Zanim kupisz dziecku

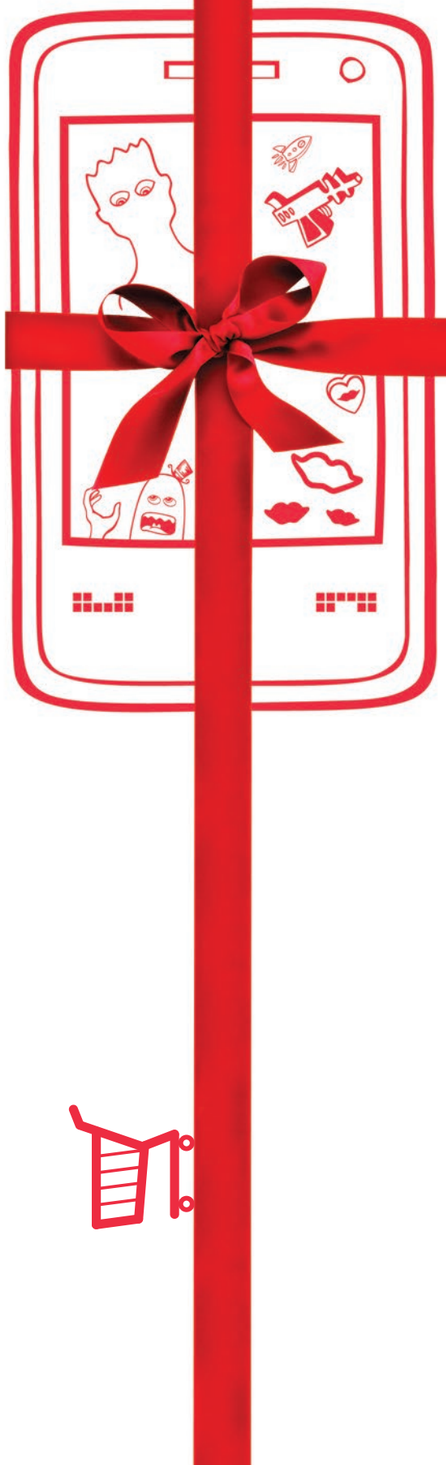
komputer, tablet, smartfon, laptop,
konsolę, grę komputerową...
pomyśl o jego bezpieczeństwie.

więcej na: www.zanimkupisz.saferinternet.pl

bezpłatne konsultacje: 800 100 100 telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci

Główny Partner Partner

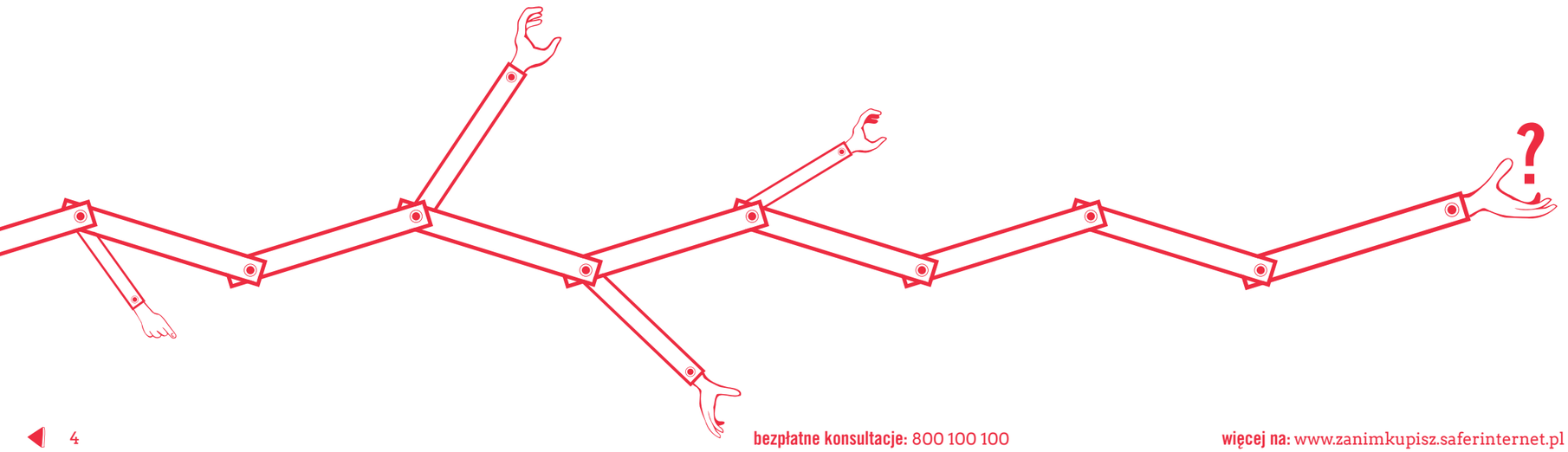
FUNDACJA DZIECI NICZYJE · NASK · saferinternet.pl · Współfinansowane przez Unię Europejską Instrument „Łącząc Europę" · orange Fundacja · Europejskie Centrum Konsumenckie ECC-Net



Wstęp: POMYŚL, ZANIM KUPISZ

Komputer, internet, telefon komórkowy w ostatnich latach stały się nieodłącznym elementem życia dzieci i młodzieży. Nic więc dziwnego, że technologiczne nowinki są jednym z popularniejszych pomysłów na gwiazdkowy, urodzinowy czy komunijny prezent. Musimy jednak pamiętać, że technologia niewłaściwie wykorzystywana może stanowić zagrożenie dla bezpieczeństwa dziecka i jego właściwego rozwoju. Dlatego tak ważna jest świadomość opiekunów dotycząca zagrożeń związanych z nowoczesnymi technologiami oraz możliwości zapobiegania im i dbania o bezpieczeństwo młodych internautów.

