swoim adresem, a w przypadku gdy się powtarzają – zgłosić je moderatorowi serwisu. Reagowanie na nie agresją prowadzi jedynie do ich eskalacji.
- Przekonaj dziecko, że powinno cię informować o wszystkich niepokojących sytuacjach.
- Zanim zamieścisz w internecie zdjęcie swojego dziecka, zastanów się czy z jego powodu nie znajdzie się w niezręcznej sytuacji np. wobec swojej grupy rówieśniczej. Nie publikuj zdjęć kompromitujących lub (nawet w przypadku małych dzieci) przedstawiających je nago. W przypadku starszych dzieci – zamieszczaj zdjęcia w porozumieniu z nimi.
- Poinformuj swoje dziecko o bezpłatnym Telefonie Zaufania dla Dzieci i Młodzieży 116 111 **(116111.pl).**
- Jeśli sam, jako rodzic, potrzebujesz wsparcia lub informacji w zakresie pomocy dzieciom przeżywającym kłopoty i trudności związane m.in. z nowymi technologiami, agresją lub przemocą w szkole, skorzystaj z pomocy konsultantów Telefonu dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100 **(800100100.pl).**

WAŻNE!

Naucz dziecko zasady ograniczonego zaufania do osób poznawanych w sieci i przekonaj je, że liczba znajomych w serwisach społecznościowych nie jest wyznacznikiem jego wartości.

Czaty/komunikatory

- Czaty i komunikatory to narzędzia pozwalające kontaktować się z innymi. Wyjaśnij dziecku, że nie powinno udostępniać wszystkich informacji, o jakie proszą je rozmówcy, a przede wszystkim danych osobowych, prywatnych informacji i zdjęć.
- Młodsze dzieci powinny mieć ograniczony dostęp do serwisów komunikacyjnych, korzystać z nich jedynie w obecności rodziców.
- Sprawdź czy czat, z którego korzysta dziecko jest moderowany, czy obowiązują w nim ograniczenia wiekowe, jak prowadzona jest weryfikacja wieku, czy jest możliwość zgłaszania niepokojących sytuacji i blokowania agresywnych użytkowników.
- Porozmawiaj z dzieckiem o tym, że osoby znane mu tylko z czatu lub komunikatora mogą ukrywać swoją prawdziwą tożsamość i mieć zupełnie inne intencje, niż sądzi dziecko – ktoś przedstawiający się jako rówieśnik dziecka może okazać się osobą dorosłą, gotową wykorzystać zaufanie dziecka.
- Ostrzeż dziecko, by w rozmowie za pośrednictwem komunikatora nie dało się namówić na zachowanie, które może sprowadzić na nie kłopoty, np. żeby nie przesyłało zdjęć o charakterze intymnym i nie rozbierało się przed kamerką internetową.

Blogi/wideoblogi

- Blog, w postaci strony lub kanału z filmami (tzw. wideoblog) zawiera przemyślenia, osobiste lub tematyczne (moda, kuchnia, gry) wpisy, samodzielnie przygotowane materiały wideo lub zdjęcia. To częsta forma ekspresji młodych internautów, może być ciekawą formą prezentowania i rozwijania pasji dziecka. Tym bardziej trzeba zadbać o jego bezpieczeństwo.
- Zapoznaj się z serwisem, na którym dziecko prowadzi lub planuje prowadzić blog, sprawdź, czy udostępnia on regulamin, informuje o polityce prywatności.
- Porozmawiaj z dzieckiem o tym, jakie materiały może bezpiecznie publikować na blogu. Zwróć szczególną uwagę na prywatne zdjęcia i filmy. Z młodszym dzieckiem należy się umówić, że każdorazowo będziesz akceptował materiały przed ich publikacją (np. filmy publikowane na YouTube).
- Zwróć uwagę dziecka, by nie podawało na blogu nazbyt prywatnych informacji dotyczących jego i bliskich osób (przede wszystkim danych osobowych).
- Porozmawiaj z dzieckiem o szanowaniu praw autorskich związanych z materiałami, które decyduje się publikować online.

WAŻNE!

Zaglądaj regularnie na blog prowadzony przez dziecko. Doceń jego inicjatywę, reaguj na niepokojące treści i sytuacje.

Cyberprzemoc

Cyberprzemoc (cyberbullying), czyli przemoc z użyciem internetu i telefonów komórkowych (często rówieśnicza), to jedno z poważniejszych i bardziej powszechnych zagrożeń, z jakimi mogą mieć kontakt młodzi internauci, szczególnie w wieku gimnazjalnym. To na przykład publikowanie ośmieszających filmów i zdjęć, wulgarne i złośliwe komentarze, włamania na konta w serwisach społecznościowych, nękanie telefonami i SMS-ami oraz cały szereg intryg i ataków w sieci.

Przemoc w sieci często występuje równolegle z tradycyjną przemocą rówieśniczą, ale specyfika sieci (zasięg, możliwość pozornie anonimowego działania sprawcy) powoduje, że nawet błaha sytuacja może się stać dla dziecka bardzo poważnym doświadczeniem. W skrajnych przypadkach akty cyberprzemocy mogą prowadzić do załamania nerwowego ofiary, a nawet do prób samobójczych.

Porozmawiaj z dzieckiem na temat podstawowych zasad reagowania wobec cyberprzemocy:

- Powiedz dziecku, że jeśli padnie ofiarą przemocy w sieci, powinno się natychmiast zwrócić do ciebie lub innej zaufanej osoby dorosłej (nauczyciel, pedagog szkolny).
- Przekonaj je, że nie powinno odpowiadać na cyberprzemoc przemocą, doprowadzi w ten sposób do jej eskalacji.
- Pokaż dziecku, jak może poinformować moderatora serwisu o nadużyciu (przycisk „Zgłoś nadużycie").
- Pokaż dziecku, jak zabezpieczyć dowody cyberprzemocy (zapisanie e-maili, zrzutów ekranu z agresywnymi komentarzami w serwisach społecznościowych, natrętnych SMS-ów, więcej str. 61). Pomoże to w przypadku postępowania prawnego wobec sprawcy.
- Przekaż dziecku, że jako świadek cyberprzemocy powinno reagować: udzielić wsparcia ofierze, poinformować o sytuacji osobę dorosłą.
- Przekonaj dziecko, że nigdy nie powinno popierać przemocy (np. poprzez udostępnienie krzywdzących materiałów, klikanie „Lubię to!" czy przyłączanie się do złośliwych komentarzy).
- Sprawdź, czy w szkole twojego dziecka została wprowadzona polityka bezpieczeństwa dzieci w internecie, również w kontekście cyberprzemocy.
- Jeśli nie wiesz, jak rozwiązać problem związany z cyberprzemocą, zwróć się do konsultantów Telefonu dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci, telefon 800 100 100, **800100100.pl.**

WAŻNE!

Reaguj na przejawy cyberprzemocy i naucz dziecko, jak powinno na nie reagować. Nigdy nie bagatelizuj tego problemu.

Niebezpieczne kontakty

Dzieci samodzielnie korzystające z internetu są narażone na kontakty z obcymi osobami, m.in. za pośrednictwem czatów, komunikatorów, poczty elektronicznej, serwisów społecznościowych. Nie wszyscy użytkownicy sieci mają uczciwe intencje – dziecko może paść ofiarą próby wyłudzenia danych osobowych, kradzieży lub stać się źródłem informacji o bliskich, co może ułatwić popełnienie przestępstwa przeciwko nim. Zagrożeniem są również osoby próbujące zainteresować je niebezpiecznymi treściami (np. pornografią), zachowaniami (np. obrót narkotykami) lub ideami (np. faszyzmem, sektami).

Bardzo poważnym zagrożeniem są również próby uwodzenia dzieci w internecie, których celem jest doprowadzenie do spotkania z dzieckiem i/lub pozyskania od niego materiałów o charakterze erotycznym. Sprawcy uwodzenia w sieci często wprowadzają dzieci w błąd, fałszują swoją tożsamość, szantażują dzieci pozyskanymi materiałami lub zapisami intymnych rozmów.

WAŻNE!

Przekonaj dziecko, że nie wszyscy w internecie są tymi, za których się podają, powinno więc stosować zasadę ograniczonego zaufania do wszystkich osób poznanych w sieci.

Podstawowe zasady kontaktów online:

- Ustal z dzieckiem kategoryczny zakaz przesyłania w sieci materiałów o charakterze intymnym/seksualnym. Wyjaśnij mu, jakie wiążą się z tym zagrożenia (str. 23).
- Młodsze dzieci powinny mieć ograniczony dostęp do serwisów komunikacyjnych, korzystać z nich jedynie w obecności rodziców.
- Uświadom dziecku, jakie możliwości manipulacji daje internet i jakie intencje mogą mieć obce osoby próbujące nawiązać z nim kontakt.
- Przekaż dziecku, żeby kontaktowało się online jedynie z osobami, które zna spoza sieci. W przypadku nowych znajomości ustal z dzieckiem, że cię o nich poinformuje.
- Przestrzeż dziecko przed przyjmowaniem w serwisach społecznościowych zaproszeń do grona znajomych od osób nieznanych.
- Zwróć uwagę dziecka, by w kontaktach online z nieznajomymi nie przesyłało prywatnych informacji i materiałów (zdjęć, filmów).
- Przypomnij dziecku, że w sytuacji niepewności lub zagrożenia ze strony kogokolwiek w sieci zawsze powinno się do ciebie zwrócić o pomoc.

Zwróć uwagę dziecka na zagrożenia związane ze spotkaniami z osobami poznanymi w sieci:

- W przypadku młodszych dzieci najbezpieczniej jest całkowicie wykluczyć spotkania z osobami znanymi jedynie z internetu. W przypadku dzieci starszych, spotkania takie mogą się odbywać jedynie zgodnie z ustalonymi zasadami, pod ścisłym nadzorem rodziców.
- Ustal z dzieckiem, że poinformuje cię o każdej propozycji spotkania otrzymanej od osoby poznanej w sieci.
- Uzgodnijcie, że do spotkania może dojść jedynie za zgodą rodziców.
- Ustal z dzieckiem zasady bezpiecznego spotkania z osobą poznaną w sieci:
  - dziecku powinna towarzyszyć zaufana osoba dorosła lub (w przypadku starszych dzieci) przynajmniej znajomi rówieśnicy,
  - spotkanie powinno się odbyć w ciągu dnia w miejscu publicznym.

WAŻNE!

Już samo nawiązywanie przez osobę dorosłą w internecie kontaktów z dzieckiem, których celem jest doprowadzenie do spotkania i wykorzystania seksualnego lub pozyskanie od dziecka materiałów pornograficznych, jest przestępstwem. Zawsze kiedy podejrzewasz, że twoje dziecko padło ofiarą uwodzenia, poinformuj o tym policję.

Seksting i kamerki internetowe

W przypadku sekstingu (zjawiska polegającego na przesyłaniu osobistych zdjęć i filmów o charakterze seksualnym za pośrednictwem telefonu i internetu, więcej str. 10), zdarza się, że intymne zdjęcia trafiają do sieci – czasami wbrew intencjom ich odbiorcy, czasami w formie zemsty lub szantażu. W każdym z tych przypadków – jeśli już zostaną rozpowszechnione – ich usunięcie może się okazać niemożliwe.

Podobnym zagrożeniem wobec dzieci są serwisy internetowe oferujące transmisję na żywo – dla pojedynczego odbiorcy lub wielu widzów. Część z nich specjalizuje się w pokazach erotycznych, część umożliwia zarabianie pieniędzy osobom występującym przed kamerą internetową. Ryzykowne zachowania dziecka przed kamerą internetową (zazwyczaj jedynym zabezpieczeniem przed dostępem osób nieletnich do tego typu serwisów jest deklaracja użytkownika, że ukończył 18 lat) mogą wynikać z odkrywania własnej seksualności, chęci zysku lub prowokacji ze strony widowni, która komentując to, co dzieje się na ekranie i nagradzając autora transmisji realnymi pieniędzmi, ma możliwość wymuszania konkretnych zachowań, również o charakterze seksualnym. Grono odbiorców tego typu pokazów nie musi się ograniczać do odbiorców transmisji na żywo, mogą one zostać zarejestrowane w postaci filmu lub zrzutów ekranu.

Upewnij się, że kamera w tablecie, telefonie, laptopie dziecka jest wyłączona. Pamiętaj jednak, że niektóre aplikacje po ich uruchomieniu włączają domyślnie kamerę. Sprawdź czy w opcjach aplikacji można wyłączyć kamerę na stałe. Jeśli masz jakiekolwiek wątpliwości czy urządzenie nie przekazuje obrazu z kamery – zaklej jej obiektyw nieprzezroczystą taśmą klejącą.

WAŻNE!

Naucz dziecko, żeby pod żadnym pozorem nie wysyłało ani nie publikowało w sieci zdjęć i filmów nago lub o charakterze seksualnym. Rozmawiaj z dzieckiem o seksualności i zagrożeniach związanych z upublicznianiem intymnych zdjęć.

Gry

Gry, zarówno komputerowe, jak i te dostępne jako aplikacja na smartfonie lub tablecie, gry na konsole są dla dzieci i młodzieży stałym elementem spędzania wolnego czasu. Rodzice, nie wiedząc zbyt wiele na temat gier, mogą się niepokoić ich rolą w życiu dziecka. Duża część gier jest przeznaczona dla nastolatków, a czasem wyłącznie dla osób pełnoletnich, ponieważ zawiera niebezpieczne treści związane z przemocą, erotyką lub pornografią. W przypadku gier sieciowych pojawia się dodatkowo ryzyko niebezpiecznych kontaktów i cyberprzemocy. Ta forma spędzania czasu zazwyczaj jest bardzo wciągająca – stąd też ryzyko uzależnienia.

Jednocześnie gry komputerowe mogą być dla dziecka pozytywnym doświadczeniem – rozwijają umiejętności manualne, ćwiczą koncentrację, uczą pracy w zespole, a gry edukacyjne w atrakcyjny sposób poszerzają wiedzę dziecka.

APLIKACJE DLA NAJMŁODSZYCH DZIECI

Dla najmłodszych dzieci Fundacja Dajemy Dzieciom Siłę wraz z Fundacją Orange przygotowały bezpłatne, niezawierające reklam aplikacje: Necio (dla dzieci w wieku 4-6 lat, zawierająca m.in. grę zręcznościową, bajkę edukacyjną, materiały do wydrukowania i zabawy w domu, necio.pl/aplikacja) oraz BeStApp (katalog bezpiecznych stron dla dzieci w wieku 3-6 lat, fdds.pl/bestapp).

Zanim twoje dziecko zacznie grać:

- Znajdź grę odpowiednią dla jego wieku. Możesz się oprzeć na systemie oznaczeń PEGI (str. 25) i/lub opisie danej gry w internecie. Przekonać się, z czym będzie miało kontakt dziecko, możesz również, oglądając fragmenty gry w serwisie **youtube.com.**
- Towarzysz dziecku w czasie gry.

