Bezpieczne dziecko w sieci

Porady dla rodziców dotyczące bezpieczeństwa dziecka w Internecie

ENJOY SAFER TECHNOLOGY™

Dzieci to nasza przyszłość. W firmie ESET wiemy o tym doskonale, ponieważ też jesteśmy rodzicami - tak jak Ty. My także czujemy potrzebę prowadzenia naszych pociech przez życie i chronienia ich przed ewentualnymi niebezpieczeństwami i wiemy, że współczesne rodzicielstwo stawia przed opiekunami nowe wyzwania, którym niełatwo sprostać.

Wraz z rozwojem technologii i urządzeń mobilnych (smartfonów i tabletów) oraz szybką ewolucją samego języka, naszpikowanego terminologią technologiczną, rodzice odczuwają ogromną presję – muszą sami bardzo szybko uczyć się nowych rzeczy, by skutecznie edukować o nich swoje dzieci.

Rady zawarte w niniejszym podręczniku nie stanowią zestawu niepodważalnych reguł. Wszystkie teksty zostały przygotowane w taki sposób, by wskazać Tobie – rodzicowi – kluczowe obszary, na jakie musisz zwrócić uwagę, by zapewnić dziecku bezpieczeństwo podczas korzystania z Internetu.

Kto powinien rozmawiać z dziećmi?

Bez względu na to jak bardzo jest to dla Ciebie niekomfortowe, tą osobą powinieneś być właśnie Ty.

Przez całe dzieciństwo Twoja córka lub syn spotkają ludzi, którzy będą odgrywali ważne role w ich życiu np. krewni, przyjaciele czy nauczyciele.

Jednak żadna z tych osób nie przejmie za Ciebie roli rodzica. W oczach dziecka to Ty jesteś osobą, która zna wszystkie odpowiedzi i która jest w stanie mu pomóc – szczególnie w sytuacjach, gdy czuje się zagubione i bezradne.

Kiedy powinieneś porozmawiać ze swoim dzieckiem?

Teraz. Albo najszybciej jak to jest możliwe.

Gdy tylko Twoje dziecko dorasta, pojawiają się nowe wyzwania. Twoja dobra rada w nowej sytuacji może okazać się decydująca i może sprawić, że Twoje dziecko podejmie na jej podstawie właściwą decyzję.

Od samego początku dziecko wykazuje zainteresowanie tabletem, smartfonem, komputerem i Internetem. Powinieneś wyjaśnić dziecku, że wszystko czego nauczyło się w życiu codziennym o bezpieczeństwie dotyczy także Internetu. Innymi słowy - środki się zmieniają, ale zagrożenia wciąż pozostają takie same.

Rodzice uczą dzieci i sami zdobywają od nich nową wiedzę

Czy czujesz, że Twoje dziecko wie więcej o komputerach i smartfonach niż Ty sam? Nie jesteś jedynym rodzicem, który boryka się z tego typu kompleksami.

O ile obecne pokolenie wydaje się „rodzić ze smartfonem w dłoni", to wielu dorosłych umiejętności związane z obsługą najnowszych gadżetów zdobywa w późniejszym czasie. Nie oznacza to jednak, że Twoje dziecko powinno być jedyną osobą potrafiącą kontrolować wszystkie urządzenia w Twoim domu.