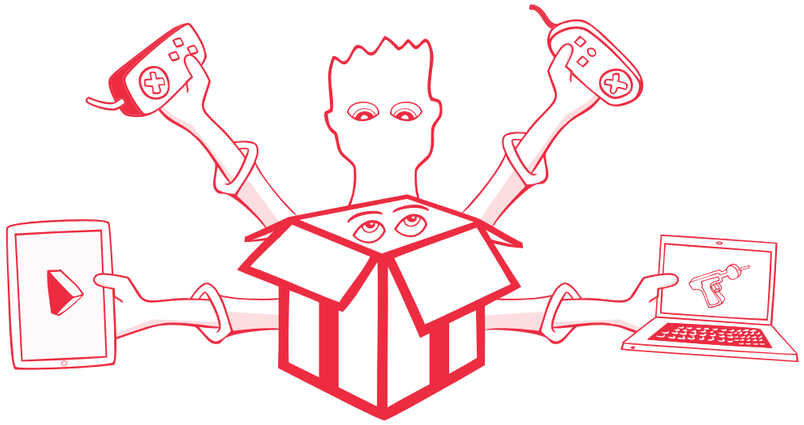
Kampania informacyjna pod hasłem „Pomyśl, zanim kupisz", przygotowana przez Polskie Centrum Programu Safer Internet (w skład którego wchodzą Naukowa i Akademicka Sieć Komputerowa oraz Fundacja Dzieci Niczyje), ma pomóc dorosłym w świadomym wyborze multimediów, kupowanych z myślą o dzieciach. Mamy nadzieję, że dzięki tej kampanii młodzi internauci będą bezpiecznie i konstruktywnie wykorzystywać nowe technologie, a fascynacja elektronicznymi gadżetami nie odbije się na relacjach społecznych dzieci.



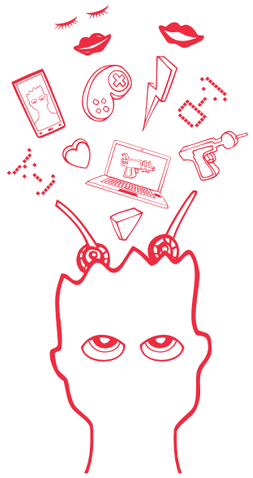
1. Młodzi ludzie a nowe technologie

Internet to medium, którego dynamiczny rozwój i potencjał wykorzystują przede wszystkim młodzi ludzie. Jest nieodłącznym elementem ich życia społecznego, codziennych aktywności i rozrywki. Dziś nie ma raczej nastolatka, który potrafiłby obejść się bez nowych technologii. O ile w 2007 roku w Polsce tylko nieco ponad połowa gospodarstw domowych z dziećmi poniżej 16 lat miała dostęp do sieci, o tyle w 2015 roku odsetek ten wyniósł 95 proc. (GUS, 2015). Zdecydowana większość gimnazjalistów (86,2 proc.) korzysta z internetu codziennie, w tym 43,2 proc. młodych ludzi jest online bez przerwy – głównie za sprawą urządzeń mobilnych (Pedagogium WSNS, 2014). Do połączenia się z siecią nastolatki najczęściej wykorzystują smartfony (54,3 proc.) oraz laptopy (52,5 proc.).

Najpopularniejszą czynnością młodych ludzi w internecie jest oglądanie klipów wideo i filmów – co najmniej raz w tygodniu robi to 84 proc. gimnazjalistów (EU NET ADB, 2013). Niewiele mniej, bo 80 proc. korzysta z komunikatorów. Inną, równie powszechną formą aktywności jest korzystanie z serwisów społecznościowych – przynajmniej raz w tygodniu zagląda do nich 79 proc. gimnazjalistów, a konto na przynajmniej jednym z portali ma 90 proc. nastolatków. Kolejne pozycje wśród form aktywności młodzieży w sieci zajmują odpowiednio: odrabianie prac domowych i poszukiwanie informacji (76 proc.) oraz ściąganie muzyki (66 proc.).



Internet otwiera przed młodym pokoleniem wiele możliwości, ale jednocześnie niesie ze sobą nowe wyzwania. Dla młodych ludzi sieć nierzadko staje się pozornie prostym narzędziem do kształtowania swojego wizerunku, miejscem złudnie bezpiecznym, gwarantem anonimowości czy panaceum na ich problemy. Internet to kopalnia możliwości i okno na świat, w którym obok wartościowych treści i odpowiedzialnych internautów, spotykamy drastyczne obrazy i agresywnych użytkowników. Na destrukcyjny wpływ internetowych treści szczególnie narażeni są młodzi ludzie. Spośród polskich gimnazjalistów 67,3 proc. zetknęło się w internecie z różnego rodzaju materiałami pornograficznymi (EU NET ADB, 2013), a niejednokrotnie młodzi ludzi napotkali w sieci szkodliwe treści, takie jak przekazy pełne nienawiści bądź agresywne ataki słowne (40 proc.), treści na temat skrajnego odchudzania się (prawie 30 proc.), doświadczenia z zażywania narkotyków (24 proc.) oraz sposobów samookaleczenia się (ponad 20 proc.) (Kirwil, 2011). Internet nie tylko może dać przestrzeń dla treści nieodpowiednich dla dzieci, ale także może stać się narzędziem cyberprzemocy, czyli rówieśniczej agresji. 21,5 proc. nastolatków doświadczyło przemocy w sieci (EU NET ADB, 2013), która przybrała formę wyzywania, straszenia, poniżania, podszywania się pod kogoś lub robienia komuś zdjęć lub filmów i publikowania ich bez zgody ofiary. Omawiając tematykę bezpieczeństwa młodych internautów nie sposób pominąć problemu sekstingu. Jest to niebezpieczne zjawisko przesyłania treści o charakterze erotycznym, głównie swoich nagich lub półnagich zdjęć, za pomocą internetu i telefonu komórkowego, popularne szczególnie wśród młodzieży. Ponad połowa (58 proc.) ankietowanej młodzieży przyznała, że ich kolegom zdarzyło się przesyłać znajomym rówieśnikom za pomocą telefonu lub internetu zdjęcia lub filmy przedstawiające ich nago lub prawie nago (GfK Polonia dla FDN, 2014).



Kolejnym rodzajem zachowania ryzykownego wartym zaznaczenia jest pewna otwartość nastolatków na interakcje bezpośrednie z osobami poznanymi w świecie wirtualnym. Świadczy o tym fakt, że co dziesiąty (10,6 proc.) nastolatek przyznał się do spotkania poza internetem z osobą dorosłą, a prawie co trzecia (28,7 proc.) z tych osób nie poinformowała o tym nikogo ze swojego otoczenia. W zdecydowanej większości (78,5 proc.) badani deklarują świadomość, że takie spotkania mogą być niebezpieczne (Pedagogium WSNS, 2014). Ich wiedza dotycząca zagrożeń internetowych i ich konsekwencji jest też względnie dobra. Dziwi zatem skala podejmowanych w sieci niebezpiecznych zachowań.

Dynamiczny rozwój nowych technologii fascynuje i „wciąga" nastolatków, dlatego są oni narażeni na utratę kontroli nad czasem korzystania z internetu, co może prowadzić do izolacji, a także zaniedbywania nauki, zdrowia czy kontaktów z rówieśnikami. Odsetek nastolatków dysfunkcyjnie korzystających z sieci, czyli nadużywających internetu lub zagrożonych nadużywaniem wynosi 13,3 proc. (EU NET ADB, 2013).