- Spróbuj rozmawiać z dzieckiem o grach – co jest w nich najbardziej interesujące, a co może być nieodpowiednie. Zwracaj uwagę, jakie zachowania są nagradzane/promowane w grze i rozmawiaj o tym z dzieckiem. Zagrożenia płynące z gier komputerowych często są związane z treściami, z którymi dziecko ma kontakt. Rozmawiajcie o tym, co widzi, jak to odbiera. U graczy często następuje proces zobojętnienia na brutalne zachowanie – zabijanie, kradzieże, wulgarny język. Często angażowanie się w przemoc jest warunkiem przejścia do następnego poziomu gry. Regularne powtarzanie agresywnych zachowań modeluje i wzmacnia taką postawę.
- Ustal z dzieckiem zasady, m.in. czas, który może poświęcać na grę, porę dnia.
- Przypomnij dziecku, żeby podczas interakcji z innymi graczami nie podawało prywatnych informacji na swój temat i przestrzegało zasad netykiety. Możliwość wspólnego grania i komunikowania się z innymi użytkownikami oznacza kontakt z nieznanymi osobami.
- Zwróć uwagę dziecka, by w przypadku gier sieciowych nie ujawniało innym loginu i hasła, np. z prośbą o pokonanie trudniejszego etapu gry.
- Dodatkowe oprogramowanie, rozszerzenie gry, możliwość grania online może zmienić klasyfikację wiekową wybranej pozycji.
- Zachęć dziecko do mówienia o niepokojących zdarzeniach w sieci i zapewnij je, że może się zwrócić do ciebie w trudnej sytuacji.

Młodsze dzieci powinny korzystać z gier pod okiem rodziców. Starszym dzieciom również należy od czasu do czasu towarzyszyć podczas grania. Może się to okazać ciekawym doświadczeniem i pozwolić na zaobserwowanie, czy nie dzieje się nic niepokojącego.

Więcej o grach na konsole i ich zabezpieczeniach technicznych – str. 56.

WAŻNE!

Reaguj, jeżeli zauważysz, że granie negatywnie wpływa na zachowanie dziecka. Zwróć uwagę na ewentualne symptomy uzależnienia (str. 27).

System PEGI

PEGI to ogólnoeuropejski system klasyfikacji gier (*Pan-European Game Information*, **pegi.info/pl/**), odnoszący się do wieku graczy, informujący o charakterze treści zawartych w grach komputerowych i wideo oraz aplikacjach. Klasyfikacja PEGI pomaga w podjęciu decyzji o zakupie gry dostosowanej do wieku gracza. Oznaczenia odnoszą się do treści zawartych w produkcie (nie jest to informacjach o poziomie trudności czy wymaganych umiejętnościach). I tak np. oznaczenie „16" informuje, że jest to gra odpowiednia dla osób powyżej 16. roku życia.

Z kolei piktogramy informują o charakterze zawartości, np. przemocy czy wulgarnym słownictwie.

Wulgarny język. W grze jest używany wulgarny język.

Dyskryminacja. Gra pokazuje przypadki dyskryminacji lub zawiera materiały, które mogą do niej zachęcać.

Narkotyki. W grze pojawiają się nawiązania do narkotyków lub jest pokazane zażywanie narkotyków.

Seks. W grze pojawiają się nagość i/lub zachowania seksualne, lub nawiązania do zachowań o charakterze seksualnym.

Strach. Gra może przestraszyć młodsze dzieci.

Przemoc. Gra zawiera elementy przemocy.

Hazard. Gry, które zachęcają do uprawiania hazardu lub go uczą.

Online. Gra, w którą można grać online.

PEGI Online

Znak PEGI Online przysługuje tym internetowym serwisom udostępniającym gry, które spełniają standardy określone przez PEGI. Dotyczą one m.in. ochrony przed niezgodnymi z prawem i obraźliwymi treściami tworzonymi przez użytkowników, niepożądanymi linkami, a także ochrony prywatności podczas gier internetowych. Logo PEGI Online (zamieszczone na pudełku i/lub witrynie gry) wskazuje, czy gra jest kontrolowana przez operatora dbającego o ochronę użytkowników.

Nadużywanie internetu i telefonów

Internet i komputer mogą uzależniać. Dostęp do ogromnej ilości informacji, rozrywki, rywalizacja z innymi graczami, łatwy kontakt ze znajomymi powodują, że część użytkowników internetu traci kontrolę i zaczyna szukać coraz silniejszych bodźców. Najczęściej młodzi ludzie nadużywają gier, serwisów społecznościowych oraz serwisów pornograficznych.

O uzależnieniu można mówić, kiedy spełnione są dwa podstawowe warunki:

1. Czas spędzany w internecie i intensywność poszukiwanych doznań wymykają się spod kontroli.
2. Korzystanie z sieci prowadzi do zaniedbywania innych aspektów życia, nawet potrzeb fizjologicznych, powoduje cierpienie – osoby uzależnionej bądź osób z jej otoczenia.

By zapobiec patologicznemu używaniu internetu i komputera, ustal z dzieckiem zasady korzystania z mediów elektronicznych dostosowanych do jego wieku.

- Uzgodnij czas, jaki dziecko może poświęcić na korzystanie z mediów elektronicznych i porę dnia na to przeznaczoną. W przypadku dzieci w wieku wczesnoszkolnym i młodszych nie powinno to być więcej niż pół godziny dziennie.
- Ustal z dzieckiem, z jakich serwisów może korzystać, wybierzcie te, które są dostosowane do jego wieku. Skieruj jego uwagę na pozytywne zastosowania sieci.
- Zainteresuj dziecko formami aktywności niezwiązanymi z mediami elektronicznymi.
- Wykorzystaj oprogramowanie filtrujące i programy kontroli rodzicielskiej, pamiętaj jednak, że dzieci w wieku przedszkolnym i wczesnoszkolnym powinny korzystać z sieci pod okiem rodziców.

Zastanów się, czy twoje dziecko nie nadużywa sieci. Występowanie u niego nawet kilku spośród poniższych objawów nie musi świadczyć o uzależnieniu, ale na pewno jest sygnałem do wzmożonego zainteresowania:

- spędza przy komputerze coraz więcej czasu kosztem innych zainteresowań,
- z powodu aktywności w internecie zaniedbuje obowiązki rodzinne i szkolne,
- pojawiają się konflikty rodzinne na tle używania komputera lub internetu,
- pojawiają się kłamstwa dotyczące czasu, jaki spędza w internecie,

- podejmowane próby ograniczenia czasu online są nieudane, reaguje rozdrażnieniem lub nawet agresją, gdy korzystanie z komputera jest utrudnione lub niemożliwe.

Jeśli podejrzewasz, że dziecko nadużywa internetu lub mediów elektronicznych:

1. Nazwij problem. Porozmawiaj z dzieckiem, powiedz mu, co niepokojącego widzisz w jego zachowaniu.
2. Przyjrzyj się sytuacjom, w których dziecko ucieka w internet lub sięga po elektroniczne gadżety. Wspólnie z dzieckiem poszukaj alternatywy, np. działań, które sprawiają mu równie dużo przyjemności lub w podobny sposób pomagają odreagować negatywne emocje.
3. Ustalcie harmonogram dnia, by zrównoważyć czas spędzany przez dziecko w sieci i poza nią.
4. Ustalcie zasady i etapy ograniczania korzystania z internetu. Warto wraz z dzieckiem omówić stopniowe ograniczenie czasu przed monitorem.
5. Nagradzaj sukcesy w ograniczaniu czasu spędzanego w internecie.
6. Jeśli dziecko korzysta z internetu lub komputera w sposób, który zagraża jego zdrowiu i/lub życiu (np. zaniedbuje podstawowe potrzeby fizjologiczne), odłącz internet, wyłącz komputer, ale wyjaśnij dziecku przyczyny tych ograniczeń. Dziecko poczuje się bezpieczniej, gdy będzie znało twoje intencje.

WAŻNE!

W skrajnych przypadkach nadużywanie internetu i komputera może się okazać poważnym problemem, wymagającym profesjonalnej pomocy. Szukaj jej u pedagoga lub psychologa szkolnego oraz specjalistów w poradniach uzależnień.

Zakupy w internecie

Dzieci coraz częściej samodzielnie dokonują transakcji w sieci. Co prawda, z wszystkich praw konsumenta dziecko zacznie korzystać wraz z ukończeniem 18. roku życia, jednak w wieku 13-18 lat może samodzielnie kupować drobne towary, takie jak książki, prasa, żywność.

Duża część płatności w internecie odbywa się w oparciu o karty kredytowe. Niektórzy rodzice dla własnej wygody podają dzieciom numer swojej karty. To ryzykowna praktyka, mogąca narazić ich na poważne konsekwencje finansowe. Problemem mogą być nie tylko nadmiar i kwoty transakcji dokonanych przez dziecko, ale również ryzyko kradzieży numeru karty.

WAŻNE!

Nie udostępniaj dziecku numeru swojej karty kredytowej. Sprawdź wiarygodność ewentualnej transakcji i sam wprowadź niezbędne dane. Sprawdź, czy dane karty nie zostały zapamiętane przez aplikację, dzięki której dokonałeś płatności.

Coraz częściej specjalne usługi dla niepełnoletnich użytkowników udostępniają też serwisy internetowe, np. konto Junior w serwisie aukcyjnym Allegro, o ograniczonej wysokości transakcji oraz wykluczające pewne kategorie towarów (erotyka, samochody, broń itp.).

Porozmawiaj z dzieckiem o podstawowych zasadach zachowania bezpieczeństwa w transakcjach online:

- Naucz dziecko, że dane karty płatniczej oraz loginy i hasła do serwisów transakcyjnych w sieci powinno utrzymywać w tajemnicy, nawet przed najbliższymi znajomymi.
- Pokaż dziecku, jak można zweryfikować wiarygodność sprzedawców:
  - zapoznając się z regulaminem sklepu,
  - sprawdzając, jak długo działa sklep,
  - zasięgając opinii znajomych,
  - czytając opinie kontrahentów,
  - sprawdzając liczbę pozytywnie zrealizowanych transakcji.

Opisy przedmiotów sprzedawanych w sklepach internetowych lub na portalach aukcyjnych często nie są wiarygodne. Naucz dziecko weryfikowania informacji marketingowych. Zwróć jego uwagę na fakt, że nawet prywatne komentarze na temat danego produktu mogą być manipulacją marketingową.

Przydatne informacje dotyczące zakupów w internecie znajdują się na specjalnej stronie Urzędu Ochrony Konkurencji i Konsumentów: **ezakupy.uokik.gov.pl**.

Oszustwa sieciowe

Pozwalając dziecku na dysponowanie pieniędzmi w sieci, zwróć jego uwagę na popularne oszustwa sieciowe.

- Fałszywe e-maile z prośbą o pomoc (choremu dziecku, bezdomnym zwierzętom itp.) lub zawierające ofertę wyjątkowo korzystnej transakcji. Zazwyczaj adresat proszony jest o przesłanie pieniędzy na wskazany numer konta.
- Nierzetelne transakcje. Zdarza się, że zakupiony towar nie dociera do nabywcy lub nie jest zgodny z opisem, a jego wartość jest istotnie niższa niż spodziewana.

- Kradzież numerów kart płatniczych, loginów i haseł do systemów bankowych lub serwisów aukcyjnych *(phishing)*. Zazwyczaj polega ona na stworzeniu fałszywej strony, łudząco podobnej do strony np. banku, na którą ofiara próbuje się zalogować, podając poufne dane. Może również polegać na rozsyłaniu maili udających oficjalną korespondencję (np. z banku) z prośbą o podanie poufnych informacji.
- Wyłudzenia. Złodzieje w sieci biorą czasem na cel dzieci, wykorzystując ich naiwność. Na przykład pod pretekstem uruchomienia nowych funkcji w grze proszą o podanie poufnych danych, w ten sposób je pozyskując.

WAŻNE!

Zdecydowana większość stron, na których dokonywane są płatności online, posługuje się protokołem szyfrującym przekazywane dane (HTTPS, znak kłódki w polu adresu). Brak tego bezpiecznego protokołu powinien wzbudzić podejrzenia co do rzetelności sprzedawcy.

Plagiat

Obecne pokolenie dzieci i młodzieży nazywane jest pokoleniem „kopiuj, wklej". I rzeczywiście, metoda ta znajduje częste zastosowanie, chociażby w trakcie odrabiania prac domowych. Wiele popularnych serwisów udostępnia gotowe wypracowania i inne teksty pomocnicze. Przedmiotem bezprawnego wykorzystywania są również zdjęcia, grafiki i filmy.

Utwory, dzieła (w tym rysunki, teksty, fotografie, utwory muzyczne) są objęte ochroną praw autorskich. By uniknąć nieporozumień, najlepiej wykorzystywać te dzieła i utwory, co do których ich autorzy jasno określili, w jaki sposób można się nimi posługiwać. Jednym z najbardziej popularnych systemów informowania o tym, jak można wykorzystać dane dzieło, czy można je modyfikować lub udostępniać, są licencje Creative Commons. Więcej informacji na ich temat: **creativecommons.pl**.

Naucz dziecko poszanowania cudzej własności intelektualnej i przestrzeż je przed kopiowaniem prac domowych z sieci.

- Pokaż dziecku, jak poszukiwać w sieci materiałów i jak wykorzystywać je do przygotowania samodzielnych opracowań.
- Naucz dziecko, jak należy cytować cudze teksty i jak wskazywać źródła oryginalnych tekstów, zdjęć i innych materiałów.
- Uświadom dziecku, jakie konsekwencje może ponieść, posługując się plagiatem i jakie są możliwości zweryfikowania oryginalności tekstu, np. przy użyciu programów antyplagiatowych.
- Zadbaj, by zadania domowe dziecka były jego własną pracą.

Netykieta

W sieci, tak jak i poza nią, uczciwość i zasady kulturalnego zachowania obowiązują wszystkich. Zwróć na to uwagę swojego dziecka, bo poczucie anonimowości i brak bezpośredniego kontaktu z odbiorcą powodują, że dzieci łatwiej łamią te zasady w internecie, niż w świecie rzeczywistym.

Netykieta nie jest jednym ogólnie przyjętym kodeksem zasad, zmienia się wraz z internetem. Przekaż dziecku kilka najbardziej podstawowych reguł:

- Komunikuj się kulturalnie i bez używania wulgaryzmów.
- Pisz z sensem i na temat.
- Nie pisz wiadomości wielkimi literami.
- Jeżeli stosujesz emotikony, rób to z umiarem.
- Nie wysyłaj spamu i „łańcuszków szczęścia".
- Nie przesyłaj e-mailem zbyt ciężkich załączników. Duże pliki można przekazać, używając np. wirtualnych dysków.
- Nie zamieszczaj w sieci „ciężkich" grafik.
- Nie publikuj cudzych materiałów bez podania źródła lub wbrew ich licencji.
- Nie publikuj zdjęć na których są widoczne inne osoby bez ich zgody.
- Nie upubliczniaj adresów odbiorców maila pisanego do kilku osób (korzystaj z pola UDW – „ukryte do wiadomości").
- Nie zadawaj na forach pytań, które już zostały zadane, nie otwieraj dyskutowanych wcześniej wątków (korzystaj z wyszukiwarki).

Wiarygodność informacji

Młodzi ludzie są z natury łatwowierni i często bezkrytycznie podchodzą do informacji znalezionych w sieci. Tymczasem obok treści wartościowych można znaleźć w internecie informacje nierzetelne, przekłamania historyczne, błędnie prezentowane ustalenia naukowe, a także trafić na teksty promujące nietolerancję, gloryfikujące faszyzm, niezdrowy tryb życia (anoreksja i inne), umniejszające szkodliwości używek lub propagujące błędne praktyki medyczne.