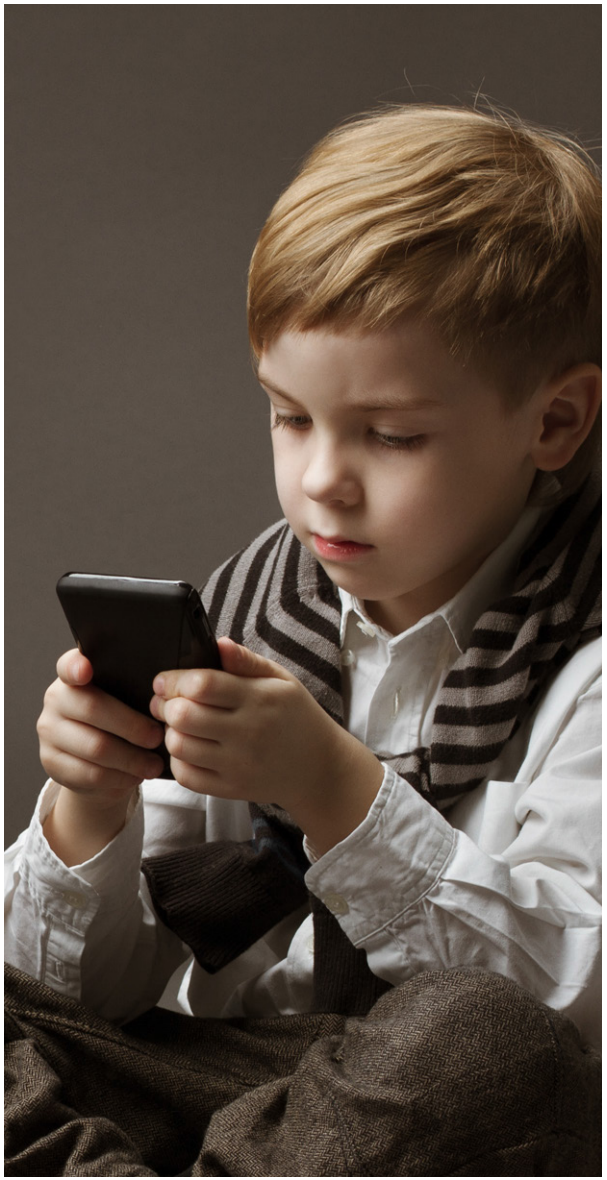
Pamiętaj, że wiedza o tym jak używać Internetu nie jest tym samym co rozumienie konsekwencji i niebezpieczeństw z tym związanych.

Nie ma konieczności, abyś jako rodzic wiedział o świecie wirtualnym więcej niż Twoje dziecko. Ale powinieneś potrafić zidentyfikować moment, w którym Twoja pociecha przekracza pewne ustalone wcześniej granice lub napotka na coś niebezpiecznego. Twoim zadaniem, jeśli sam nie potrafisz tego zrobić, jest wtedy zorganizowanie rozmowy z kimś bardziej doświadczonym w nowych technologiach.

Ogromnie ważne jest, aby dziecko było stroną w rozmowie. Dlatego też należy stworzyć atmosferę, w której Twoja pociecha swobodnie będzie mogła zadawać pytania i przyswajać wszystkie nowe informacje.

Wiek dziecka, a aktywność w Internecie

Poniżej przedstawiamy zestawy porad, na które warto zwrócić uwagę by Twoje dziecko było bezpieczne w Internecie. Skorzystaj z tych odpowiednich dla wieku Twojej pociechy.



DZIECI DO 10 ROKU ŻYCIA

1. Towarzysz dziecku podczas pierwszych doświadczeń w Internecie

Upewnij się, że jesteś w pobliżu, podczas gdy Twoje dziecko stawia pierwsze kroki w wirtualnym świecie. To idealny moment, by być przewodnikiem w tej niezwykłej przygodzie.

2. Ustal warunki korzystania z Internetu

Jako rodzic powinieneś ustalić pewne zasady. Dobrą praktyką jest kontrola czasu i godzin w jakich dziecko korzysta z Internetu.

3. Bądź dobrym przykładem

Dzieci zazwyczaj biorą przykład ze swoich rodziców. Dotyczy to zarówno życia codziennego jak i aktywności w Internecie. Dobre nawyki członków rodziny w szybkim czasie przełożą się na dobre nawyki dzieci.

DZIECI W WIEKU 11 – 14 LAT

1. Używaj narzędzi kontroli rodzicielskiej

Skorzystaj z możliwości oferowanych przez najnowsze technologie. Narzędzie ESET Parental Control umożliwia blokowanie pojedynczych stron Internetowych oraz całych kategorii witryn zawierających potencjalnie niebezpieczne dla dzieci treści. Pozwala także na ustalenie limitu czasu korzystania z Internetu i gier. Jednocześnie ESET Parental Control nie ogranicza swobody dziecka - daje możliwość poproszenia rodzica o udostępnienie konkretnych stron, które są blokowane i z których dziecko chciałoby skorzystać.