Lista niebezpieczeństw jest długa i zmienia się wraz z rozwojem nowych technologii. Dorosłym może się wydawać, że nie sposób nadążyć za rozwojem sieci, czy wirtualnymi nawykami i zainteresowaniami ich dzieci. Stąd potrzeba podnoszenia świadomości rodziców na ten temat, mówienia o nowych, niepokojących zjawiskach oraz o tym, jak najskuteczniej postępować w przypadku wirtualnych zagrożeń. Wydaje się to szczególnie ważne z uwagi na fakt, że ponad połowa (55,6 proc.) nastolatków zadeklarowała, że ich rodzice nie interesują się tym, co robią w internecie (Pedagogium WSNS). Ważne, by rodzice zrozumieli, że nie muszą być ekspertami w dziedzinie nowinek technologicznych i wirtualnych trendów, aby móc rozmawiać z dziećmi

o ich aktywnościach online. Dorośli powinni towarzyszyć najmłodszym w ich pierwszych internetowych krokach i uczyć je, że obecność oraz aktywne uczestnictwo w sieciowym życiu społecznym powinno być oparte na podstawowych, ponadczasowych wartościach, czyli m.in. na szacunku względem siebie oraz drugiego człowieka. Rodzice nie powinni zapominać także o tym, że internet to narzędzie, bez którego dziecko się dziś nie obejdzie, jednak nie może ono zastąpić relacji z rodziną, z rówieśnikami czy ruchu na świeżym powietrzu.

Zwróć uwagę

Lista internetowych zagrożeń zmienia się wraz z postępem nowych technologii. By zapewnić bezpieczeństwo swoim pociechom, rodzice muszą mieć świadomość, na jakie zagrożenia narażone są ich dzieci.

- kontakt z nielegalnymi materiałami (np. przedstawiającymi seksualne wykorzystanie dzieci, rasizm, ksenofobię) lub szkodliwymi treściami (np. pornografia, przemoc),
- uwodzenie za pośrednictwem internetu (grooming),
- nękanie za pośrednictwem sieci (cyberprzemoc),
- przesyłanie swoich nagich lub półnagich zdjęć (sexting),
- kradzież lub nieświadome udostępnianie informacji (np. numerów kart, adresów, haseł itp.),
- nadużywanie internetu i multimediów.

Warto, by rodzice i nauczyciele zwrócili uwagę młodych internautów na fakt, że większość zasad znanych im z życia, obowiązuje także w sieci. Obok netykiety to także regulacje prawne. Konsekwencje naruszenia prawa online mogą być dużo poważniejsze niż usunięcie danego wpisu czy zablokowanie dostępu do określonego serwisu.

Prywatność

Jedną z podstawowych zasad bezpiecznego zachowania w internecie jest dbałość o swoją prywatność, a przede wszystkim o informacje, pozwalające na jednoznaczne zidentyfikowanie konkretnej osoby: imię, nazwisko, wiek, adres, nazwa szkoły, zdjęcia. Publikując dane na swój temat, należy trzymać się prostej zasady – umieszczajmy tylko takie informacje, które bylibyśmy w stanie powierzyć nieznajomemu spotkanemu na ulicy. Należy pamiętać też o tym, że informacja raz zamieszczona w internecie pozostanie w nim na zawsze, a dostęp do niej może mieć praktycznie każdy, również za kilka, kilkanaście lat.

Zwracajmy także uwagę na to, jakie informacje zamieszczają na nasz temat inni, np. sprawdzając, jakie dane o nas pokaże wyszukiwarka internetowa. Szanujmy też prywatność innych – np. kiedy publikujemy zdjęcie innej osoby, zapytajmy ją o pozwolenie.

Zwróć uwagę na to, jakie informacje publikuje dziecko w internecie, a także czy dobrze strzeże swojej prywatności. Zapytaj je czy treści, jakie publikuje online zamieściłoby także w miejscu publicznym np. gablocie szkolnej. Pomóż mu skonfigurować ustawienia prywatności, a także uczul, aby nikomu nie udostępniało swoich haseł.

Niebezpieczne kontakty

Komunikacja internetowa, oprócz wielu zalet, niesie również pewne zagrożenia. Uwiedzenie przez osobę dorosłą, nazywane groomingiem, to tylko jedno z niebezpieczeństw. Kontakty z nieznajomymi mogą być szczególnie groźne, jeżeli prowadzą do spotkania w rzeczywistości. Dlatego w kontaktach zawieranych przez internet należy stosować zasadę ograniczonego zaufania – nigdy nie wiadomo, czy osoba, z którą kontaktujemy się online, jest tym, za kogo się podaje. Kontakty z osobami znanymi wyłącznie z internetu mogą sprzyjać próbom wyłudzenia loginów i haseł do serwisów internetowych, danych bankowych lub pieniędzy. Zagrożeniem jest również kontakt z osobami propagującymi działalności sekt lub innych niebezpiecznych grup, a także zachęcającymi do ryzykownych zachowań.

Wytłumacz, że nawiązywanie kontaktów przez internet może być niebezpieczne, bo trudno zweryfikować, czy osoba, z którą rozmawia jest tym, za kogo się podaje. Przekonaj dziecko, że jeśli ktoś lub coś je zaniepokoi, powinno Ci o tym powiedzieć.

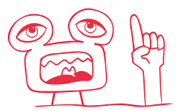
Cyberprzemoc

Cyberprzemoc to przemoc rówieśnicza z użyciem mediów elektronicznych. Może przybierać wiele form, m.in.: wyzywanie, straszenie, poniżanie kogoś w internecie lub przy użyciu telefonu, robienie komuś zdjęć lub filmów bez jego zgody, ich publikowanie i rozsyłanie lub podszywanie się pod kogoś w sieci. Zewnętrznemu obserwatorowi akty cyberprzemocy mogą wydawać się niewinne, wywołują jednak u ofiary cierpienie i poczucie krzywdy. Nawet ignorowanie przez rówieśników profilu społecznościowego danej osoby lub jej wpisów, może okazać się dla młodych ludzi bardzo bolesnym doświadczeniem.

Cechą specyficzną dla cyberprzemocy jest jej ciągłość, ofiara cierpi zarówno w szkole, jak i w domu, dziecko przez całą dobę doświadcza negatywnych emocji i lęku. Sprawcami

cyberprzemocy często są sami młodzi internauci. Niezwykle ważna jest więc świadomość możliwych konsekwencji takich działań, także prawnych.