Naucz dziecko zasady ograniczonego zaufania do treści dostępnych online. Naucz je również weryfikowania rzetelności informacji dostępnych w internecie.

- Pokaż dziecku, jak poszukiwać informacji w sieci. Naucz je metod zaawansowanego wyszukiwania.
- Naucz dziecko weryfikowania treści poprzez porównywanie informacji z różnych źródeł.

- Zwróć uwagę dziecka na fakt, że blogi i inne fora wymiany opinii prezentują subiektywne poglądy ich autorów i obarczone są wysokim ryzykiem nierzetelności.
- Pokaż dziecku sprawdzone serwisy, które uznajesz za wiarygodne.
- Zwróć uwagę dziecka na treści marketingowe, które mogą sprawiać wrażenie obiektywnych informacji.
- Przekonaj dziecko, by w sytuacji wątpliwości co do wiarygodności znalezionych w sieci treści zwróciło się do ciebie o pomoc.

Jak zweryfikować wiarygodność informacji na stronie internetowej?
By ocenić wiarygodność informacji zamieszczonych na stronie internetowej, warto odpowiedzieć sobie na pytania:

- Czy na stronie dostępne są dane kontaktowe prowadzącej ją firmy lub osoby?
- Czy strona publikuje daty aktualizacji?
- Czy strona udostępnia regulamin?
- Czy podano imię i nazwisko autora tekstu? Czy wpisanie go do wyszukiwarki przynosi dodatkowe informacje na temat autora?
- Czy autor tekstu reprezentuje konkretną organizację/instytucję? Czy jego powiązania z daną organizacją mogą mieć (pozytywny lub negatywny) wpływ na tekst?
- Czy podane informacje poparte są dowodami?
- Czy cytaty i odnośniki, definicje są opatrzone źródłami? Czy można je zweryfikować?

Publikowanie zdjęć dzieci w sieci

Popularność serwisów społecznościowych i internetowych albumów pozwalających na publikowanie własnych zdjęć powoduje, że rodzice bezrefleksyjnie zamieszczają w sieci setki fotografii swoich pociech. Publikowanie zdjęć przedstawiających dziecko może być dla niego zagrożeniem, szczególnie jeżeli jest przedstawione na nich nago lub w niezręcznej sytuacji. Nawet po latach takie materiały mogą przyczynić się do skompromitowania nastolatka lub nawet dorosłej osoby. W przypadku zdjęć nagiego lub prawie nagiego dziecka problemem może być również zainteresowanie takimi materiałami pedofilów.

WAŻNE!

Przed zamieszczeniem zdjęcia dziecka w internecie zastanów się, czy nie będzie to dla niego w przyszłości źródłem wstydu i zakłopotania.

Jeżeli decydujesz się na publikowanie zdjęć lub filmów przedstawiających twoje dziecko, pamiętaj o następujących zasadach:

- Nie publikuj materiałów z nagim dzieckiem lub ubranym jedynie w bieliznę.
- Nie publikuj materiałów przedstawiających dzieci w intymnych lub niezręcznych sytuacjach (np. w toalecie, podczas czynności pielęgnacyjnych).
- Nie rejestruj i nie publikuj materiałów ośmieszających dzieci (w przebraniu, przeklinających, opatrzonych „zabawnymi” opisami).
- Profil, na którym publikowane są materiały, ustaw jako zamknięty (niedostępny dla osób nieznajomych).
- Każdorazowo w „ustawieniach” oznaczaj dostępność zdjęcia jako np. widoczne tylko dla rodziny i najbliższych znajomych.
- Nie podpisuj zdjęć imieniem i nazwiskiem dziecka.

WAŻNE!

Fascynacja portalami społecznościowymi powoduje, że rodzice zakładają swoim pociechom profile już w wieku niemowlęcym. To niezgodne z regulaminem większości tego typu serwisów, przede wszystkim jednak – to narażanie bezpieczeństwa dziecka i jego prywatności na niepotrzebne ryzyko.

Zdrowie

Nadmierne korzystanie z mediów elektronicznych przez dzieci i młodzież może mieć negatywny wpływ na ich zdrowie. Spędzanie godzin przed komputerem, w pozycji zaprzeczającej zasadom ergonomii i w złych warunkach oświetleniowych, może spowodować:

- skrzywienie kręgosłupa,
- zanik mięśni,
- zwyrodnienie stawów (np. zespół cieśni nadgarstka, będący efektem długotrwałego używania myszki),
- otyłość,
- choroby wzroku (np. zespół suchego oka, wynikający z mniejszej częstości mrugania przed ekranem komputera).

Ustal z dzieckiem pory korzystania z komputera, maksymalny dzienny czas, jaki może spędzić przy komputerze i innych mediach, czas jednorazowej sesji. Zadbaj o dobrze zorganizowane stanowisko komputerowe dziecka:

- Biurko powinno być dostosowane do wzrostu dziecka, ekran powinien znajdować się na poziomie oczu dziecka.
- Dziecko powinno siedzieć bokiem lub przodem do pokoju.
- Światło dzienne i/lub sztuczne (lampa) nie powinno padać wprost na monitor.
- Krzesło powinno być stabilne, obrotowe, wyposażone w kółka, z regulowaną wysokością oparcia i siedziska.
- Podłokietniki powinny być ustawione na tej samej wysokości co dłonie, aby przedramię mogło być ułożone poziomo.

Zdrowie a urządzenia mobilne

Co prawda, badania nie rozstrzygają jednoznacznie, czy korzystanie z telefonów komórkowych wpływa np. na zwiększoną zapadalność na choroby nowotworowe, warto jednak, szczególnie w przypadku dzieci, zwrócić uwagę na bezpieczeństwo ich użytkowania. Wydawane do tej pory zalecenia podkreślają, że dzieci i młodzież powinny korzystać z telefonów komórkowych z umiarem. Jeżeli zgadzasz się, by twoje małe dziecko używało własnego telefonu komórkowego, zadbaj, by korzystanie z niego było ograniczone do niezbędnego minimum, maksymalny czas przeznaczony na rozmowy należy ustalić również w przypadku starszych dzieci (np. 20-30 minut dziennie).

	Porozmawiaj z dzieckiem o bezpieczeństwie używania urządzeń mobilnych i minimalizowaniu wpływu fal radiowych.
	Przekonaj dziecko, by korzystało z zestawu słuchawkowego (przewodowego lub Bluetooth – moc wykorzystywana przez Bluetooth jest wielokrotnie niższa niż w przypadku transmisji w sieci komórkowej). Jego używanie powoduje oddalenie telefonu od głowy, a co za tym idzie – wydatne zmniejszenie jej ekspozycji na fale radiowe.
	Przekonaj dziecko, by zamiast rozmów telefonicznych wykorzystywało SMS-y i internet. Patrzenie na ekran wymusza oddalenie urządzenia od ciała i zmniejsza jego ekspozycję na fale radiowe.
	Zwróć uwagę dziecka na fakt, że w przypadku słabego zasięgu nadajnik telefonu pracuje z maksymalną mocą. Przekaż dziecku, że rozmowy telefoniczne, szczególnie te dłuższe, powinno się prowadzić z miejsc zapewniających wysoki poziom sygnału (poza garażami podziemnymi, windą). Optymalna siła sygnału to 4-5 kresek na wyświetlaczu telefonu.

	Zadbaj, by dziecko nie nosiło telefonu bezpośrednio przy ciele (z dala od podbrzusza, lepiej w torbie niż w kieszeni) i nie spało w bezpośredniej bliskości telefonu. W przypadku laptopów i tabletów dziecko nie powinno ich opierać bezpośrednio o ciało, np. trzymając na kolanach. Regularne przegrzewanie ciała może prowadzić do chorób skóry. Urządzenia mobilne nie powinny być również używane w bezpośredniej bliskości brzucha kobiety w ciąży.
	Zwróć również uwagę dziecka na fakt, że nie powinno używać telefonu, nawet z zestawem sluchawkowym, np. trakcie jazdy rowerem – tak jak u kierowcy – rozmowa telefoniczna opóźnia reakcję na wydarzenia na drodze. Co więcej – ze słuchawkami w uszach, nie słysząc niebezpieczeństwa, dziecko może być narażone na wypadki komunikacyjne.
	Telefon i inne urządzenia mobilne nie powinny być używane w bezpośredniej bliskości elektronicznego sprzętu medycznego (w tym rozruszników serca, pomp insulinowych i neurostymulatorów). Jeśli dziecko korzysta z aparatu słuchowego, poszukaj telefonu, który będzie mógł z nim współpracować.
	Przekaż dziecku, że powinno przestrzegać zakazów używania telefonów komórkowych – większość z nich ma swoje uzasadnienie.
	Zwróć uwagę dziecka na fakt, że używając słuchawek, nie powinno ustawiać maksymalnej głośności – grozi to uszkodzeniem słuchu.
	Używaj i przekazuj dziecku do użytku tylko telefony komórkowe kupione w autoryzowanych punktach sprzedaży – gwarantuje to spełnianie przez urządzenie wymagań bezpieczeństwa. Mogą one nie być spełniane przez telefony przerabiane, „z drugiej ręki", pochodzące od nieznanych producentów.

Więcej: ondes-radio.orange.com/pl/Accueil

WAŻNE!

Pamiętaj, że korzystanie z mediów elektronicznych nie może być dominującą formą aktywności dziecka. Zadbaj o jego ruch i spędzanie czasu na świeżym powietrzu.

Bezpieczeństwo sprzętowe

Wszystkie urządzenia, zarówno mobilne, jak i stacjonarne, wymieniające informacje poprzez internet są narażone na zainfekowanie złośliwym oprogramowaniem. Ryzyko, że w komputerze lub tablecie znajdzie się oprogramowanie, które negatywnie wpłynie na jego działanie, bezpieczeństwo danych, a nawet uniemożliwi korzystanie z niego, rośnie w przypadku, kiedy jego użytkownikiem jest dziecko – nieświadome zagrożeń i możliwości zabezpieczenia się przed nimi.

Ze względu na błyskawiczną ewolucję zagrożeń komputerowych i coraz bardziej zaawansowane metody ataku, nie sposób zabezpieczyć się w stu procentach. Można jednak wydatnie ograniczyć ryzyko związane z korzystaniem z sieci, stosując właściwe zabezpieczenia.

Złośliwe oprogramowanie *(malware)* to wszystkie programy, których celem jest spowodowanie szkód w naszym komputerze lub tablecie. Programy tego typu mogą wykradać dane (zwłaszcza numery kart płatniczych oraz loginy i hasła, przede wszystkim do serwisów bankowych), niszczyć pliki, zakłócać lub uniemożliwiać działanie systemu operacyjnego. Czasami zainfekowanie nimi komputera wymaga naszego działania (np. otwarcia załącznika z poczty elektronicznej lub użycia pamięci USB, na którą skopiowano pliki z już zarażonego komputera), czasem jednak wystarczy wizyta na niebudzącej podejrzeń stronie, kontrolowanej przez cyberprzestępców. Najistotniejsze zagrożenia to:

- Trojany (konie trojańskie) – oprogramowanie, które pod pozorem użyteczności otwiera dostęp do komputera ofiary wyspecjalizowanym, złośliwym programom.
- Programy szpiegujące – oprogramowanie zbierające w nieuprawniony sposób informacje o użytkowniku i zazwyczaj przekazujące zawartość komputera na zewnętrzne serwery, kontrolowane przez cyberprzestępców.
- Wirusy i robaki – samopowielające się programy, które są w stanie wbrew woli użytkownika ingerować w zawartość komputera i rozpowszechniać się na kolejne komputery, np. poprzez pocztę elektroniczną lub wraz z plikami, np. na nośnikach USB.

WAŻNE!

Warto regularnie odwiedzać witrynę cert.orange.pl/cybertarcza, by sprawdzić swoją domową sieć po kątem nowych, niewykrywalnych przez antywirusy zagrożeń (dostępne wyłącznie dla klientów Orange Polska).

Oprogramowanie antywirusowe. Dostępne są zarówno programy komercyjne, jak również udostępniane bezpłatnie, np. tylko na potrzeby użytku domowego. Instalując program tego typu, warto zadbać nie tylko o to, by systematycznie aktualizował swoją bazę wirusów, ale też i systematycznie skanował nasz komputer w ich poszukiwaniu. Znanymi darmowymi programami antywirusowymi są: Avast Free Antivirus, AVG Anti-virus Free Edition lub Microsoft Security Essentials (dostępny dla systemów Windows XP/Vista/7). W Windows 8 standardowym (dostarczanym wraz z systemem) programem służącym do ochrony komputera jest Windows Defender.

Zapora sieciowa *(firewall)***.** To oprogramowanie, które kontroluje dane wymieniane przez komputer za pośrednictwem internetu. Zapobiega lub informuje o łączeniu się naszego komputera z podejrzanymi serwerami, przeciwdziała próbom włamania. W systemach Windows (począwszy od XP) zapora jest elementem systemu komputera i jest domyślnie włączona (w Windows XP i Vista funkcja dostępna w „Centrum zabezpieczeń", w Windows 7 i 8/8.1 w „Centrum akcji").

Aktualizacje systemu/oprogramowania. Kolejnym elementem zwiększającym bezpieczeństwo komputera jest regularne aktualizowanie systemu operacyjnego oraz oprogramowania, w szczególności używanych przez nas przeglądarek internetowych. Często dopiero po wypuszczeniu na rynek nowego oprogramowania są wykrywane w nim luki w bezpieczeństwie, umożliwiające atak na nasz komputer. Wtedy również są publikowane przez twórców oprogramowania aktualizacje. W przypadku systemu Windows warto wybrać opcję automatycznego sprawdzania i instalowania aktualizacji i absolutnie nie opóźniać aktualizacji.

WAŻNE!

Chociaż Microsoft nie udostępnia już bieżących aktualizacji systemów Windows XP i Vista, są one wciąż popularne w domowych komputerach. Trzeba jednak pamiętać, że komputer z takim systemem nie jest już chroniony przez producenta tak, jak nowsze systemy MS. Komputera z tymi systemami nie należy używać do operacji bankowych, lepiej nie przechowywać na nim istotnych dla nas informacji. Najskuteczniejszym sposobem zadbania o bezpieczeństwo komputera z takim systemem jest odłączenie go na stałe od sieci. Tymczasowo pomóc mogą regularne aktualizacje zainstalowanych programów (w tym obowiązkowo firewalla i antywirusa), docelowo należy jednak rozważyć zmianę systemu operacyjnego na wspierany przez producenta.

Objawami zainfekowania komputera przez szkodliwe oprogramowanie mogą być: wolniejsze działanie lub zawieszanie się systemu, wolniejsze działanie sieci, uszkodzone pliki, komunikaty zapory sieciowej o próbie łączenia się z internetem przez nowe, nieznane programy, niespodziewana zmiana wyglądu przeglądarki internetowej, strony startowej lub menu programów.

Jeśli komputer został zainfekowany, zaktualizuj ręcznie program antywirusowy i przeskanuj twardy dysk. W przypadku wykrycia zagrożenia program antywirusowy zazwyczaj pyta użytkownika, co ma zrobić i sugeruje najwłaściwsze rozwiązanie (najczęściej jest to kwarantanna lub usunięcie zainfekowanych plików). Jeśli masz problemy z aktualizacją programu antywirusowego (złośliwe oprogramowanie często blokuje tę możliwość), skorzystaj z dostępnych w sieci skanerów online, a po przeskanowaniu dysku ponownie spróbuj zaktualizować antywirusa.