2. Naucz dziecko, aby nie ujawniało w sieci informacji mogących je zidentyfikować

Niezwykle ważne jest, aby uświadomić dziecko, że w wirtualnym świecie nie każdy jest przyjacielem, a niektóre osoby mogą chcieć je skrzywdzić.

Wyjaśnij niebezpieczeństwa związane z ujawnie--niem swojego adresu, numeru telefonu oraz aktywności szkolnych i poza szkolnych. Ustal jasną regułę, by dziecko prosiło Cię o zgodę przed publikowaniem swoich zdjęć.

3. Prowadź otwarty dialog

Zachęć swoje dziecko, aby było otwarte i swobo--dnie pytało Cię o rzeczy napotkane w Internecie. Jeśli to możliwe, ustaw komputer w miejscu, w którym większość czasu spędza cała rodzina, i gdzie mogłoby korzystać z niego pod Twoim nadzorem (np. kuchnia, salon).

DZIECI W WIEKU 15 – 18 LAT

1. Nikt nie powinien znać ich hasła

Doskonale wiemy, jak złożeni potrafią być nastolatkowie, ale upewnij się, że Twoje dziecko zna dobre praktyki związane z hasłami dostępu. Przedstaw mu zasadę, by hasło traktować tak samo jak klucz do Waszego domu – nikt poza nim nie powinien go mieć.

Szanuj prywatność swojego nastoletniego już dziecka, ale zadbaj o zapewnienie z jego strony, że nigdy nie poda hasła obcej osobie i nie udostępni go w świecie realnym czy wirtualnym.

2. Natychmiast zgłaszaj przypadki stalkingu i cyberprzemocy

Wróć na chwilę pamięcią do czasów szkolnych. Przypominasz sobie osoby, które dokuczały innym w szkole? W dzisiejszych czasach wiele z nich przeniosło swoje działania do Internetu.

Uświadom dziecko, że każde niepożądane działanie i zachowanie ze strony osób trzecich winno być natychmiast zgłaszane rodzicom.

3. Transakcje finansowe - tylko dla dorosłych

Zakupy w Internecie nie stanowią problemu pod warunkiem, że dokonywane są w bezpieczny sposób. Dopóki nie masz pewności czy Twoje dziecko w pełni rozumie konieczność stosowania środków ostrożności, powinieneś zobowiązać go, aby tego typu transakcje dokonywane były wyłącznie pod Twoim nadzorem.

Słownik cyberbezpieczeństwa

W domu lub w szkole

Mimo tego, że odpowiedzialność za bezpieczeństwo dziecka w Internecie spoczywa głównie na rodzicach, nie oznacza to, że musisz radzić sobie z tym sam.

Warto sprawdzić czy tego typu zagadnienia poruszane są w szkole. Jeżeli takie zajęcia prowadzone są przez nauczyciela o silnym autorytecie, może on być wzorem do naśladowania dla dzieci, które mają obawy lub wątpliwości by poruszać temat bezpieczeństwa w sieci z rodzicami. Jeśli takich zajęć szkoła nie organizuje warto przekonać do tego wychowawcę lub dyrekcję placówki.

Kontrola rodzicielska

Wyobraź sobie, że posiadasz program zarządzający dostępem do Internetu w smartfonie lub tablecie, których pozwala na korzystanie z sieci w określonych godzinach, blokuje wybrane kategorie stron internetowych, kontroluje używanie gier i pozwala lokalizować dziecko w sytuacjach alarmowych. Takie oprogramowanie nazywane jest kontrolą rodzicielską i daje możliwość m.in. kontrolowania aktywności Twojego dziecka w Internecie i stosowania się przez nie do ustalonych wcześniej reguł.

Ważne by tego typu program dawał dziecku możliwość komunikacji - zbyt restrykcyjne i autorytarne ograniczenia mogą zachęcać pociechę do prób ich ominięcia.