Rozmawiaj ze swoim dzieckiem o jego znajomych, relacjach między nimi, sympatiach i antypatiach. Dzięki temu łatwiej zauważysz, jeśli dotknie je cyberprzemoc. Reaguj natychmiast na przemoc w sieci doświadczaną przez dziecko. W razie potrzeby współpracuj ze szkołą, policją, rodzicami sprawców i świadków. Razem z dzieckiem zabezpieczcie dowody przemocy w sieci.



Treści nielegalne i szkodliwe

Polskie prawo zabrania prezentowania, rozpowszechniania, produkcji, utrwalania, sprowadzania, przechowywania, posiadania treści pornograficznych z udziałem małoletniego do 18 roku życia oraz treści pornograficznych związanych z prezentowaniem przemocy lub posługiwaniem się zwierzęciem; publiczne propagowanie faszystowskiego lub innego totalitarnego ustroju państwa lub nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość.

Oprócz treści nielegalnych w internecie dziecko może mieć kontakt z treściami uznawanymi za szkodliwe (ze względu na jego wiek i poziom rozwoju psychospołecznego). Można do nich zaliczyć m.in.:

- treści pornograficzne,
- treści obrazujące przemoc, obrażenia fizyczne, deformacje ciała,
- treści nawołujące do samookaleczeń lub samobójstw, bądź zachowań szkodliwych dla zdrowia,
- treści dyskryminacyjne, nawołujące do wrogości, a nawet nienawiści wobec różnych grup społecznych lub jednostek.

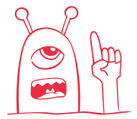
Łatwo jest natrafić w sieci na różnego rodzaju zachęty do stosowania wyniszczających diet, lub substancji zwiększających masę mięśniową i innych używek, zaproszenie do wstąpienia do sekt czy innych grup o radykalnych poglądach. Treści nieodpowiednie są często poszukiwane przez młodego odbiorcę, a forma ich prezentacji jest bardzo atrakcyjna. Należy pamiętać, że kontakt dzieci i młodzieży z treściami tego typu może spowodować długotrwałe negatywne konsekwencje emocjonalne oraz poznawcze. Może skutkować fałszywym postrzeganiem świata, podważyć poczucie bezpieczeństwa lub zbudować przekonanie, że patologiczne zachowania są normą.

Komputer przeznaczony dla dziecka powinien być wyposażony w program filtrujący, który może pomóc w ograniczeniu dostępu zwłaszcza młodszego dziecka do szkodliwych treści. Należy rozmawiać z dzieckiem o tym, co robi w internecie.

Sexting

To niebezpieczne zjawisko przesyłania treści o charakterze erotycznym – głównie swoich nagich lub półnagich zdjęć – za pomocą internetu i telefonu komórkowego, popularne szczególnie wśród nastolatków. W przypadku sekstingu mamy do czynienia z sytuacją, kiedy nastolatek nie tylko jest autorem treści o charakterze erotycznym, ale także dobrowolnie przekazuje je swoim znajomym. Popularność sekstingu bierze się przede wszystkim z typowej dla wieku fascynacji seksem, zainteresowania płcią przeciwną, braku doświadczenia w relacjach z innymi, mody na tego typu zachowania, ciekawości lub nieśmiałości. Konsekwencje tego zjawiska mogą być bardzo poważne. Niejednokrotnie wysłane znajomemu lub przyjacielowi zdjęcie było wykorzystywane do szantażu lub trafiało do publicznego obiegu w formie żartu, w celu ośmieszenia lub zemsty.

Porozmawiaj z dzieckiem o niebezpieczeństwach związanych z tego rodzaju zachowaniami, z publikowaniem lub nagrywaniem intymnych sytuacji. Uświadom dziecku, że zdjęcie, jakie wysyła znajomemu może trafić w niepowołane ręce.



Pomoc

Punkt kontaktowy, do którego można anonimowo zgłaszać przypadki występowania w internecie treści szkodliwych lub zabronionych prawem (szczególnie związanych z prezentacją materiałów przedstawiających seksualne wykorzystanie dzieci):

dyżurnet.pl

e-mail: dyzurnet@dyzurnet.pl
tel. 801 615 005 (koszt połączenia lokalnego)
formularz elektroniczny na stronie: www.dyzurnet.pl

Bezpłatna, anonimowa pomoc telefoniczna i online dla rodziców oraz nauczycieli w sprawach bezpieczeństwa dzieci:

800 100 100
telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci

e-mail: pomoc@800100100.pl
tel. 800 100 100 (połączenie bezpłatne)
www.800100100.pl

2. Kiedy kupujesz komputer

Komputer to jedno z podstawowych urządzeń w naszych domach. Dla wygody i uniknięcia domowej rywalizacji o dostęp do komputera, coraz częściej każdy domownik ma swoje własne urządzenie. Chcąc obdarować dziecko laptopem lub komputerem stacjonarnym, powinniśmy pamiętać o kilku sprawach, które mogą się okazać istotne zarówno w chwili zakupu, jak i użytkowania sprzętu:

- Kupując komputer, upewnij się, czy został na nim zainstalowany program antywirusowy i przez jaki okres czasu będziesz mógł z niego korzystać. Jeśli go nie ma – koniecznie go zainstaluj, istnieje wiele bezpłatnych programów antywirusowych na domowe komputery, które często w niczym nie ustępują skutecznością czy funkcjonalnością ich płatnym odpowiednikom.
- Dbaj o to, aby nie instalować na komputerze zbędnego oprogramowania. Jeśli nie jesteś pewien, do czego służy dany program, nie instaluj go. Kupując lub pobierając programy, korzystaj tylko ze sprawdzonych, bezpiecznych źródeł. Korzystanie z programów pirackich jest nie tylko łamaniem prawa, ale także niesie ze sobą ryzyko zarażenia systemu komputerowego wirusem.
- W wielu programach dostępnych na rynku wykrywane są błędy, wpływające na bezpieczeństwo ich użytkownika. Nie wolno zaniedbywać aktualizacji – nie tylko systemu operacyjnego, ale i przeglądarki internetowej oraz innych programów. Jeśli aplikacja umożliwia automatyczne sprawdzanie dostępności aktualizacji, skorzystaj z tej funkcji i instaluj je, kiedy tylko się pojawiają. Rozważ też korzystanie z bezpłatnych produktów do sprawdzania aktualności oprogramowania.
- Nawet jeśli komputer ma służyć wyłącznie dziecku, zastanów się, kto będzie posiadał uprawnienia administracyjne, pozwalające m.in. na instalowanie nowego oprogramowania lub zmianę kluczowych ustawień bezpieczeństwa. W przypadku najmłodszych użytkowników zaleca się, by takie uprawnienia posiadała osoba dorosła, a dziecko miało wydzielony profil użytkownika z ograniczonymi prawami.
- Zwracaj uwagę na podłączane do komputera urządzenia przenośne, w szczególności pendrive'y lub dyski USB. Mogą one bardzo łatwo przenosić wirusy – wystarczy, że były wcześniej podłączone do zainfekowanego komputera. Dobrą praktyką jest skanowanie antywirusowe każdego urządzenia podłączanego do komputera.
- Pamiętaj o archiwizacji danych, co pozwoli Ci odzyskać najcenniejsze zdjęcia i dokumenty w przypadku awarii lub kradzieży. Możesz w tym celu wykorzystać dodatkowe urządzenia, takie jak: zewnętrzny dysk twardy, nagrywarka DVD, Blu-Ray czy sieciowy serwer plików. Możesz także umieścić swoje dokumenty „w chmurze", czyli w jednym ze specjalnych serwisów do przechowywania danych – wiele z nich dostępnych jest bezpłatnie.
- Korzystając z publicznej sieci Wi-Fi dostępnej np. w kawiarni, na stacji benzynowej lub lotnisku, pamiętaj, by przy logowaniu się do poczty, banku lub innego serwisu używać połączenia szyfrowanego SSL. Pamiętaj również o każdorazowym wylogowaniu się!
- Komputer przeznaczony dla dziecka powinien być wyposażony w program filtrujący, pozwalający na uchronienie dziecka przed kontaktem ze szkodliwymi treściami. Programy kontroli rodzicielskiej dysponują też możliwościami ograniczania aktywności dziecka w internecie zarówno na urządzeniach stacjonarnych, jak i mobilnych (np. tablet) – takimi jak brak dostępu do treści niedostosowanych dla dzieci, wypełnianie formularzy online, korzystanie z komunikatorów. Programy te mogą również monitorować czas, który dziecko spędza przed komputerem.
- Jeśli komputer, który ofiarowujesz dziecku, jest początkiem jego przygody z internetem, wykorzystaj tę okazję do przekazania mu podstawowych zasad bezpieczeństwa online.

Zanim podarujesz komputer dziecku, odpowiednio go zabezpiecz. Zwracaj uwagę na to, w jaki sposób Twoje dziecko spędza czas online i czy jest bezpieczne.

3. Kiedy kupujesz konsolę

Konsola do gier to jedno z dziecięcych marzeń. Dzięki niej możemy tańczyć i śpiewać jak gwiazdy teledysków, próbować swoich sił jako rajdowiec lub zostać bohaterem filmu akcji. Nowe możliwości konsoli oraz bogactwo gier na rynku sprawiają, że od kilku lat urządzenia te zyskują na popularności. Kupując konsolę, warto pamiętać:

- Konsole są coraz silniej zintegrowane z serwisami online, dzięki czemu można pobierać dodatkowe treści, grać w sieci z udziałem wielu użytkowników, udostępniać własne wyniki. Pomóż dziecku skonfigurować dostęp do tych usług tak, aby nie było narażone na nieodpowiednie treści. Wystarczy upewnić się, że przy rejestracji konta został podany rzeczywisty wiek dziecka, o resztę powinien zadbać sam serwis.
- Porozmawiaj z dzieckiem na temat tego, co może, a czego nie może publikować online. Czy powinny tam się znaleźć zdjęcia lub filmy z jego udziałem i w jego domu? Pełen adres?
- Część funkcji online wymaga dodatkowych opłat, wykupienia abonamentu lub jest całkowicie niedostępna dla dzieci. Kupując grę, dowiedz się wcześniej, jakie ograniczenia wprowadził producent. Pozwoli to uniknąć frustracji dziecka wynikającej np. z braku możliwości rozegrania wirtualnego meczu z kolegami.
- Za dodatkowe treści dostępne online trzeba często zapłacić. Zamiast wykorzystywać w tym celu kartę kredytową, warto rozważyć posługiwanie się specjalnymi kartami przedpłaconymi, które można kupić w sklepach z grami. W ten sposób łatwiej będzie nam kontrolować wydatki, a w przypadku kradzieży/wycieku danych z serwisu nie ryzykujemy utraty kontroli nad wydatkami. W przypadku kont dla dzieci, warto także ustalić limity wydatków.
- Zwracaj uwagę na oznaczenia wieku, umieszczane przez producentów gier na pudełkach. W przypadku zakupów online w serwisie internetowym konsoli oferta będzie automatycznie dostosowana do wieku właściciela konta.

Konsola może być świetną zabawą rozwijającą dziecko. Trzeba jednak świadomie potraktować związane z nią potencjalne zagrożenia.

4. Kiedy kupujesz smartfon/tablet

Telefon i tablet to kolejne pozycje z listy dziecięcych marzeń. Dzięki intuicyjnej obsłudze, atrakcyjnym aplikacjom, nowoczesnemu wyglądowi i łatwości, z jaką za ich pośrednictwem można się połączyć z internetem, stają się nieodłącznymi towarzyszami dzieci i nastolatków. Już prawie 60 proc. dzieci w wieku 12-15 lat łączy się z siecią właśnie przez urządzenia mobilne (GUS, 2015). Jednak rodzice, dbając o bezpieczeństwo domowego komputera swojego dziecka, często zapominają, że praktycznie takie same możliwości dostępu do internetu ma ono w swoim telefonie. Jeśli uznasz, że Twoje dziecko jest już gotowe, by korzystać ze smartfonu lub tabletu, warto zadbać o kilka kwestii:

- Obdarowując dziecko telefonem komórkowym lub tabletem, dajesz mu możliwość tworzenia internetowych treści, zaistnienia w sieci, komunikowania się z innymi. Dzięki temu może być autorem tekstów, obrazów i filmów, które łatwo rozpowszechniać na stronach internetowych. Może uzyskać dostęp do treści internetowych, również tych szkodliwych, np. pornografii i przemocy.
- Wielu rodziców kupuje urządzenia mobilne już dla bardzo małych dzieci. Według badań Fundacji Dzieci Niczyje (2015 r.) własne komórki i tablety posiada jedna czwarta maluchów w wieku 0-6 lat. Dla tak małych dzieci nie jest zalecane kupowanie własnego urządzenia, ponieważ nie są one jeszcze gotowe do korzystania z tych technologii.
- Jeśli uznasz, że Twoje dziecko jest już wystarczająco duże, by korzystać ze smartfonu lub tabletu, ustal z nim zasady korzystania z urządzenia, np. wyłączanie telefonu podczas lekcji, w szkole, w nocy; określ czas korzystania z urządzenia w ciągu dnia.
- Aplikacje kontroli rodzicielskiej pomagają wyłączyć w urządzeniu funkcje, z których nie powinno korzystać dziecko. Różnią się one w zależności od marki telefonu/tabletu oraz systemu operacyjnego. Wszystkie najpopularniejsze mobilne systemy operacyjne (Android, iOS, Windows Phone) mają fabrycznie wbudowane ustawienia kontroli rodzicielskiej, które wystarczy aktywować. Warto dokładnie poznać zakres ich działania. Jeśli oczekujesz lepszej ochrony, możesz skorzystać z szeregu aplikacji dostępnych na rynku.
- Zwróć uwagę dziecka na fakt, że część aplikacji dostępnych na smartfony/tablety jest płatna, podobnie jak dostęp 3G do internetu (również dodatkowo, np. po przekroczeniu limitu przesyłanych danych) i jeśli będzie z nich korzystać, użytkowanie urządzenia może stać się kosztowne. Z nastolatkiem możesz wspólnie przyjrzeć się miesięcznemu rachunkowi. Warto, żeby dziecko od początku miało świadomość, ile czasu poświęca na rozmowy telefoniczne, korzystanie z iternetu oraz jakie wiążą się z tym koszty.
- Pobieraj aplikacje tylko z zaufanych źródeł. Cyberprzestępcy tworzą złośliwe aplikacje, które bardzo przypominają te prawdziwe, lecz są zainfekowane wirusami lub robakami, pozwalającymi nawet na przejęcie kontroli nad urządzeniem. W takiej sytuacji telefon może np. łączyć się z kosztownymi serwisami. Warto uzgodnić z dzieckiem, by zanim ściągnie na telefon nową aplikację, skonsultowało się z rodzicem. Szczególnie ostrożnym należy być wobec aplikacji, które żądają dostępu do poufnych informacji (np. loginu, hasła dostępu, danych osobowych, książki telefonicznej i innych informacji zapisanych w telefonie) i pozwolenia na ich przechowywanie. W przypadku młodszych dzieci, polecamy aplikacje z bezpiecznego katalogu bestapp.fdn.pl
- Zwróć uwagę na to, ile czasu Twoje dziecko spędza na korzystaniu z nowych technologii. Amerykańska Akademia Pediatrii zaleca rodzicom ograniczenie dzieciom czasu spędzanego przed ekranem do 2 godzin dziennie. Niektóre aplikacje na smartfony i tablety

umożliwiają określenie czasu, jaki dziecko może spędzić online. Taką możliwość dają również programy kontroli rodzicielskiej. Dzieci poniżej 6 roku życia nie powinny korzystać z urządzeń mobilnych jednorazowo dłużej niż 15 minut. Dzieci poniżej 2 lat nie powinny w ogóle korzystać z urządzeń ekranowych.

» Dzieci i młodzież chętnie korzystają z internetu za pośrednictwem darmowych sieci publicznych. Korzystanie z nich może wiązać się z ryzykiem – jeśli telefon nie posiada odpowiedniego oprogramowania zabezpieczającego, jest narażony na zainfekowanie złośliwym oprogramowaniem i próby włamania. Warto wyposażyć urządzenie mobilne dziecka we właściwe programy antywirusowe.

» Rozważ, czy Twoje dziecko powinno móc korzystać z mikropłatności. To system szybkich płatności za usługi online lub doładowanie konta w grze. Coraz więcej firm oferuje aplikacje na smartfony, pozwalające na korzystanie z wirtualnego portfela zasilanego z konta bądź karty kredytowej. Mogą z nich 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.

» Formą mikropłatności jest również wysyłanie wiadomości SMS. W odpowiedzi abonent otrzymuje kod aktywacyjny, który umożliwia uruchomienie danej usługi. Warto zwrócić uwagę na SMS-y o podwyższonej opłacie (tzw. sms premium). Blokowanie tego rodzaju wiadomości tekstowych możliwe jest u operatorów sieci komórkowych.

» Pamiętaj o archiwizacji danych, która umożliwi odzyskanie najcenniejszych kontaktów, zdjęć w przypadku awarii lub utraty telefonu/tabletu. Możesz w tym celu zgrać dane na komputer, a potem skopiować je na dysk twardy, nagrywarkę DVD lub Blu-Ray albo serwer plików.

✓ Każda płatna usługa telefoniczna powinna mieć swój regulamin, zwykle zamieszczony w sieci. Jego treść powinna zawierać informację nt. sposobów rezygnacji z jej dalszego świadczenia.
✓ Jeśli dziecko padło ofiarą przestępstwa, sprawa powinna zostać zgłoszona policji.
✓ Zabezpiecz dowody, które pomogą w ustaleniu sprawcy:
>> zachowaj otrzymane SMS-y, które mogą stanowić w przyszłości dowód w sprawie prowadzonej przez organy ścigania,
>> zwróć się do operatora telefonicznego o rachunek szczegółowy dotyczący SMS-ów oraz połączeń wychodzących i przychodzących (zazwyczaj do 12 miesięcy wstecz).
✓ Kiedy nie masz pewności, jak postąpić, skontaktuj się z bezpłatnym telefonem dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci 800 100 100 (www.800100100.pl)

5. Kiedy kupujesz grę

Blisko połowa gier komputerowych i wideo dostępnych na rynku jest odpowiednia dla graczy w każdym wieku, wiele jednak przeznaczonych jest dla starszych dzieci, młodzieży lub tylko dla osób dorosłych. PEGI (Pan European Game Information) to ogólnoeuropejski system klasyfikacji gier opracowany w celu ochrony nieletnich przed dostępem do treści dla nich nieodpowiednich. Klasyfikacja PEGI to informacja dla konsumentów (przede wszystkim dla rodziców), pomagająca w podjęciu decyzji o zakupie gry komputerowej. System ten jest stosowany i uznany w całej Europie, zyskał również poparcie Komisji Europejskiej. Kupując grę, zwróćmy szczególną uwagę na oznaczenia:

Wiek – klasyfikacja wiekowa informuje o stosowności gry dla danego wieku. Na przykład liczba „18” oznacza, że gra jest zalecana dla pełnoletnich użytkowników. Klasyfikacja ta nie dotyczy poziomu trudności gry oraz umiejętności wymaganych od gracza, ale jedynie treści adekwatnych dla danego wieku.

Treść gry – piktogramy treści wskazują na występowanie w grze konkretnych elementów decydujących o klasyfikacji wiekowej lub oznaczających treści nieodpowiednie dla młodszych dzieci.