Bardzo często szkodliwe oprogramowanie jest uruchamiane przez samych użytkowników, którzy nieświadomie np. otwierają załączniki z poczty elektronicznej (nawet w przypadku maila pochodzącego od znanej nam osoby, mógł on zostać wygenerowany bez jej wiedzy) bądź instalują podejrzane oprogramowanie.

WAŻNE!

Jeśli z komputera korzysta dziecko (nawet, jeśli jest to jego własny komputer, a przede wszystkim – jeśli jest to komputer używany przez kilku domowników), warto rozważyć stworzenie dla niego osobnego konta użytkownika z ograniczonymi uprawnieniami. Nie będzie wówczas mogło np. samodzielnie instalować nowych programów, co zminimalizuje ryzyko zainfekowania komputera złośliwym oprogramowaniem. Zainstalowanie nowego programu będzie wymagało hasła administratora, którym dysponować będzie rodzic.

WAŻNE!

Ostrzeż dziecko, że obok wirusów zagrożeniem są również fałszywe alarmy lub żarty. Przekonaj dziecko, by nie „naprawiało" urządzenia bez twojej wiedzy i informowało cię o napotkanych problemach. Naucz dziecko, by nie „przeklikiwało" bez czytania wyskakujących na ekranie komunikatów – część z nich może być pytaniem o zgodę na instalację złośliwego oprogramowania. W przypadku stron wyświetlających podejrzane okienka z komunikatami o wygranym konkursie lub niespodziewanej nagrodzie, bezpieczniejsze będzie zamknięcie całej strony niż „przeklikiwanie" kolejnych okienek.

Niechciane reklamy

Spam to wszelkie niechciane lub niepotrzebne wiadomości przesyłane pocztą elektroniczną, zazwyczaj zawierające reklamę. Warto pamiętać, że dziecko często nie jest w stanie odróżnić reklamy od rzetelnej informacji, może być także podatne na obietnice nagród bądź darmowych gadżetów. Zdarza się, że w ten sposób są promowane produkty nieprzeznaczone dla dziecka. Co więcej – spam może być powiązany ze szkodliwym oprogramowaniem, instalującym się w komputerze po otwarciu reklamy.

Większość serwerów i programów pocztowych posiada filtr antyspamowy, automatycznie wykrywający wiadomości reklamowe. Dodatkowo, możliwe jest wskazanie nadawców, od których otrzymujemy spam – od tej chwili wiadomości tego typu zostaną skasowane lub trafią do osobnego folderu.

WAŻNE!

Nie należy odpisywać na e-maile będące spamem. Otrzymanie odpowiedzi (nawet jeśli jest to prośba o nieprzesyłanie reklam) może być potraktowane jako potwierdzenie, że adres jest aktywny i w konsekwencji może być powodem nadsyłania jeszcze większej liczby reklam.

Nasz adres e-mail może trafić do baz danych natarczywych reklamodawców, jeśli publikujemy go online lub podajemy, rejestrując się w różnych serwisach. Należy maksymalnie ograniczać podawanie adresu e-mail w internecie, a jeśli to niezbędne, najlepiej używać oddzielnego adresu, stworzonego specjalnie w celu rejestracji w serwisach, które mogą się wydawać podejrzane.

WAŻNE!

W przypadku reklam na stronach WWW możliwe jest zainstalowanie wtyczki/dodatku do przeglądarki internetowej, który zapobiegnie wyświetlaniu natarczywych reklam. Popularnym dodatkiem tego typu jest AdBlock+ dostępny dla większości przeglądarek internetowych.

Kontrola rodzicielska

Żadne z rozwiązań technicznych nie zastąpi uwagi rodzica i zdrowego rozsądku. Ale programy kontroli rodzicielskiej mogą ułatwić sprawowanie nadzoru nad dzieckiem – zarówno w przypadku korzystania z laptopa lub komputera stacjonarnego, jak i urządzeń mobilnych, takich jak tablet lub smartfon.

Ich podstawowe funkcje to:

- blokowanie dostępu do nieodpowiednich dla dzieci stron WWW,
- stałe lub czasowe ograniczanie dostępu do określonych programów i opcji urządzenia,
- monitorowanie i raportowanie.

W przypadku blokowania dostępu do stron WWW rodzic (administrator urządzenia) ma możliwość określenia, jakie kategorie stron nie powinny być wyświetlane, np.:

- erotyczne,
- ofensywne/agresywne,
- umożliwiające pobieranie plików z internetu,
- portale wideo,
- portale społecznościowe.

Inną metodą jest określenie listy stron, które rodzic uznaje za nieodpowiednie dla dziecka (tak zwana „czarna lista" stron). Równocześnie rodzic może określić słowa lub frazy, które użyte w treści strony spowodują jej zablokowanie.

Najwyższym poziomem zabezpieczenia jest zezwolenie na dostęp jedynie do konkretnych stron, które rodzic określił jako bezpieczne. To tak zwana „biała lista" stron.

Wprowadzenie **ograniczenia stałego lub czasowego dostępu** do określonych programów i opcji urządzenia daje rodzicom możliwość:

- określenia czasu (długości i częstotliwości) korzystania z komputera i internetu;
- określenia usług internetowych, z których dziecko nie będzie mogło skorzystać; blokada może zostać nałożona na: komunikatory, listy dyskusyjne, e-maile, pobieranie programów z internetu, pobieranie dokumentów;
- ograniczenia dostępu do funkcji komputera – blokada może dotyczyć np.: zapisu na pamięciach USB, dostępu do panelu sterowania, dostępu do panelu „Dodaj i usuń programy", funkcji „Uruchom z menu start".

Funkcja monitorowania i raportowania daje rodzicom możliwość kontroli zachowania dziecka. Programy kontroli rodzicielskiej umożliwiają zapisywanie obrazu zawartości monitora np. co minutę, 2 lub 10 minut. Ponadto zapisywane są strony, które dziecko przeglądało lub które zostały zablokowane przez oprogramowanie kontroli rodzicielskiej. Zrzuty ekranu lub wykaz zakazanych stron, które dziecko próbowało odwiedzić, rodzic może obejrzeć w panelu administracyjnym oprogramowania. Niektóre z aplikacji umożliwiają przesyłanie zarejestrowanych zdarzeń (obrazy i adresy WWW) na adres mailowy.

WAŻNE!

Programy ochrony rodzicielskiej dają możliwość utworzenia niezależnych profili dla różnych użytkowników – innego dla dziecka, innego dla osoby dorosłej. Panel administracyjny (pozwalający na zmianę ustawień) jest chroniony hasłem, dzięki czemu rodzic ma pewność, że dziecko korzysta tylko z przeznaczonego i ustawionego specjalnie dla niego profilu.

Kontrola rodzicielska może się odbywać dzięki autonomicznym programom, opcjom wyszukiwarki internetowej *(SafeSearch)* lub programom wbudowanym w system operacyjny.

System Windows udostępnia funkcję *Bezpieczeństwo rodzinne* pozwalającą m.in. na określenie jakie strony internetowe będą dostępne z konta dziecka, określenie limitów czasowych, ograniczenie dostępu do zainstalowanych aplikacji oraz raportowanie aktywności dziecka na komputerze (szczegółowe informacje dotyczące konfiguracji dostępne na stronach firmy Microsoft: **microsoft.com/pl-pl**).

URUCHOMIENIE KONTROLI RODZICIELSKIEJ KROK PO KROKU

Ograniczeniu dostępu dzieci do szkodliwych treści w internecie została poświęcona kampania edukacyjna „Chroń dziecko w sieci" prowadzona przez Fundację Dajemy Dzieciom Siłę i NASK. Na uruchomionej w ramach kampanii stronie dzieckowsieci.pl znaleźć można informacje dotyczące konkretnych narzędzi i zasad pozwalających na ograniczenie kontaktu dziecka ze szkodliwymi treściami w internecie. Dostępne są również filmy pokazujące krok po kroku, jak uruchomić ustawienia kontroli rodzicielskiej.

Kontrola rodzicielska Android:

Kontrola rodzicielska iOS:

Kontrola rodzicielska Windows 7:

Możliwe jest również ograniczenie dzieciom korzystającym z wyszukiwarki Google dostępu do nieodpowiednich treści. Filtr *SafeSearch* usuwa z wyników wyszukiwania obrazy, filmy i strony zawierające treści pornograficzne lub zawierające materiały tylko dla dorosłych. Włączenie filtra nie daje całkowitej gwarancji, że w wynikach wyszukiwania nie pojawią się niepożądane materiały, jednak zdecydowana większość materiałów nieprzeznaczonych dla dzieci powinna zostać odfiltrowana. By filtr pozostawał włączony, konieczna jest zgoda na używanie plików *cookies*, ich usunięcie może zresetować ustawienia filtra. Filtrowanie to nie obejmuje automatycznego blokowania treści przedstawiających przemoc.

Filtr *SafeSearch* można włączyć w *Ustawieniach wyszukiwania* wyszukiwarki zaznaczając opcję *Włącz filtr SafeSearch*. By uniemożliwić dziecku wyłączenie filtra, należy zablokować jego ustawienia poprzez zaznaczenie opcji *Zablokuj ustawienie filtra SafeSearch*.

O włączonym i zablokowanym filtrze *SafeSearch* informują kolorowe kule w prawym górnym rogu wyszukiwarki. Są widoczne nawet z daleka, mogą więc być dla rodzica informacją, w jakim trybie dziecko przegląda sieć (bezpiecznym lub pełnym).

Tryb bezpieczny w serwisie YouTube powoduje ukrycie filmów i komentarzy zawierających nieodpowiednie treści (oznaczonych w ten sposób przez użytkowników). By go uruchomić, należy w menu w prawym górnym rogu strony wybrać zakładkę *Tryb ograniczonego dostępu*. Uruchomienie tego trybu w serwisie YouTube dotyczy jedynie konkretnej przeglądarki w której został on włączony. Włączenie trybu bezpiecznego w YouTube powoduje również włączenie *SafeSearch* w wyszukiwarce Google.

Filtrowanie treści pod kątem materiałów, które są przeznaczone wyłącznie dla osób dorosłych, może odbywać się również na poziomie dostawcy internetu lub administratora lokalnej sieci komputerowej.

WAŻNE!

Żaden filtr, żadne oprogramowanie kontroli rodzicielskiej nie zapewnia stuprocentowej skuteczności. Ich uruchomienie nie oznacza, że można zapomnieć o siedzącym przy komputerze dziecku. Żaden z systemów kontroli rodzicielskiej nie jest w stanie zastąpić uwagi rodzica.

Bezpieczeństwo urządzeń mobilnych

Smartfon, tablet – te urządzenia coraz częściej zastępują komputer stacjonarny. Mają nad nim podstawową przewagę – można się z nimi swobodnie przemieszczać i korzystać z nich tam, gdzie jest dostępny bezprzewodowy internet, czyli praktycznie wszędzie.

Ogromna zaleta, jaką jest ich uniwersalność, jest równocześnie ich słabością – ze względu na możliwość instalowania dowolnych aplikacji, dotyczą ich te same zagrożenia, co komputera domowego – m.in. złośliwe oprogramowanie, kradzież danych. By dziecko mogło bezpiecznie korzystać z urządzeń mobilnych, trzeba zatroszczyć się o odpowiednią ich ochronę przed wirusami, szkodliwym oprogramowaniem oraz działaniem osób trzecich.

Aplikacje mobilne

To programy stworzone z myślą o urządzeniach mobilnych. Są one dostępne w tzw. sklepach/marketach związanych z producentem danego systemu operacyjnego. Wiele z nich jest bezpłatnych (np. wersje o ograniczonej funkcjonalności lub wyświetlające reklamy), część z nich jest płatna (od kilku do kilkudziesięciu, a nawet kilkuset złotych). Płatność zazwyczaj odbywa się przy użyciu karty kredytowej, z poziomu aplikacji Sklep Play można ustawić wymaganie potwierdzenia każdej transakcji finansowej kodem PIN.

WAŻNE!

Dokonując płatności kartą kredytową, warto upewnić się, że jest to jednorazowa transakcja (nie należy zezwalać urządzeniu na zapamiętanie danych karty). Dzięki temu dziecko chcące wykupić aplikację lub jej płatną część będzie zmuszone poprosić o to rodzica, nie mogąc samodzielnie dysponować kartą.

Najpopularniejszym systemem operacyjnym urządzeń mobilnych w Europie jest Android. Korzysta z niego blisko 70 proc. użytkowników tabletów i telefonów. Aplikacje na ten system dostępne są w sklepie Google Play (Sklep Play). Każda z nich została opisana przez producenta, widoczne są również oceny innych użytkowników, data aktualizacji oraz ocena treści, w Europie odwołująca się do kategoryzacji PEGI (więcej informacji o systemie PEGI str. 25). To informacja dla rodziców, czy dziecko powinno korzystać z określonej aplikacji. W opcjach aplikacji Sklep Play można na stałe włączyć kontrolę rodzicielską (zabezpieczoną PIN-em), ograniczającą pobieranie i kupowanie aplikacji lub treści w oparciu o klasyfikację wiekową.

Materiały kierowane do całej rodziny znaleźć można w kategorii *Familijne*. Są one oznaczone zieloną gwiazdką i opatrzone informacją o sugerowanym wieku odbiorców. Google wymaga, by każda z aplikacji i gier oznaczonych gwiazdką zawierała link do polityki prywatności, określającej w jaki sposób są zbierane i wykorzystywane informacje o użytkownikach.

Urządzenia mobilne firmy Apple wyposażone są w system operacyjny iOS, ich użytkownicy pobierają aplikacje ze sklepu App Store. By kontrolować z jakich aplikacji korzysta dziecko, można skorzystać z chmury rodzinnej. Dzięki wykorzystaniu tego narzędzia każdy zakup aplikacji przez dziecko musi być zatwierdzany przez rodzica z jego własnego urządzenia. Udostępniając swój tablet lub smartfon dziecku, można ograniczyć dostęp do konkretnych aplikacji oraz możliwości instalowania nowych. W tym celu należy w *Ustawieniach* skonfigurować opcję *Ograniczenia*.

Użytkownicy systemu operacyjnego Windows Phone mają do dyspozycji sklep o nazwie MarketPlace. Wśród kategorii aplikacji znajdziemy w nim m.in. dzieci + rodzina. Dostępna w witrynie Windows Phone usługa *Moja rodzina* umożliwia zarządzanie pobieraniem gier i aplikacji przez dzieci oraz ich klasyfikowanie. Posiadacze urządzeń z systemem Windows Phone 8 do wprowadzenia ograniczeń w smartfonie mogą wykorzystać wbudowaną funkcję *Kącik dziecięcy*. Dzięki niej można udostępnić dziecku tylko wybrane treści (gry, muzykę i filmy oraz inne aplikacje) w specjalnym trybie.