Portale społecznościowe

Pomyśl o wszystkich kolegach ze szkoły i znajomych jakich kiedykolwiek poznałeś. Umieść ich w jednym pomieszczeniu i daj im możliwość powiedzenia co robią w danym momencie, pokazywania zdjęć z wakacji lub ulubionych filmów wideo. Mniej więcej tak działają dzisiejsze portale społecznościowe. Pozwalają użytkownikom organizować wydarzenia, komunikować się, dzielić zdjęciami i filmami oraz łączyć się w grupy.

Ten mikrokosmos, który byś stworzył byłby zaledwie małą częścią ogromnej struktury tworzonej przez setki milionów użytkowników mogących tworzyć interakcje. Dlatego korzystanie z portali społecznościowych posiada wiele zalet, ale również obarczone jest wieloma ryzykami.

Główne zagrożenia

Złośliwe oprogramowanie

Jego celem jest uszkodzenie komputera na różne sposoby. Programy te mogą zaszyfrowywać pliki znajdujące się na komputerze i szpiegować Ciebie i Twoje dziecko, a nawet pobierać inne złośliwe aplikacje.

W większości przypadków zainfekowanie powodowane jest błędami użytkowników (lub ich dzieci) – musisz uwierzyć na słowo, cyberoszuści dobrze wiedzą jak wzbudzić zaufanie i skłonić np. do kliknięcia w zainfekowany wirusem załącznik wiadomości email.

Stosując sprawdzone rozwiązania zabezpieczające i postępując zgodnie z dobrymi praktykami, możesz zminimalizować ryzyko zainfekowania komputera.

Spam

Z pewnością miałeś już z nim do czynienia. To wszystkie niechciane „wiadomości śmieci" wypełniające Twoją skrzynkę pocztową każdego dnia.

Zazwyczaj tego typu wiadomości zawierają reklamę zachęcającą do skorzystania z „niepowtarzalnej" oferty i odwiedzenia strony, mogącej zawierać potencjalnie szkodliwe pliki.

Scam

To podstępne działania prowadzone w Internecie przybierające różne formy takie jak spam czy techniki socjotechniczne. Atakujący mogą próbować coś sprzedać, zachowywać się jak znajomi lub podszywać się pod bank, podczas gdy jedyne na czym im zależy to pozyskanie poufnych danych. Wiadomości proszące o login i hasło do portali społecznościowych to kolejny przykład scamu.

Cyberprzemoc

To wrogie zachowanie skierowane jest wyjątkowo często w stronę dzieci. Ofiara bywa zastraszana i poniżana w sieci przez rówieśników np. poprzez publikację zdjęć lub filmów, przedstawiających atakowaną osobę w niekorzystny dla niej sposób. Zachowanie to jest częste u nastolatków. Cyberprzemoc wywiera ogromną presję psychiczną, która może doprowadzić do traumy lub popchnąć nawet do samobójstwa. Ma miejsce najczęściej w serwisach społecznościowych, ale same smartfony, a nawet konsole do gier również mogą być wykorzystane do realizacji tego typu działań.

Uwodzenie

Mamy z nim do czynienia w sytuacji, gdy dorosła osoba namawia dziecko do aktywności seksualnej stwarzającej atmosferę zaufania, budując jednocześnie więź emocjonalną. W wielu przypadkach atakujący (głównie osoby dorosłe) podają się za dzieci, aby ugruntować bliską relację i doprowadzić do spotkania. Ważne jest, aby rodzice zawsze wiedzieli kim są osoby wchodzące z dzieckiem w interakcje przez Internet.

Sexting

Sprowadza się do wiadomości (SMS, MMS, maile, czat) zawierających treści erotyczne. Wraz z rozwojem technologii sexting ewoluował do procesu wymiany zdjęć i filmów video i stał się dość powszechną praktyką.

Wykradanie informacji

Wszystkie informacje przesyłane nieostrożnie przez Internet mogą zostać przechwycone przez osoby trzecie. Informacje te są często celem ataków. Zazwyczaj pożądane są dane personalne Twoje lub Twoich dzieci. Nieostrożne działania mogą prowadzić nawet do kradzieży.