WULGARYZMY
gra zawiera niecenzuralne słownictwo w dialogach lub napisach

DYSKRYMINACJA
gra pokazuje przykłady dyskryminacji lub zawiera elementy, które mogą do niej zachęcać

STRACH
gra zawiera obrazy lub dźwięki, które mogą przestraszyć młodsze dzieci

NARKOTYKI
w grze pojawiają się nawiązania do narkotyków lub jest pokazane ich zażywanie

PRZEMOC
gra zawiera elementy przemocy w stosunku do ludzi lub zwierząt

EROTYKA
w grze występują elementy nawiązujące do zachowań o charakterze seksulanym

HAZARD
w grze występują elementy nawiązujące lub zachęcające do hazardu

Darmowa aplikacja PEGI dostępna jest zarówno na urządzenia działające w systemie Android, Windows 7 Phone, jak i na iPhony/iPody/iPady. Aplikacja ta umożliwia użytkownikom przeglądanie bazy wszystkich gier sklasyfikowanych w systemie PEGI (ponad 16 tysięcy).

- ✓ Z góry ustal, w co, jak długo i kiedy Twoje dziecko może grać.
- ✓ Poszukaj streszczenia lub opisu treści gry, a najlepiej sam w nią najpierw zagraj.
- ✓ Graj ze swoimi dziećmi, nadzoruj je podczas gry i rozmawiaj o ich doświadczeniach.
- ✓ Wyjaśnij im, dlaczego niektóre gry nie są dla nich odpowiednie.
- ✓ Pamiętaj, że niektóre gry internetowe umożliwiają pobieranie dodatków, które mogą zmienić treść gry i jej klasyfikację wiekową.
- ✓ Gry internetowe mogą być rozgrywane z udziałem wielu uczestników, co naraża dzieci na kontakt z nieznanymi osobami. Powiedz dzieciom, aby nie podawały swoich danych i mówiły Ci o niewłaściwych zachowaniach innych graczy.

6. Kiedy kupujesz przez internet

Zanim zawrzemy umowę online

Specyfika zakupów online, brak obecności stron umowy przy jej zawieraniu, może powodować problemy. Europejskie Centrum Konsumenckie przypomina, by przed dokonaniem zakupu upewnić się, czy mamy do czynienia z przedsiębiorcą, gdyż w przeciwnym razie nie będziemy mogli korzystać z uprawnień wynikających z ustaw konsumenckich. Kluczowe jest ustalenie, czy sprzedawca działa legalnie i czy jest wiarygodny (wpis do KRS, certyfikaty zaufania itp.).

Prawa związane z zakupami w sieci

Najpóźniej w chwili wyrażenia przez konsumenta woli związania się umową przedsiębiorca musi poinformować konsumenta m.in. o: swoim adresie, danych rejestrowych, czy prawie do odstąpienia od umowy. Każdy sprzedawca odpowiada za sprzedany przedmiot w terminie 2 lat od dnia dostarczenia konsumentowi towaru. Rzecz zakupiona winna przede wszystkim odpowiadać opisowi zawartemu w ofercie oraz nadawać się do celu określonego w umowie. Konsument może żądać w kolejności naprawy/wymiany rzeczy oraz obniżenia ceny/odstąpienia od umowy. Warto dodać, że mogą istnieć także niezależne od opisanych uprawnienia wynikające z gwarancji (najczęściej producenta).

Sprzedana rzecz powinna zostać wydana niezwłocznie, nie później niż w terminie 30 dni od daty zawarcia umowy – chyba że uzgodniono inaczej. Od umowy takiej możemy odstąpić w ciągu 14 dni od otrzymiania towaru lub rozpoczęcia świadczenia usługi, nie musząc podawać przyczyny.

Nie zawsze jednak można od umowy odstąpić, np.: w przypadku, gdy kupujemy nagrania dźwiękowe lub wizualne albo programy komputerowe dostarczane w zapieczętowanym opakowaniu.

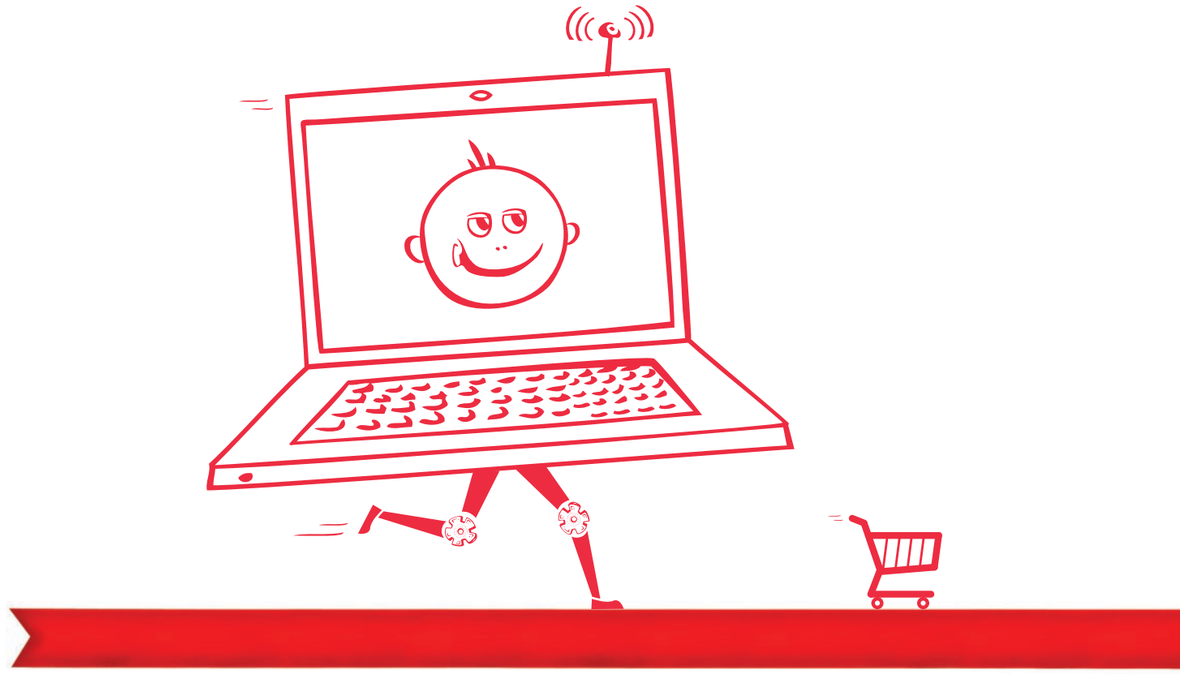
Kiedy transakcja się komplikuje…

Przede wszystkim należy złożyć reklamację. Jeśli nie przyniesie ona spodziewanego rezultatu polecamy skorzystanie z wyszukiwarki pomocnych instytucji na stronie www.uokik.gov.pl.
Gdy skarżony sklep ma swoją siedzibę poza granicami Polski, ale w UE, Islandii i Norwegii, sugerujemy zgłosić skargę do ECK, będącego członkiem sieci ECC-Net – www.konsument.gov.pl.