Zabezpiecz urządzenie dziecka przed wirusami i złośliwym oprogramowaniem
Złośliwe oprogramowanie może przejąć kontrolę nad urządzeniem lub danymi na nim zapisanymi. Zdarza się, że wirusy np. generują połączenia z numerami o podwyższonej płatności, wysyłają SMS-y na numery tego typu, przekazują informacje zawarte w urządzeniu bez zgody właściciela, wyświetlają niechciane reklamy. Mogą również śledzić za pomocą GPS położenie urządzenia, a więc i jego właściciela. Jeśli zauważymy, że urządzenie działa w inny niż zazwyczaj sposób (wszystkie procesy są spowolnione, pojawiają się nietypowe komunikaty) lub wysokość rachunku niespodziewanie wzrosła, warto sprawdzić, czy nie jest to wynikiem zainfekowania wirusem lub innym złośliwym oprogramowaniem. By chronić się przed takimi sytuacjami, trzeba pamiętać o zainstalowaniu programu antywirusowego. Oprócz skanowania urządzenia, wykrywania i likwidacji zagrożeń w oparciu o aktualne biblioteki wirusów, część programów posiada również zabezpieczenia antykradzieżowe.

Włącz oprogramowanie kontroli rodzicielskiej
Niektóre urządzenia przygotowane z myślą o dzieciach standardowo są wyposażone w programy ochrony rodzicielskiej. Warto to sprawdzić w momencie zakupu. Jeśli taka aplikacja nie jest zainstalowana w urządzeniu, można ją pobrać, również bezpłatnie, ze sklepu związanego z systemem operacyjnym urządzenia.

KONTROLA RODZICIELSKA W TELEFONIE I TABLECIE DZIECKA

Dla klientów Orange Polska dostępna jest usługa *Chroń Dzieci w Sieci* (chrondzieciwsieci.pl). Po zainstalowaniu aplikacji na urządzeniu dziecka, możliwe jest ustalenie dostępnych dla dziecka kategorii stron (ograniczenia oparte o „czarną" i „białą listę" – odpowiednio: zakazanych i dozwolonych adresów), określenie aplikacji mobilnych z których może korzystać, ustalenie godzin korzystania z internetu i aplikacji oraz kontrolę czasu z uwzględnieniem poszczególnych dnia tygodnia. Najprostsza konfiguracja aplikacji polega na określeniu wieku dziecka. Aplikację można również precyzyjnie dopasować do naszych potrzeb.
Osoby poszukujące jeszcze prostszych rozwiązań mogą sięgnąć po *Bezpieczny Starter* w sieci Orange. Wystarczy włożyć kartę SIM do urządzenia mobilnego, by wszystkie połączenia z tego urządzenia były chronione przed dostępem do niebezpiecznych dla dzieci stron WWW.

Korzystaj z filtrów przeglądarki
Aby zapewnić lepszą ochronę dziecku przed szkodliwymi treściami, warto włączyć i zablokować filtr *SafeSearch* w wyszukiwarce Google (str. 42).

Ustal z dzieckiem, że będzie pobierało aplikacje tylko z zaufanych źródeł
Instalowanie aplikacji pochodzących z oficjalnego sklepu, od sprawdzonego programisty, przetestowanych, opatrzonych licznymi komentarzami zmniejsza ryzyko ściągnięcia złośliwego oprogramowania. Zwróć uwagę dziecka, by zanim pobierze aplikację na telefon, zapoznało się z informacjami dotyczącymi producenta, liczby pobrań oraz opiniami testerów i innych użytkowników, a przede wszystkim by sprawdziło, do jakich danych aplikacja chce mieć dostęp i czy jest to uzasadnione jej funkcjonalnością. Jeśli aplikacja do odtwarzania muzyki żąda dostępu do wszystkich danych zapisanych w telefonie oraz aparatu i kamery, jej wymagania są podejrzanie szerokie. Ustal z dzieckiem, że będzie instalowało aplikacje pochodzące tylko z zaufanych źródeł lub będzie je instalowało w twojej obecności.

WAŻNE!

Również w dobrze znanych sklepach można natrafić na aplikacje zawierające złośliwe oprogramowanie. Udostępniane przez sklep aplikacje, pochodzące od zewnętrznych deweloperów są testowane zazwyczaj tylko automatycznie, korzystanie więc nawet wyłącznie z takich źródeł, nie gwarantuje stuprocentowego bezpieczeństwa.

Aktualizuj oprogramowanie
System operacyjny urządzeń mobilnych powinien być aktualizowany tak, jak system operacyjny komputera. Aktualizacje udostępniane przez producenta są reakcją na np. wykryte ataki cyberprzestępców. Systematycznie powinny być również instalowane aktualizacje aplikacji udostępniane przez ich producentów.

Usuwaj zbędne aplikacje
Nieużywane aplikacje należy systematycznie usuwać z telefonu, nawet jeśli z nich nie korzystamy, mogą pracować w tle spowalniając jego działanie. Nieaktualizowane aplikacje mogą narazić nas na utratę danych lub uszkodzenie urządzenia.

Telefon i tablet w szkole

Jeśli zgadzasz się na to, by dziecko zabierało do szkoły telefon, smartfon lub tablet, sprawdź, czy używanie tego typu urządzeń nie jest zabronione lub w jakiś sposób ograniczane przez regulamin szkoły. Drugą istotną kwestią jest ochrona prywatności – zarówno dziecka, jak i innych osób.

Zwróć uwagę dziecka na fakt, że urządzenia te nie służą do zabawy w trakcie lekcji. Na czas zajęć telefon powinien być wyłączony lub wyciszony.

Przypomnij dziecku, że korzystanie z takich urządzeń rządzi się również podstawowymi zasadami kultury i np. nie wolno filmować nikogo ani robić mu zdjęć, jeśli nie wyraża na to zgody.

Porozmawiaj z dzieckiem o udostępnianiu telefonu innym osobom, w tym jego kolegom. Dostęp do urządzenia oznacza również dostęp do zawartych w nim informacji, którymi właściciel telefonu niekoniecznie chce się dzielić z innymi.

WAŻNE!

Pamiętaj, że drogie urządzenie może być przedmiotem zawiści rówieśników dziecka. Rozważ, czy twoje dziecko rzeczywiście wykorzysta wszystkie funkcje najnowocześniejszego smartfona i czy posiadanie go nie narazi dziecka na nieprzyjemne sytuacje (np. próby kradzieży) lub nie wpłynie negatywnie na jego relacje z rówieśnikami.

Blokowanie dostępu

Dostęp do telefonu, smartfona lub tabletu można zabezpieczyć hasłem, gestem (wzorem), kodem PIN lub (w niektórych modelach) odciskiem palca. Razem z dzieckiem sprawdź, jaki sposób blokowania jest dostępny w jego telefonie, dzięki czemu w razie pozostawienia urządzenia bez opieki bądź utraty kontroli nad nim niepowołane osoby będą miały utrudniony dostęp do jego zawartości. Pamiętaj, by hasło, symbol lub kod nie były zbyt oczywiste, zwróć również uwagę dziecka na fakt, że są to informacje bezwzględnie poufne i nie powinno się nimi dzielić z rówieśnikami.

WAŻNE!

Kilkukrotne nieudane próby odblokowania ekranu urządzenia mogą doprowadzić do jego zablokowania, co z kolei może oznaczać konieczność przywrócenia ustawień fabrycznych i utratę zapisanych danych.

Mikropłatności

Mikropłatności służą do dokonywania opłat za np. usługi online, doładowanie konta w grze, zakup pakietów internetowych. Popularnymi formami mikropłatności są SMS-y o podwyższonej płatności oraz wirtualne portfele.

Numery, na które wysyłane są SMS-y o podwyższonej płatności, zaczynają się od cyfr 7 lub 9. Po wysłaniu SMS-a pod wskazany numer użytkownik otrzymuje w zamian kod aktywacyjny, który umożliwia mu korzystanie z usługi, np. transmisji lub gry. Zdarza się, że dzieci nie zwracają uwagi na koszty wiadomości SMS o podwyższonej płatności, które są wielokrotnie droższe niż zwykła wiadomość tekstowa. Dlatego warto przekonać dziecko, by nie dokonywało tego rodzaju płatności bez zgody rodzica. SMS-y o podwyższonej płatności można zablokować, używając aplikacji kontroli rodzicielskiej lub u operatora sieci komórkowej.

WAŻNE!

Przy numerze zaczynającym się od cyfry 7, kolejna cyfra po niej jest informacją o koszcie SMS-a. Analogicznie, w przypadku numeru SMS-a zaczynającego się od cyfry 9 – dwie kolejne cyfry ujawnią cenę netto SMS-a.

Zwróć uwagę dziecka na fakt, że oszuści internetowi często wykorzystują SMS-y o podwyższonej płatności, a wysłanie jednego SMS-a może oznaczać zgodę na systematyczne obciążanie rachunku telefonicznego lub konta przedpłaconego opłatą. Decydując się na udział w konkursie, należy zapoznać się z jego regulaminem, a jeśli zasady okażą się niejasne – lepiej z niego zrezygnować.

W przypadku usług sieciowych wykorzystywane są również wirtualne portfele. Korzystanie z nich wymaga założenia konta, prowadzonego przez firmę oferującą usługę (np. grę). Konto jest zasilane SMS-ami lub kartą kredytową, a realne pieniądze są zazwyczaj przeliczane na jednostki obowiązujące w grze. Z wirtualnych portfeli mogą korzystać osoby niepełnoletnie, za zgodą rodziców lub opiekunów prawnych. Niektórzy producenci oferują również ochronę rodzicielską, która pozwala na pełny wgląd w transakcje dokonywane przez dziecko.

Podawanie numeru telefonu w internecie

Warto przekonać dziecko, by nigdy nie podawało w internecie swojego numeru telefonu. Zdarza się, że popularne portale zachęcają swoich użytkowników do publikowania numeru telefonu. Może to jednak stanowić istotne zagrożenie dla prywatności dziecka, narażając je na niechciane kontakty ze strony nieznajomych lub osób, które mają wobec niego złe intencje. Numer, który raz pojawił się w sieci, może zostać skopiowany przez innych użytkowników – łatwo więc utracić kontrolę nad tym, gdzie i w jakim kontekście będzie widoczny.

Innym zagrożeniem jest wykorzystywanie numeru telefonu podanego w trakcie rejestracji w konkretnym serwisie. Może to oznaczać wyrażenie zgody na np. cykliczne przesyłanie płatnych wiadomości, których koszt obciąży użytkownika telefonu. By tego uniknąć, należy się zapoznać szczegółowo z regulaminem serwisu.

WAŻNE!

Warto uświadomić dziecku, że w sieci pojawiają się różnego rodzaju fałszywe konkursy, które kuszą atrakcyjnymi nagrodami, a w rzeczywistości służą wyłudzeniu danych osobowych użytkowników.

ICE

ICE (ang. *In Case of Emergency*, w nagłym wypadku) to oznaczenie numeru telefonu, będące informacją np. dla ratowników medycznych, z kim powinni się skontaktować w razie np. wypadku. Skrót ten należy umieścić w opisie numeru telefonu najbliższej osoby w książce adresowej telefonu. Jeśli takich osób jest więcej, można oznaczyć je dodatkową cyfrą, np. ICE1 Mama, ICE2… itd.

Ze względu na fakt, że większość użytkowników telefonu korzysta z blokady ekranu, na wypadek nagłej sytuacji warto mieć przy sobie również kartę ICE, np. formatu wizytówki, zawierającą imię, nazwisko i numer kontaktowy osoby, która powinna być powiadomiona. To ważne, również ze względu na dodatkowe informacje, jakie ratownicy medyczni mogą w ten sposób uzyskać, np. na temat przyjmowanych leków lub alergii.

IMEI

Unikalnym numerem IMEI (ang. *International Mobile Equipment Identity*) jest opatrzone każde urządzenie mobilne, które ma wbudowany moduł GSM, a więc wszystkie telefony i smartfony oraz część tabletów i laptopów. Numer ten jest używany do identyfikacji urządzenia przez sieć telefoniczną. Numer IMEI jest zapisany na obudowie urządzenia, można go również sprawdzić po wybraniu sekwencji klawiszy *#06# lub w zakładce „Informacje o urządzeniu". Dzięki temu numerowi można np. zablokować skradziony telefon, uniemożliwiając korzystanie z niego, nawet jeśli zostanie użyta inna karta SIM. Wyjątek od tego stanowią sytuacje, gdy przestępca zmieni w telefonie numer IMEI.

WAŻNE!

Pamiętaj, by przechowywać dokumenty zawierające numer IMEI, mogą one być potrzebne w przypadku kradzieży urządzenia. Jeśli nie masz takich dokumentów, zanotuj numer IMEI wyświetlony na ekranie urządzenia.

Blokowanie usług

Dziecko (z powodu braku wiedzy, niedojrzałości społecznej) może nie być w stanie racjonalnie zarządzać wszystkimi funkcjami swojego urządzenia mobilnego. Dlatego zablokuj usługi, które nie są niezbędne dziecku, a mogą je narazić na dodatkowe koszty lub niebezpieczeństwo.

Co można zablokować?

- Usługi o podwyższonej płatności. Blokada dotyczy określonych numerów o podwyższonej płatności, a także wiadomości SMS i MMS. Usługa jest bezpłatna u wszystkich operatorów. Blokadę można wprowadzić również w aplikacji kontroli rodzicielskiej.
- Alternatywą dla blokady jest ustanowienie limitu kosztów połączeń do określonych numerów, w tym numerów o podwyższonej płatności.

- Połączenia wychodzące do określonych numerów. Blokada dostępna u operatora lub poprzez zmianę ustawień telefonu.
- Połączenia przychodzące z konkretnych numerów, np. od osób, które nękają dziecko. Blokada dostępna jest z poziomu telefonu.
- Połączenia przychodzące z numerów zastrzeżonych (z ukrytą prezentacją numeru).
- Dostęp do stron ze szkodliwymi treściami. Blokadę dostępu do stron z treściami dla dorosłych możemy ustanowić za pomocą programów kontroli rodzicielskiej.

W sprawowaniu opieki nad dzieckiem korzystającym z nowych technologii mogą pomóc programy do kontroli rodzicielskiej (str. 40). Pozwalają na kontrolę wydatków telefonicznych, chronią przed szkodliwymi treściami zawierającymi np. przemoc lub pornografię, dzięki nim można zablokować wiadomości SMS i połączenia na numery o podwyższonej opłacie, włączyć ograniczenia czasowe rozmów, zablokować dostęp do niektórych aplikacji lub internetu, monitorować zawartość i treść wiadomości, a także logi GPS.

WAŻNE!

Pamiętaj, że żaden program nie jest w stanie zastąpić uwagi i rozsądku rodziców.

Dostęp do internetu

Urządzenia mobilne zostały zaprojektowane z myślą o stałym podłączeniu do internetu. Transmisja danych jest wykorzystywana nawet wtedy, kiedy użytkownik nie przegląda stron lub swojej poczty. Z przesyłu danych korzystać może zarówno system operacyjny telefonu (np. pobierając aktualizacje), jak i poszczególne aplikacje – nie tylko aktualizując się, ale i pobierając bieżące informacje (np. aplikacje typu pogoda, mapy). O ile w przypadku łączenia się smartfona z siecią poprzez Wi-Fi ryzykujemy zazwyczaj tylko szybsze rozładowanie się baterii, w przypadku przesyłu danych pakietowych (jeśli nie został wykupiony specjalny pakiet internetowy) koszty ich transmisji zostaną uwzględnione w rachunku lub pobrane z konta *prepaid*. Może to być dość przykrą niespodzianką, szczególnie w przypadku wyjazdu za granicę, ponieważ transmisja danych będzie rozliczana w ramach roamingu.

Porozmawiaj z dzieckiem o tym, jak uchronić się przed dodatkowymi kosztami korzystania z internetu (jeśli nie korzysta z abonamentu umożliwiającego nieograniczone przesyłanie danych):

1. Wyłączenie przesyłania danych pakietowych. To najskuteczniejszy sposób ograniczenia niespodziewanych kosztów. W telefonach z Androidem możemy się wspomóc aplikacjami, które pozwalają na szybkie włączenie i wyłączenie dostępu do internetu, np. APNDroid lub APN OnOff. Przesył zawsze można włączyć, np. w celu pobrania MMS-a.

2. Domowa sieć Wi-Fi. Nie warto całkowicie rezygnować z połączenia z internetem – aktualizacje systemu i aplikacji często są istotne ze względu na bezpieczeństwo smartfona. Można je pobierać, korzystając z domowej sieci Wi-Fi. Jeśli w telefonie ustawimy automatyczne łączenie się z domową siecią Wi-Fi, podczas wysyłania i odbierania danych urządzenie spróbuje w pierwszej kolejności użyć tego połączenia i nie będzie zużywało transferu danych sieci komórkowej.
3. Wyłączenie zadań w tle. Niektóre aplikacje, nawet nieużywane, mogą korzystać z przesyłu danych. Wykorzystanie ich transferu można ograniczyć poprzez wyłączenie niepotrzebnych programów działających w tle. Warto przeanalizować ustawienia telefonu i poszczególnych aplikacji, a następnie zablokować dostęp do internetu w tych, z których nie korzystamy na bieżąco.
4. Zmiana ustawień synchronizacji poczty e-mail. Odbierana przez smartfon poczta e-mail wymaga systematycznego łączenia się z internetem, by pobrać nowe wiadomości. Można określić częstotliwość synchronizacji smartfona ze skrzynką pocztową lub dokonywać jej samemu, w dogodnym dla nas czasie.
5. Wykorzystanie kompresji danych. Aby zmniejszyć przesył danych, warto korzystać z przeglądarek internetowych, które zmniejszają rozmiar stron internetowych i tym samym zużycie transferu niezbędnego do ich załadowania.

Co telefon wie o swoim użytkowniku?

Smartfony powoli zaczynają zastępować komputery. Angażując urządzenia mobilne w każdy aspekt naszego życia, warto uświadomić sobie fakt, że przechowując nasze różnorodne, często poufne dane, stają się one źródłem informacji o nas. Nawet najprostszy telefon zawiera sporo informacji na nasz temat: spis kontaktów, rejestr rozmów, odebrane i wysłane SMS-y, zdjęcia. W bardziej zaawansowanych urządzeniach mogą to być np. pliki pobrane jako załączniki do poczty elektronicznej lub numery karty kredytowej zapisane w aplikacjach. Niebezpieczeństwo rodzić mogą również notatki zawierające PIN-y lub np. hasła do kont. Warto pamiętać, że zagrożeniem jest nie tylko utrata danych i problemy z ich odtworzeniem, ale przede wszystkim – dostęp do nich niepowołanych osób.

WAŻNE!

Zwróć uwagę dziecka, by nie wykorzystywało w telefonie funkcji zapamiętywania hasła do serwisów i usług sieciowych – w przypadku przejęcia telefonu przez inną osobę będzie ona miała swobodny dostęp np. do konta pocztowego naszego dziecka.

Dane gromadzone w usługach internetowych

Warto pamiętać, że jeśli coś w internecie jest za darmo, to najprawdopodobniej my stajemy się towarem. Firmy internetowe, udostępniając bezpłatnie szereg usług, wykorzystują informacje na temat użytkowników, np. przekazując je innym firmom w celach reklamowych. Dzięki temu np. wyszukiwanie stron poświęconych danym technicznym tabletów skutkuje wyświetlaniem przez kilka kolejnych dni reklam tabletów na stronach informacyjnych.

WAŻNE!

Warto również zdać sobie sprawę z tego, że wyniki wyszukiwania mogą nie być obiektywne i różnić się pomiędzy komputerami, ponieważ zostały dopasowane do naszych preferencji ustalonych na podstawie historii surfowania i plików cookies. To swego rodzaju bańka informacyjna, która uniemożliwia nam dostęp do pełnych zasobów internetu.

- Przekonaj dziecko, by z ostrożnością podchodziło do aplikacji i stron, które żądają informacji osobistych, nikt nie może mieć pewności, w jaki sposób będą przechowywane i używane jego dane.
- Naucz dziecko, że instalować należy tylko te aplikacje, których się później będzie używać. Aplikacja nieużywana i nieaktualizowana może posiadać luki w zabezpieczeniach i stanowić zagrożenie dla urządzenia i danych.
- By zainstalować część aplikacji pochodzących z nieoficjalnych źródeł, konieczny jest tzw. *jailbreak*, czyli wyłączenie ograniczeń ustalonych przez producenta systemu. Taka operacja wyłącza zabezpieczenia urządzenia lub zmienia działanie funkcji związanych z bezpieczeństwem. W konsekwencji telefon może utracić gwarancję, może też być narażony na ingerencję osób trzecich.
- Jeśli tylko jest taka możliwość, należy korzystać z połączeń szyfrowanych (https://) uniemożliwiających przechwycenie danych przez osoby trzecie.
- Przypomnij dziecku o stosowaniu różnorodnych i silnych haseł.
- Pamiętaj o programach chroniących urządzenie mobilne przed wirusami i innym złośliwym oprogramowaniem.

Geotagowanie

Geotagowanie to inaczej umieszczanie informacji dotyczących lokalizacji danej osoby lub obiektu. Dzięki urządzeniom mobilnym wyposażonym w GPS oznaczanie pozycji może odbywać się automatycznie. Geotagowanie jest wykorzystywane np. przez portale społecznościowe, które informują nas, że znana nam osoba odwiedziła jakieś miejsce. Warto się zastanowić, czy chcemy, by informacja o tym, gdzie przebywa nasze dziecko, była dostępna w sieci. Śledzenie kolejnych lokalizacji dodanych w portalu społecznościowym łatwo pozwala ustalić miejsca, w których ono systematycznie bywa.

Dodatkowym aspektem jest geotagowanie zdjęć (również wykonanych tabletem lub smartfonem). Jeśli korzystamy z tej opcji, w pliku zdjęcia zostaje zaszyta informacja określająca miejsce jego wykonania. W funkcję geotagowania zdjęć mogą być wyposażone również niektóre aparaty fotograficzne. O ile bardzo ułatwia to katalogowanie np. fotografii z podróży, o tyle w przypadku zdjęć rodzinnych może już być zagrożeniem – upubliczniając zdjęcia robione np. we własnym ogrodzie wraz ze współrzędnymi zapisanymi przez GPS, jasno określamy miejsce, w którym mieszkamy.

Wi-Fi w domu

Domowa sieć Wi-Fi pozwala na wygodne korzystanie z internetu przy użyciu urządzeń przenośnych, takich jak laptop, tablet lub smartfon. Konieczne jest jednak jej zabezpieczenie przed dostępem niepowołanych osób. Pozostawienie sieci bez ochrony to przyzwolenie na korzystanie z naszego routera przez nieznane nam osoby, co więcej – niezabezpieczony router może również oznaczać ryzyko kradzieży danych przesyłanych przez sieć (np. loginy i hasła) bądź instalowania bez naszej wiedzy złośliwego oprogramowania na komputerach korzystających z Wi-Fi.

- Zmień nazwę sieci ze standardowej (zazwyczaj określonej typem urządzenia lub usługi) na unikalną, własną. Pozostawienie nazwy fabrycznej to informacja dla włamywacza, jakim urządzeniem się posługujemy i na jakie formy ataku jest ono podatne.
- Zablokuj możliwości dostępu do ustawień routera/modemu od strony internetu (szczegóły znajdziesz w instrukcji).
- Zadbaj o silne hasło dostępu do sieci. Powinno się ono różnić od hasła do routera oraz innych usług sieciowych. Więcej na temat haseł – str. 16.
- Używaj szyfrowania w standardzie WPA2, które jest obecnie najlepszym sposobem na zabezpieczenie przesyłu danych w domowej sieci komputerowej.

WAŻNE!

Twoje dziecko może mieć wpływ na bezpieczeństwo i jakość działania domowej sieci bezprzewodowej. Zastanów się, czy przekazać mu dane pozwalające na dostęp do sieci Wi-Fi, czy też jedynie zapisać je w urządzeniach, z których dziecko korzysta. Jeżeli zdecydujesz się na pierwsze rozwiązanie, powiedz mu, by nie zmieniało ustawień sieci bez twojej zgody oraz nie udostępniało nazwy i hasła do Wi-Fi osobom trzecim, np. kolegom.

Publiczne sieci Wi-Fi

Bezprzewodowy internet udostępniany jest na terenie szkół, bibliotek, galerii handlowych i kawiarni, a coraz częściej nawet w parku lub na ulicy. Zazwyczaj sieci te są ogólnodostępne, a korzystanie z nich nie wymaga podawania hasła. Nie powinniśmy traktować ich jednak jako bezpiecznych – dużo łatwiej w nich o możliwość przechwycenia danych, przekierowania na strony ze szkodliwymi treściami bądź zainfekowania urządzenia wirusem.

1. Zwróć uwagę dziecka, by używając ogólnodostępnego Wi-Fi, nie korzystało z serwisów wymagających logowania (poczta, serwisy społecznościowe) lub podawania danych osobowych. Jeśli się na to decyduje, to tylko w sytuacji, kiedy dane przekazywane są w postaci zaszyfrowanej (protokół HTTPS – informacja w oknie adresu przeglądarki, widoczna miniaturowa kłódka).
2. Wyposaż urządzenie dziecka w filtry kontroli rodzicielskiej, dzięki którym będzie chronione przed szkodliwymi treściami, takimi jak np. pornografia. Pamiętaj jednak, że filtry nie dają stuprocentowego zabezpieczenia przed materiałami tego typu.
3. Upewnij się, że w urządzeniu korzystającym z publicznej sieci, nawet tylko w celu przeglądania stron, jest włączona zapora sieciowa (*firewall*) oraz zaktualizowany program antywirusowy.
4. Przekonaj dziecko, by wyłączało Wi-Fi w swoim telefonie, jeśli z niego nie korzysta i usuwało zapamiętane przez urządzenie sieci publiczne. Jeśli sieć taka została zapamiętana w danym urządzeniu, może się ono z nią połączyć, nawet bez wiedzy użytkownika. Dodatkową zaletą wyłączonego Wi-Fi jest dłuższy czas pracy bez ładowania baterii.

Kopie zapasowe

Utrata danych zapisanych na urządzeniu mobilnym należącym do dziecka (zdjęć, plików muzycznych, ale i zawartości książki telefonicznej) może być bolesna, nawet jeśli mają one jedynie wartość sentymentalną. Upadek lub zalanie urządzenia wodą, uszkodzenie karty pamięci może oznaczać, że dostęp do danych zapisanych w urządzeniu będzie niemożliwy (lub – ze względu na koszty odzyskiwania danych – nieopłacalny).

Większość producentów urządzeń mobilnych udostępnia swoim użytkownikom bezpłatne wirtualne dyski, służące m.in. do tworzenia kopii zapasowych zawartości telefonu i wszystkich indywidualnych ustawień. Kopia zapasowa może być również przydatna w przypadku zmiany telefonu na nowy – pozwoli przenieść zawartość starego urządzenia i większość jego ustawień. Przestrzeń dyskową oferują również producenci aplikacji dla urządzeń mobilnych.

Konto w tzw. chmurze (przestrzeni dyskowej dostępnej w internecie) umożliwia umieszczenie tam naszych zdjęć, nagrań audio i wideo, synchronizację kontaktów i kalendarza pomiędzy różnymi urządzeniami (również stacjonarnymi), jak i (po zalogowaniu się) dostęp do jego zawartości z każdego urządzenia podłączonego do internetu. Do chmury dostęp jest możliwy za pośrednictwem przeglądarki internetowej, wygodniejsze jest jednak zainstalowanie specjalnej aplikacji do zarządzania naszą przestrzenią dyskową i synchronizowania danych. Zawartość chmury można udostępniać znajomym poprzez portale społecznościowe lub e-mail.

WAŻNE!

Zwróć uwagę dziecka na fakt, że zawartość jego konta w chmurze jest bezpieczna do momentu, dopóki nie udostępni innym osobom hasła.

NFC i płatności zbliżeniowe

Near Field Communication (komunikacja bliskiego zasięgu) pozwala na przekazywanie plików lub wiadomości dzięki zetknięciu ze sobą dwóch urządzeń (wyposażonych w moduł NFC). Technologia ta pozwala np. na zakodowanie w telefonie biletów, kart wstępu, udostępnianie informacji o miejscu, w którym się znaleźliśmy – wystarczy przyłożyć smartfon do umieszczonego w widocznym miejscu taga NFC (naklejka lub pole opatrzone tym skrótem), by nasz smartfon odczytał zawartą w nim informację i wykonał zapisane w tagu działanie. Najpopularniejszą usługą wykorzystującą NFC są płatności dotykowe (zamiast karty do terminalu przykładamy smartfon). Jeśli zdecydujemy się udostępnić dziecku tę funkcję (jako kartę przedpłaconą – dokonywanie płatności wymaga zasilenia wcześniej konta powiązanego z kartą SIM), wyjaśnijmy mu, że ma do czynienia z *de facto* kartą płatniczą. Pomimo zapewnień o bezpieczeństwie tej technologii (dokonując płatności, cały czas mamy telefon w ręku), warto wykorzystywać ją z rozwagą – nie udostępniać telefonu kolegom, nie pozostawiać aparatu w miejscach publicznych. Środki dostępne na koncie oraz historię ostatnich transakcji można sprawdzić w specjalnej aplikacji powiązanej z kartą, uruchamianej wraz z aktywacją karty. Potwierdzenie transakcji PIN-em jest niezbędne powyżej kwoty 50 zł.

WAŻNE!

Zagubienie lub kradzież karty SIM NFC należy jak najszybciej zgłosić – z telefonu Orange pod numerem *100, z telefonu innego operatora/telefonu stacjonarnego lub spoza granic Polski – pod numerem +48 510 100 100. Oprócz tego, tak jak w przypadku kart płatniczych, należy również poinformować bank obsługujący naszą kartę.

Bluetooth

Bluetooth pozwala na bezprzewodową wymianę informacji z innymi urządzeniami na niewielkie odległości. Technologia ta może być wykorzystywana np. do podłączenia zestawu głośnomówiącego do telefonu, komunikację z zewnętrznym urządzeniem GPS. Jednocześnie systematycznie pojawiają się informacje na temat odkrywania nowych metod włamań za pośrednictwem Bluetootha, polegających np. na wydobywaniu zawartości urządzenia, a nawet generowaniu kosztownych połączeń. Część z tych ataków wykorzystuje luki w oprogramowaniu, część wymaga współpracy ze strony użytkownika urządzenia, np. zaakceptowania próby sparowania urządzeń pod pozorem akceptowania cyfrowej wizytówki. Ze względu na niewielki zasięg Bluetootha do prób włamania się do urządzenia może dojść szczególnie w miejscach publicznych. Najskuteczniejszą metodą zapobiegania tego typu przypadkom jest po prostu wyłączenie łączności Bluetooth, jeśli z niej nie korzystamy.

WAŻNE!

Przekaż dziecku, by nie akceptowało prób sparowania urządzenia z innym urządzeniem, jeśli go nie zna, a w przypadku natrętnego ich powtarzania – zamknęło łączność Bluetooth.

Utrata telefonu lub tabletu

Ze względu na łatwość utraty urządzeń mobilnych (zagubienie, kradzież), większość producentów wyposaża je w aplikacje ułatwiające odszukanie urządzenia lub utrudniające sprzedaż skradzionego przedmiotu, a przede wszystkim – pozwalające na zdalne usunięcie prywatnych danych (zdjęcia, kontakty, SMS-y). Aplikacje służące do odzyskiwania urządzenia są w stanie zdalnie włączyć sygnał dźwiękowy z maksymalną głośnością (przydatne, jeśli np. gdzieś zawieruszy się nam wyciszony telefon), umożliwiają śledzenie urządzenia w terenie, pokazując na mapie miejsce, w którym się znajduje, są w stanie wyświetlić na jego ekranie tekst lub numer telefonu, z którym powinien się skontaktować znalazca, ostatecznie – blokują urządzenie, ograniczając możliwość korzystania z niego i jego sprzedaży. Obok narzędzi oferowanych przez producentów urządzeń mobilnych dostępne są również inne, niezależne aplikacje o podobnej lub szerszej funkcjonalności.

WAŻNE!

Aby mieć szansę wykorzystania tego typu aplikacji, konieczne jest powiązanie naszego urządzenia z kontem internetowym (producenta urządzenia lub aplikacji), aktywacja aplikacji i jej skonfigurowanie. Trzeba to jednak zrobić, zanim dojdzie do utraty urządzenia, warto więc być przewidującym.

W przypadku utraty urządzenia należy się zalogować z dowolnego dostępnego komputera, tabletu lub telefonu na konto, z którym zostało powiązane zagubione urządzenie, a następnie wskazać je na liście (jeśli na koncie zostało zarejestrowane więcej niż jedno urządzenie). Otworzy nam to dostęp do funkcji, które pomogą w odszukaniu urządzenia, w tym włączenie sygnału dźwiękowego, lokalizacji urządzenia na mapie, usuwanie danych, blokowanie urządzenia. Warto pamiętać, że uruchomienie sygnału dźwiękowego w sytuacji, kiedy wiemy, że telefon został skradziony, będzie dla złodzieja komunikatem, że urządzenie jest śledzone i może spowodować całkowite jego wyłączenie. Trzeba pamiętać również, że usunięcie prywatnych danych i wyzerowanie telefonu do ustawień fabrycznych (w zależności od konfiguracji) może również usunąć aplikację słu-

żącą do śledzenia naszego urządzenia lub odciąć je od konta, z którym było powiązane, należy więc tę możliwość traktować jako ostateczność. W zależności od systemu operacyjnego może się również okazać, że zablokowanie urządzenia nie pozwala na jego śledzenie. Aplikacje antykradzieżowe nie zadziałają, jeśli urządzenie zostanie wyłączone, nie będzie miało dostępu do sieci lub już przywrócono w nim ustawienia fabryczne. Warto więc pamiętać, że aplikacje tego typu są najskuteczniejsze bezpośrednio po utracie (kradzieży) urządzenia, a wraz z upływem czasu szanse na jego odzyskanie spadają.

WAŻNE!

W przypadku telefonu (lub tabletu, w którym znajduje się karta SIM), pamiętaj, by kradzież karty SIM lub jej zagubienie zgłosić operatorowi telefonicznemu. Dzięki temu zostanie ona zablokowana, co uniemożliwi np. prowadzenie rozmów telefonicznych na twój rachunek.

Jeśli operatorem utraconego telefonu jest Orange, kartę można zablokować:

- w aplikacji **Mój Orange**: wejdź w **Podsumowanie**--> **wokół twojej oferty**, wybierz **Włącz blokadę kradzieżową** (do zablokowania karty SIM niezbędny będzie kod abonencki),
- na stronie **orange.pl**, zakładka **Mój Orange**, po zalogowaniu w zakładce **Podsumowanie**, sekcja **Wokół twojej oferty**, wybierz **Włącz blokadę kradzieżową** (do zablokowania karty SIM niezbędny będzie kod abonencki),
- pod numerem *100 (z telefonu Orange) lub 510 100 100,
- bezpośrednio w salonie Orange.

Kradzież telefonu powinna zostać zgłoszona policji. Zgłaszając kradzież na posterunku, trzeba zabrać ze sobą dokument tożsamości oraz np. umowę, w której został wpisany numer IMEI skradzionego urządzenia (więcej informacji na str. 48). Ze sporządzonym przez policję protokołem kradzieży i dokumentami potwierdzającymi, do kogo należał telefon, należy się udać do salonu naszego operatora, gdzie dzięki numerowi IMEI może on zostać zablokowany również u innych operatorów.

Konsole do gier

Wielu graczy wybiera konsole do gier – wyspecjalizowane urządzenia skonstruowane z myślą o grach wideo. Obsługa takiego sprzętu jest prostsza, gra bywa też bardziej atrakcyjna niż w przypadku komputera – wcielając się w postać bohatera, piosenkarza lub sportowca, korzystamy nie z myszki i klawiatury, ale pada, maty i kontrolerów ruchu. Odrębną kategorią są konsole przenośne umożliwiające granie poza domem (np. na wakacjach, w drodze do szkoły).

Konsole stacjonarne są podłączane do monitora lub telewizora. Większość posiada napęd Blu-ray (lub DVD, CD), złącze HDMI, Wi-Fi do łączenia się z internetem. Konsole nie tylko dają możliwości przeglądania stron internetowych, ale mogą też służyć do oglądania zdjęć, filmów i słuchania muzyki. Gros urządzeń umożliwia też podłączenie czujnika ruchu, dzięki któremu grę kontrolujemy ruchami ciała.

Platformy do rozgrywek elektronicznych mogą łączyć się z wieloma serwisami internetowymi, umożliwiając pobieranie aplikacji i korzystanie z portali społecznościowych, czatów i wideokonferencji. Pozwalają również na wspólną grę i umożliwiają komunikowanie się z innymi graczami. Najnowsze modele oferują również możliwość transmitowania w czasie rzeczywistym (*streaming*) swoich rozgrywek na popularnych serwisach online.

Opłaty za gry

- Nierzadko gry przeznaczone na konsole są droższe niż ich wersje na komputery osobiste.
- Granie na konsoli online może być dodatkowo płatne. W takich sytuacjach konieczne jest wykupienie abonamentu i założenie konta na wybranej platformie.
- Dodatki do gier, dodatkowe poziomy również nierzadko mogą być płatne. W przypadku korzystania z zabezpieczeń kontroli rodzicielskiej możliwe jest ustawienie limitu wydatków dla naszego konta.
- Kontrolowanie wydatków dziecka jest również możliwe poprzez użycie kodów przedpłaty (nie wymagają one płatności kartą kredytową). Kody przedpłaty zakupione w zwykłym sklepie można wykorzystać zarówno w przypadku konsoli, jak i komputera.

Gry a bezpieczeństwo dziecka

Konsole są zintegrowane z usługami internetowymi, dzięki czemu nawet dzieci mogą pobierać dodatkowe treści, kontaktować się z innymi użytkownikami i udostępniać swoje dane. Producenci urządzeń do grania oferują różne formy kontroli rodzicielskiej – warto z nich skorzystać. Często punktem odniesienia jest wiek graczy, dający rodzicom możliwość decydowania o doborze metody zabezpieczeń.

- Zapoznaj się z instrukcją dotyczącą zabezpieczeń dołączoną do urządzenia. Zajrzyj na stronę producenta poświęconą kontroli rodzicielskiej.
- Poznaj zasady korzystania z wybranej przez dziecko gry i sprawdź, w jaki sposób można zgłaszać nadużycia innych graczy.
- Zadecyduj, w co może grać twoje dziecko i wprowadź te ograniczenia do urządzenia.
- Ustal czas korzystania z konsoli w ciągu dnia, zabezpiecz dostęp do profilu na platformie hasłem.
- Kontroluj dostęp do internetu i skonfiguruj ustawienia prywatności konta.
- Sprawdź dopuszczalny wiek użytkownika. Wiele gier popularnych wśród najmłodszych jest przeznaczonych dla młodzieży lub tylko dla osób dorosłych.

Telefon stacjonarny

Mimo triumfu telefonii komórkowej telefon stacjonarny wciąż jest dobrym wyjściem dla osób, które szukają prostych rozwiązań.

- **Identyfikowanie numeru**
  Dzięki usłudze identyfikacji numeru rozmówcy na wyświetlaczu aparatu widoczny jest numer osoby dzwoniącej. Zawsze też można sprawdzić, kto dzwonił podczas naszej nieobecności. Numer osoby dzwoniącej będzie się wyświetlał zawsze, poza połączeniami z telefonów o zastrzeżonych numerach.

WAŻNE!

Warto przestrzec dzieci przed odbieraniem połączeń nieznanych lub anonimowych. Można też rozważyć zastosowanie funkcji blokowania numeru w przypadku połączeń niewyświetlających się w aparacie telefonicznym.

- **Blokowanie połączeń na numery *premium rate***
  Warto rozważyć blokadę wszystkich numerów o podwyższonej płatności. Usługi tzw. *premium rate* są z reguły wykorzystywane przez organizatorów loterii, konkursów i plebiscytów. Często ich reklama może sugerować, że wystarczy zadzwonić, by wziąć udział w konkursie i go wygrać. Informacja o podwyższonej płatności może być mało widoczna, tak jak i regulamin usługi. Warto rozważyć wybranie blokady na różnego rodzaju połączenia, eliminując rozmowy na telefony komórkowe, połączenia *premium rate* lub międzynarodowe. W ramach tej usługi nie są blokowane rozmowy z numerami alarmowymi oraz połączenia bezpłatne do wybranych usług informacyjnych.
- **Ustalenie limitu rachunku**
  Po wyborze tej usługi dzwoniący nie ma możliwości przekroczenia rachunku – po przekroczeniu wskazanej kwoty płatne połączenia wychodzące są blokowane.

Poinformuj dziecko, że zawsze ma możliwość skorzystania z **połączenia na koszt odbiorcy**. Dzwoniąc pod numerem 19222, dziecko połączy się z operatorem i będzie mogło podać numer np. swoich rodziców. Jeśli nie pamięta numeru i nie jest on zastrzeżony, operator wyszuka go w bazie danych.

Dobrym pomysłem pozwalającym zadbać o bezpieczeństwo dziecka jest również **usługa automatycznego połączenia**. Po kilku sekundach od podniesienia słuchawki, jeśli nie zostanie wybrany inny numer, nastąpi połączenie z wcześniej wybranym numerem. Skorzystanie z takiej możliwości może być bardzo przydatne w sytuacji, gdy dziecko zostaje samo w domu.

Pamiętaj o numerach alarmowych. Warto zadbać o to, by dziecko znało numery telefonów do straży pożarnej, pogotowia i na policję, a nawet wpisać je na stałe do telefonu stacjonarnego. Jednocześnie zwróć uwagę dziecka na fakt, że numery alarmowe

można wykorzystywać tylko i wyłącznie w sytuacjach zagrożenia zdrowia lub życia. Ich niewłaściwe wykorzystanie może narazić dzwoniącego na konsekwencje – finansowe i prawne.

Połączenia alarmowe są zawsze bezpłatne i dostępne także wtedy, kiedy inne połączenia, z jakichkolwiek powodów, są zablokowane.

WAŻNE TELEFONY RATUNKOWE

112 – numer alarmowy obowiązujący na terenie całej Unii Europejskiej, służy do powiadamiania w sytuacjach zagrożenia zdrowia, życia lub mienia
997 – policja
998 – straż pożarna
999 – pogotowie ratunkowe
984 – pogotowie rzeczne
985 – ratownictwo morskie i górskie

Numery rozpoczynające się od 116 – zgodnie z regulacjami Unii Europejskiej należą do grupy numerów o tzw. walorach społecznych, czyli z założenia służących dobru społeczeństwa.

- **116 000** – to europejski numer przeznaczony dla rodziców i opiekunów, którym zaginęło dziecko, dla zaginionych dzieci oraz dla wszystkich osób, które mogą pomóc w ich odnalezieniu.
- **116 111** – to telefon zaufania dla dzieci i młodzieży.
- **116 123** – to telefon wsparcia emocjonalnego dla dorosłych.

Numer alarmowy **112** oraz numery **116** dla usług społecznych są całodobowe, bezpłatne i obowiązują na terenie całej Unii Europejskiej.

Wiele potrzebnych informacji można uzyskać pod numerem 118 000 (usługa Dobry Numer, opłata 2,08 zł z VAT / 1,69 zł netto za minutę połączenia, niezależnie od taryfy). Przykładowo: informacje o numerach telefonów, adresach służb alarmowych i pogotowia oraz dyżurach aptek i szpitali, informacje dotyczące funkcjonowania wszystkich urzędów w Polsce, numery telefonów i adresy całodobowych placówek handlowo-usługowych, rozkład jazdy PKP.

Smart TV

Smart TV to odbiorniki telewizyjne umożliwiające dostęp zarówno do treści dostarczanych przez nadawcę telewizyjnego, jak i udostępnianych za pośrednictwem internetu. By w pełni korzystać z usług Smart TV, konieczne jest połączenie telewizora ze źródłem sygnału telewizyjnego (np. kablówką, anteną satelitarną) oraz z internetem

(za pośrednictwem kabla lub sieci Wi-Fi, niezbędne jest dostatecznie szybkie łącze internetowe). Otwiera to dostęp do wielu interaktywnych usług, w tym m.in.: VOD (*Video on Demand* – wideo na żądanie), możliwości korzystania z serwisów społecznościowych i informacyjnych, sklepów internetowych. Dodatkowo telewizory Smart TV umożliwiają korzystanie z zainstalowanych na nich aplikacji, w tym wielu przygotowanych z myślą o dzieciach (materiałów edukacyjnych, gier).

Odbiorniki telewizyjne pozwalające na korzystanie z funkcji Smart TV oferują obecnie wszyscy liczący się producenci telewizorów. Modele poszczególnych producentów różnią się między sobą dostępem do różnych platform VOD oraz liczbą dostępnych aplikacji.

Z usług tego typu można również korzystać na standardowych telewizorach, niezbędne jest wówczas podłączenie do telewizora przystawki (stojącej obok telewizora – *smart tv box* lub wpiętej bezpośrednio w złącze odbiornika – *dongle*) z odpowiednim oprogramowaniem. Dostęp do usług Smart TV umożliwiają też niektóre odtwarzacze Blu-ray.

Wideo na żądanie – kontrola rodzicielska

Nie wszystkie materiały dostarczane w ramach usługi VOD są przeznaczone dla dzieci. By ograniczyć do nich dostęp, można użyć opcji kontroli rodzicielskiej. Pozwala ona na blokadę konkretnych kanałów. Ustawienia te wprowadza się w menu telewizora za pomocą pilota. Ograniczenia mogą dotyczyć wybranego programu, kanału, dekodera lub programów o określonej kategorii wiekowej. Dostęp jest zabezpieczony hasłem (PIN-em).

Po włączeniu kontroli rodzicielskiej zostają uruchomione dodatkowe opcje blokady, np.:

- poziom blokady: blokada dotyczy programów z określonej kategorii wiekowej: 7+, 12+, 16+, 18+, blokada wyłączona;
- blokada kanałów: blokowane są grupy kanałów: sport, film, dzieci, edukacja, muzyka, styl życia, informacja, dla dorosłych;
- blokowanie dekodera: na stałe lub czasowo;
- blokowanie VOD: zablokowany dostęp do wypożyczalni filmów;
- zmiana kodu PIN: warto to zrobić tuż po zakupie telewizora, ponieważ standardowy PIN to 0000, 1111, 1234 itp.
- blokada opcji kontroli rodzicielskiej: uniemożliwia zmianę ustawień kontroli rodzicielskiej.

Klasyfikacja wiekowa

Większość programów telewizyjnych (z wyjątkiem programów informacyjnych, sportowych, reklam, telesprzedaży i przekazów tekstowych) podlega klasyfikacji pod względem przeznaczenia wiekowego, a ich nadawcy są zobowiązani do wyświetlania oznaczeń przez cały czas trwania audycji.

	Od lat	ograniczenia czasowe
	Brak ograniczeń	—
7	7	—
12	12	—
16	16	20:00-6:00
18	18	23:00-6:00

Więcej informacji:

krrit.gov.pl/dla-abonentow-i-konsumentow/ochrona-maloletnich/

Jak dochodzić swoich praw?

Podczas korzystania z internetu, zarówno nam, jak i naszemu dziecku mogą się przytrafić niebezpieczne sytuacje. W przypadku gdy naruszają one prawo, dostępne **są dwie drogi ochrony prawnej: karna i cywilna**. Niektóre niebezpieczne sytuacje, jako przestępstwa, podlegają ściganiu na mocy prawa (droga karna), ale w wielu przypadkach konieczne będzie posłużenie się drogą cywilną, czyli drogą roszczeń odszkodowawczych. Zdarza się również, że przykre dla nas zdarzenia nie stoją w sprzeczności z prawem, ale np. naruszają regulamin serwisu, w którym mają miejsce.

- Przede wszystkim warto zapisać dowody tego, co się wydarzyło. Dobrze jest zachować wszystkie materiały – zapisać SMS-y, e-maile, rozmowy na czatach lub w komunikatorach, komentarze na profilach społecznościowych.

WAŻNE!

Najprostszym sposobem na zarejestrowanie zawartości ekranu jest wykonanie jego zrzutu. Aby zachować to, co jest widoczne na ekranie, należy wcisnąć klawisz „Print Screen" (PrtScn), a następnie wkleić (Ctrl + V) zrzut ekranu do Painta lub Worda i zapisać plik.

- W przypadku jeśli w internecie dojdzie do nadużyć wobec naszego dziecka, należy przede wszystkim zwrócić się do prowadzących serwis, w którym miało miejsce przykre zdarzenie. Za pomocą poczty mailowej lub formularza kontaktowego warto szybko się skontaktować z administratorem strony, opisując dokładnie sytuację.

Możemy również zażądać usunięcia określonych treści ze strony. Część serwisów udostępnia przycisk „Zgłoś nadużycie”.

- W sytuacjach naruszających prawo (m.in. groźby karalne, włamanie informatyczne, stalking, uwodzenie dziecka) należy sprawę zgłosić policji.
- Informacje i porady dotyczące praw konsumenta online można uzyskać na stronie serwisu Urzędu Ochrony Konkurencji i Konsumentów: **ezakupy.uokik.gov.pl** i pod numerem bezpłatnego telefonu infolinii konsumenckiej **800 007 707**.
- Jeżeli ty lub twoje dziecko natrafiliście w sieci na treści nielegalne (np. z pornografią dziecięcą, materiałami rasistowskimi i ksenofobicznymi), należy zgłosić niepokojącą zawartość do zespołu Dyżurnetu (komórki Naukowej i Akademickiej Sieci Komputerowej zajmującej się nielegalnymi treściami w internecie). **dyzurnet.pl**
- CERT Polska przyjmuje zgłoszenia dotyczące włamań lub prób włamania do komputera, nękania spamem przesyłanym za pośrednictwem polskich serwerów lub ataków hackerów. **cert.pl**

Oferta edukacyjna

Fundacja Orange i Fundacja Dajemy Dzieciom Siłę już od kilkunastu lat przygotowują materiały edukacyjne i kampanie społeczne poświęcone bezpieczeństwu dzieci i młodzieży w internecie. Ich autorzy dbają, by przeznaczone dla dzieci materiały, oprócz walorów edukacyjnych, miały atrakcyjną formę – to warunek edukacji przez zabawę. Materiały te doskonale sprawdzają się w domu, jako pretekst do rozmowy z dzieckiem o bezpieczeństwie w internecie. Zachęcamy również do zainteresowania nimi nauczycieli i wychowawców – można je wykorzystywać również w trakcie zajęć szkolnych.

Dla dzieci

Jeśli dziecko ma 4-6 lat:
Serwis Necio.pl – jego głównym bohaterem jest robocik Necio, w towarzystwie którego najmłodsi dowiedzą się, czym jest sieć, jak się po niej poruszać, poznają również zasady korzystania z komputera i internetu. W serwisie dostępne są gry edukacyjne, filmiki i piosenki o bezpieczeństwie w internecie. Elementem tego projektu jest bajka pt. „Mój przyjaciel Necio”. Można ją przeczytać dziecku samodzielnie albo pozostawić to aktorowi Tomaszowi Kotowi (audiobook w pliku MP3). **necio.pl**

Aplikacja Necio. Przeznaczona dla dzieci 4-6 lat, jej zadaniem jest wprowadzenie dzieci w świat internetu i przekazanie im podstawowych informacji nt. bezpieczeństwa w sieci. Przewodnikiem po aplikacji jest sympatyczny robocik Necio. Zawarte w aplikacji kolorowe ilustracje pozwalają dziecku zrozumieć czym jest internet, jak wykorzystać jego możliwości, jak korzystać z aplikacji mobilnych i co zrobić w sytuacji zagrożenia w sieci. Rymowanki z kolei mogą być pretekstem do rozmów z dzieckiem na temat bezpiecznego korzystania z internetu. Aplikacja zawiera: grę zręcznościową, materiały do wydrukowania (memo, maskę, labirynt, kolorowanki), bajkę edukacyjną, teledyski z opcją karaoke, licznik czasu, wskazówki dla rodziców i nauczycieli. **necio.pl/aplikacja**

BeStApp to katalog bezpiecznych aplikacji mobilnych dla dzieci w wieku przedszkolnym (3-6 lat). W katalogu można znaleźć wiele propozycji ciekawych aplikacji, które umilą najmłodszym czas i dadzą możliwość rozwoju nowych umiejętności. By ułatwić wybór odpowiedniej aplikacji z katalogu, propozycje zostały uszeregowane w kategoriach tematycznych. **fdds.pl/bestapp**

Owce w sieci. To seria zabawnych filmów animowanych będących doskonałym pretekstem do rozmowy z dzieckiem w wieku 6-10 lat na temat bezpieczeństwa w internecie. Filmy odwołują się zarówno do motywów bajkowych, jak i współczesnej kultury. Poruszane w nich tematy to m.in. publikacja zdjęć i nagrań zawierających nagość, prześladowania w internecie, wyłudzenia danych osobistych i informacji majątkowych, uwodzenie przez internet. Kreskówki z dubbingiem Andrzeja Grabowskiego dostępne są na **pl.sheeplive.eu**.

Jeśli dziecko ma 9-11 lat:
Sieciaki.pl. To serwis edukacyjny skierowany do dzieci pomiędzy 9. a 11. rokiem życia. Serwis opiera się na fabule walki dobra ze złem. Sieciaki – drużyna dzieci, które wiedzą, jak bezpiecznie korzystać z internetu walczy z Sieciuchami – sprawcami zagrożeń w sieci. W serwisie znaleźć można kompendium wiedzy dotyczące bezpiecznego korzystania z sieci.
Najważniejszym elementem serwisu jest kurs e-learning „Misja: Bezpieczny internet". Kurs składa się z 15 części – misji. Każda misja porusza inne zagadnienie z zakresu bezpieczeństwa online. Dzięki kursowi dzieci nie tylko dowiadują się, jak bezpiecznie korzystać z sieci, ale także uczą się, jak reagować na internetowe zagrożenia. Ponadto w serwisie znaleźć można gry edukacyjne, piosenki, teledyski, a także konkursy z nagrodami.

Katalog Bezpiecznych Stron BeSt – to zbiór bezpiecznych i przyjaznych dzieciom stron internetowych. Strony w katalogu zostały podzielone na osiem kategorii tematycznych: gry i rozrywka, książki i prasa, zwierzęta, filmy i muzyka, edukacja, kultura, czas wolny, razem z rodzicami. Katalog BeSt jest elementem serwisu Sieciaki.pl. **sieciaki.pl/best**

Aplikacja BeStApp – katalog bezpiecznych aplikacji mobilnych BeStApp został przygotowany na urządzenia z systemem operacyjnym Android (**fdds.pl/pobierz-katalog-bezpiecznych-aplikacji-mobilnych-bestapp**). Aplikację można pobrać ze sklepu GooglePlay.

Przeglądarka BeSt. Program komputerowy pozwalający na przeglądanie stron wyłącznie z katalogu Bezpiecznych Stron. Dzięki niej rodzic może mieć gwarancję, że dziecko nie natrafi na strony zawierające niewłaściwe treści lub wejdzie w kontakt z nieznanymi osobami. Przeglądarka umożliwia wyszukiwanie stron przy użyciu słów kluczowych, nazwy i opisu, a także pozwala na wybór stron z ośmiu katalogów tematycznych oraz ograniczenie zawartości w zależności od wieku użytkownika (3+, 6+, 9+ lat). Opiekun dziecka ma możliwość zablokowania zamykania programu hasłem, monitorowania stron odwiedzanych przez dzieci.

Program jest bezpłatny, został przygotowany z myślą o urządzeniach stacjonarnych wyposażonych w system operacyjny Windows, jak i tabletach oraz smartfonach. Można go pobrać ze strony **fdds.pl/best**.

Jeśli dziecko ma 11-13 lat:
„3... 2... 1... Internet!". Seria kreskówek dla dzieci w wieku 11-13 lat, poświęcona szerokiemu spektrum zagrożeń internetowych, m.in. przemocy rówieśniczej, kontaktom z obcymi i uzależnieniu od komputera. Każdy z filmów ma dwa alternatywne zakończenia – bezpieczne i ryzykowne, ich wybór należy do dziecka. Narratorem kreskówek jest kierowca rajdowy Krzysztof Hołowczyc. Kreskówki również w wersji dla dzieci niesłyszących dostępne są pod adresem **321internet.pl**.

Jeśli dziecko ma 13-16 lat:
Digital Youth. Magazyn o fenomenach internetu i bezpieczeństwie online adresowany do młodzieży zainteresowanej rozwojem sieci i nowych technologii, współtworzeniem wirtualnego świata, wykorzystywaniem możliwości, jakie daje internet. Wersja elektroniczna magazynu dostępna jest pod adresem **digitalyouth.pl**.

Fejsmen. Seria kreskówek, w których dysponujący nadnaturalnymi umiejętnościami superbohater niesie pomoc wszystkim tym, którym grozi utrata twarzy w internecie, ale za każdym razem ponosi spektakularną klęskę. Zawsze jednak daje radę – „Dbaj o fejs": kiedy publikujesz, kiedy komentujesz, kiedy wrzucasz zdjęcia… Celem kreskówek jest zwrócenie uwagi młodzieży na problem prywatności w sieci. **dbajofejs.pl**

W Sieci. Talk-show prowadzony przez Ewę Farną, w którym rozmawia ona z zaproszonymi gośćmi (ofiarami internetowych zagrożeń) na temat uwodzenia w sieci oraz cyberprzemocy. Reportaże i wywiady wykorzystane w programie prezentują również pozytywne, efektywne zastosowania sieci. **wsieci.tv**

Większość materiałów jest dostępna również w postaci kursów e-learning na platformie edukacyjnej: **edukacja.fdds.pl**.

Dla dorosłych:

Bezpiecznie Tu i Tam. Internetowy kurs dla rodziców zawierający porady dotyczące tego, jak chronić dziecko w internecie i jak unikać zagrożeń związanych z korzystaniem z nowych technologii przez najmłodszych. E-learning dostępny pod adresem: **fundacja.orange.pl/kurs**.

Zapraszamy rodziców do korzystania z materiałów edukacyjnych dla rodziców w ***Strefie wiedzy Fundacji Orange***:
fundacja.orange.pl/strefa-wiedzy/materialy-edukacyjne-dla-rodzicow/

oraz materiałów edukacyjnych dla dzieci i młodzieży:
fundacja.orange.pl/strefa-wiedzy/materialy-edukacyjne-dla-dzieci-i-mlodziezy/

Upewnij się, czy komputer, telefon i tablet twojego dziecka są bezpieczne

W przypadku komputera, sprawdź czy:

- ☐ działa i jest systematycznie aktualizowany program antywirusowy,
- ☐ jest włączona zapora sieciowa (element systemu lub niezależny program),
- ☐ jest włączone automatyczne pobieranie i instalowanie aktualizacji systemowych,
- ☐ została zaktualizowana przeglądarka internetowa,
- ☐ w przeglądarce został zainstalowany dodatek blokujący reklamy,
- ☐ program antywirusowy skanuje wiadomości e-mail,
- ☐ dziecko ma własne konto użytkownika (z ograniczonymi uprawnieniami),
- ☐ uprawnienia administratora są zabezpieczone mocnym hasłem, nieznanym dziecku,
- ☐ oprogramowanie pochodzi tylko ze znanych i sprawdzonych źródeł,
- ☐ każda zewnętrzna pamięć (przenośny twardy dysk, pamięć USB) jest przeskanowana przez program antywirusowy przed skopiowaniem plików.

W przypadku telefonu lub tabletu, sprawdź czy:

- ☐ zostały zainstalowane wszystkie uaktualnienia zalecane przez producenta,
- ☐ nieużywane lub zbędne aplikacje zostały odinstalowane,
- ☐ zostały zaktualizowane wszystkie aplikacje,
- ☐ zainstalowana i uruchomiona została aplikacja kontroli rodzicielskiej,
- ☐ zostały skonfigurowane ustawienia kontroli rodzicielskiej z marketu z aplikacjami,
- ☐ włączone jest filtrowanie treści,
- ☐ dostęp do telefonu został zabezpieczony hasłem, PIN-em lub odciskiem palca,
- ☐ zablokowane zostały połączenia typu *premium*.

Fundacja orange™

Orange Polska już od kilkunastu lat dba o bezpieczeństwo najmłodszych internautów. Poradnik „Bezpieczne media" powstał dzięki współpracy Fundacji Orange i Fundacji Dajemy Dzieciom Siłę. W ramach wspólnych działań na rzecz bezpieczeństwa dzieci w internecie przygotowano również m.in. platformę e-learningową dla uczniów i dorosłych, serwisy internetowe, odwołujące się do zasad edukacji przez zabawę oraz materiały edukacyjne i scenariusze zajęć, dedykowane profesjonalistom pracującym z dziećmi i młodzieżą, poświęcone świadomemu korzystaniu z sieci. W oparciu o nie, wykorzystując jednocześnie własną wiedzę i kompetencje, wolontariusze – pracownicy Orange Polska, którym tematyka nowych technologii jest szczególnie bliska – przeszkolili blisko 40 tys. dzieci z całej Polski.

orange.pl/bezpieczenstwo

DAJEMY DZIECIOM SIŁĘ