Porady ekspertów

1. Używaj narzędzi do kontroli rodzicielskiej

Mogą one być stosowane z poziomu przeglądarki internetowej lub oprogramowania antywirusowego. Narzędzia te dostępne są m.in. od dziewiątej wersji **ESET SMART SECURITY** lub jako dedykowana aplikacja **ESET PARENTAL CONTROL** dla smartfonów i tabletów z systemem Android. Narzędzia kontroli rodzicielskiej udostępniane są również w konsolach, takich jak NINTEDO WII czy XBOX ONE.

2. Nie pozwalaj swojemu dziecku przesyłać poufnych informacji przez Internet

Dane wrażliwe nie powinny być wysyłane przez maila lub czat. Zwróć dziecku uwagę, że banki nie stosują tego kanału informacji, aby potwierdzić dane konta lub numeru PIN. Jeśli ktoś poprosi Twoje dziecko o podanie tego typu informacji za pośrednictwem maila lub czatu, Twoja pociecha musi wiedzieć, że to prawdopodobnie próba oszustwa.

3. Nie odpowiadaj na wiadomości o charakterze stalkingu

Jeżeli Twoje dziecko padło ofiarą cyberprzemocy – nie powinno odpowiadać na działania stalkera (prześladowcy). Wyjaśnij dziecku, że taka osoba chce sprowokować u niego niechciane zachowanie. O takich działaniach koniecznie poinformuj odpowiednie organy i nie usuwaj otrzymanych wiadomości jako dowód zdarzenia.

4. Nie wszystko w sieci jest prawdą

Nie wszystkie informacje umieszczone w sieci pochodzą z wiarygodnych źródeł i ważne, aby dziecko to wiedziało. Załóż własnego bloga i pokaż dziecku jak łatwo jest stworzyć przestrzeń, której zawartością można dowolnie manipulować.

5. Otwarty dialog

Komunikacja z dzieckiem odgrywa ważną rolę w zapewnianiu mu bezpieczeństwa. Dużo bardziej efektywne jest zachęcenie dziecka do wyrażenia swoich lęków niż karanie go bez tłumaczenia szkodliwości danego działania. Dobra relacja z dzieckiem i otwarty dialog mogą być kluczem do osiągnięcia wspólnego sukcesu – bezpieczeństwa w sieci.

6. Co raz trafi do Internetu – pozostaje w nim na zawsze

Uświadom dziecko, że zdjęcie raz umieszczone w Internecie pozostaje w nim na zawsze – a co więcej - może być udostępnianie przez obce osoby. Wskaż negatywne konsekwencje umieszczania prywatnych zdjęć w Internecie i powiedz, że dotyczy to zarówno portali społecznościowych, komunikatorów, jak i komentarzy na forach internetowych.

5 dodatkowych rad dla Rodziców

1. Załóż w systemie Windows nowe konto dla swojego dziecka. To pierwszy krok, aby aktywnie kontrolować jego obecność w Internecie. Rola administratora powinna być zawsze po stronie dorosłego.

2. Aktualizuj oprogramowanie antywirusowe i narzędzia kontroli rodzicielskiej.

3. Monitoruj historię przeglądanych stron. Pusta historia to dobry pretekst do rozmowy.

4. Upewnij się, że nieużywana kamera internetowa jest odłączona lub zasłonięta.

5. Sprawdź ustawienia profilu swojego dziecka na portalu społeczno-ściowym. Upublicznianie informacji bez ograniczeń może być ryzykowne.

Wnioski końcowe

Odmawianie dziecku dostępu do nowoczesnych technologii i Internetu nie jest najlepszym rozwiązaniem. Nowinki są i zapewne będą częścią codziennego życia Twojego dziecka i istotnym elementem jego rozwoju.

Zamiast nakładać ograniczenia naucz dziecko korzystać z dobrodziejstw współczesnej technologii w sposób bezpieczny dla niego i stań się istotnym łącznikiem pomiędzy dzieckiem, a urządzeniem podłączonym do Internetu.

Warto dodać, że omówione w niniejszym poradniku ryzyka dotyczą również dorosłych, a opisane środki ostrożności mogą być stosowane niezależnie od sytuacji i wieku.

Więcej informacji znajdziesz na:
www.twojedzieckowsieci.pl

Twoje dziecko w sieci .pl