Kupując w Internecie:

- ✓ Przed dokonaniem zakupu, upewnij się, czy sprzedawca działa legalnie i czy jest wiarygodny (czy posiada wpis do KRS, certyfikaty zaufania, itp.). Podejrzenia powinien wzbudzić brak danych kontaktowych oraz brak w regulaminie informacji na temat procedury reklamacyjnej.
- ✓ Sprzedający ma obowiązek potwierdzić na piśmie wszelkie istotne informacje dotyczące m.in.: całkowitego kosztu zamówienia oraz prawa odstąpienia od umowy.
- ✓ Sklep internetowy musi zrealizować zamówienie w terminie 30 dni.
- ✓ Jeśli nasza reklamacja nie przyniesie oczekiwanego rezultatu – skorzystajmy z wyszukiwarki instytucji chroniących konsumentów dostępnej na stronie www.uokik.gov.pl.
- ✓ W przypadku kiedy skarżony sklep ma siedzibę poza granicami Polski – zgłośmy skargę do ECK, www.konsument.gov.pl.

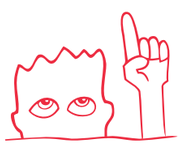
Europejskie Centrum Konsumenckie ECC-Net

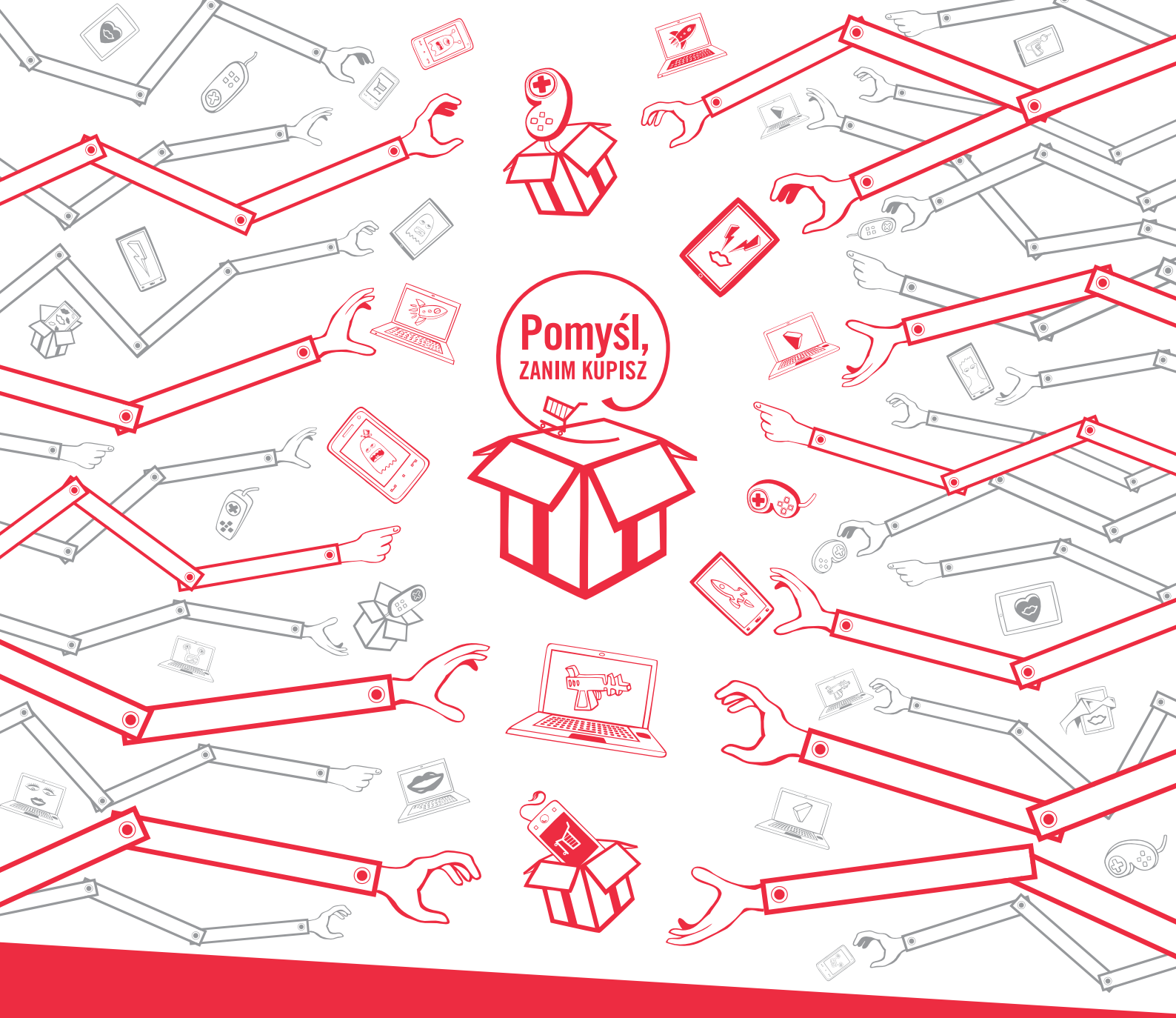


Dziecko – internetowym konsumentem

Młodzi użytkownicy sieci stają się coraz aktywniejszymi konsumentami. 12 proc. użytkowników internetowej porównywarki cen Ceneo.pl to osoby poniżej 18 roku życia (Ceneo.pl, 2011). 15 proc. nastolatków posiada konto w serwisie aukcyjnym, poprzez które trzy razy częściej kupuje produkty, niż je sprzedaje. Najmłodsi klienci kupują przede wszystkim odzież i akcesoria. Bardzo częstym zakupem są także multimedia - ponad 70 proc. osób w wieku 15-18 lat zakupiło przez internet telefony, smartfony czy tablety, a blisko 77 proc. sprzęt komputerowy (Gemius, 2014).
Co czwarte dziecko przyznało, że korzysta z kont albo kart kredytowych rodziców bez ich wiedzy, a jedynie 17 proc. rodziców deklaruje, że wie o internetowych zakupach swoich dzieci (Horton, 2011).

Ustal wspólnie z dzieckiem zasady zakupów przez internet. Przypomnij mu zasady bezpieczeństwa i naucz rozsądnego gospodarowania kieszonkowym.





więcej na: www.zanimkupisz.saferinternet.pl

bezpłatne konsultacje: 800 100 100 telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci