# Najważniejsze zalecenia dla rodziców pragnących nauczyć swoje dzieci bezpiecznego korzystania z technologii IT

## Zdrowie

- **Stwórz dziecku odpowiednie warunki do pracy z komputerem**
  Biurko, lampka, krzesło z oparciem dostosowane do wzrostu dziecka oraz monitor ustawiony na wysokości wzroku pozwolą Twemu dziecku pracować i bawić się z komputerem w wygodnej pozycji. Pamiętaj jednak o tym, że zaleca się, aby dzieci do 12 roku życia nie miały komputera w swoim pokoju.
- **Pamiętaj o nadgarstkach**
  Dłonie i nadgarstki dziecka obsługującego myszkę lub klawiaturę nie powinny być oparte o kant biurka. Zadbaj o odpowiednią podkładkę, na której Twoje dziecko będzie mogło wygodnie oprzeć ręce.
- **Maksymalnie 1,5 godziny dziennie**
  Świat zabaw z komputerem czy konsolą do gier jest niezwykle wciągający. Rób zatem wszystko, aby Twoje dziecko nie zapominało o świecie, w którym żyjemy. Trzyletnim dzieciom wystarczy kwadrans, a nastolatki nie powinny więcej niż półtorej godziny dziennie przebywać przed monitorem czy telewizorem.

## Bezpieczeństwo IT

- **Hasło to gwarancja bezpieczeństwa**
  Naucz dziecko, żeby nigdy nie ujawniało nikomu (poza rodzicami oczywiście) używanych przez nie haseł dostępu do usług sieciowych. Podsłuchanie czy nawet podpatrzenie hasła logowania np. do serwisu społecznościowego przez osobę o złych intencjach może skutkować kradzieżą tożsamości i podszywanie się pod Twoje dziecko w celu obrażania innych czy ośmieszenia właściciela konta. Pamiętaj, aby stosować hasła bezpieczne, tzn. zawierające minimum 8 znaków, wśród których znajdą się poza literami także cyfry i znaki specjalne.
- **Korzystamy z sieci publicznych tylko wyjątkowo**
  Połączenie się z siecią bezprzewodową udostępnioną w miejscu publicznym lub korzystanie z kafejek internetowych może wiązać się z ryzykiem "podsłuchiwania" przesyłanych przez nas danych przez innych użytkowników tej sieci. Wytłumacz dziecku, żeby tylko w warunkach niezbędnej konieczności używało takich sieci do łączenia się z usługami wymagającymi przesłania swoich danych do logowania i haseł.
- **Antywirusy i firewall są niezbędne, ale nie gwarantują bezpieczeństwa**
  To bardzo ważne, aby na komputerze Twojego dziecka znalazło się oprogramowanie chroniące przed atakami wirusów czy hackerów. Naucz dziecko poprawnego reagowania na komunikaty zgłaszane przez takie oprogramowanie i dbania o częste aktualizowanie definicji i reguł bezpieczeństwa. Pamiętaj jednak, że żadne oprogramowanie nie daje stuprocentowego bezpieczeństwa - współczesne programy przechwytujące znaki wpisywane z klawiatury bardzo często potrafią działać niezauważone! Poproś dziecko, aby zgłaszało Ci wszystkie podejrzane zachowania czy spowolnienia funkcjonowania systemu.
- **Bezpieczna sieć bezprzewodowa**
  Jeżeli posiadasz w domu sieć bezprzewodową, to koniecznie zabezpiecz dostęp do niej hasłem. Pamiętaj, aby hasło było bezpieczne i zaszyfrowane przy użyciu standardu WPA2, ponieważ takie hasło najtrudniej złamać.

## Zachowania

- **Ustal konkretne reguły**
  Pamiętaj o zasadach dobrej organizacji życia rodzinnego. Korzystanie przez dziecko ze sprzętu przenośnego nie powinno mieć miejsca np. podczas posiłku, na rodzinnym spacerze czy podczas kąpieli. Wyznacz dziecku konkretne reguły dotyczące miejsca i czasu korzystania z urządzeń IT.
- **Sprzęt do użytku domowego**
  Wytłumacz dziecku, że korzystanie ze sprzętu poza domem, bez obecności rodziców, może narazić je na próbę kradzieży. Chwalenie się laptopem, przenośną konsolą do gier czy telefonem komórkowym w miejscach publicznych może wiązać się z zagrożeniem bezpieczeństwa dziecka.
- **Ufajmy ale nadzorujmy**
  Twoje dziecko powinno mieć poczucie prywatności w swoich działaniach - jeżeli współdzielisz komputer domowy, to stwórz mu jego własny profil w systemie, wyznacz katalog na dysku, w którym będzie mogło przechowywać swoje dane i instalować swoje aplikacje czy gry. Staraj się jednak nadzorować to, do czego dziecko wykorzystuje komputer. Jeżeli nie wystarczy sporadyczne dyskretne zerkanie na ekran, to z pomocą mogą przyjść Ci liczne programy monitorujące zachowania użytkowników (także bez ich wiedzy).
- **Gry odpowiednie do wieku**
  Kupując dziecku grę koniecznie zwróć uwagę na jej oznakowanie. Na każdym opakowaniu z grą powinny być umieszczone ikony systemu klasyfikacji gier PEGI, informujące o minimalnym wieku graczy, dla których dana gra została przeznaczona oraz o zawartych w grze ewentualnych elementach przemocy, wulgaryzmach, kontekstach erotycznych czy scenach, które mogą wystraszyć dzieci. Klasyfikację gry możesz sprawdzić także w internecie na stronie www.pegi.info/pl.

## Telefon komórkowy

- **Korzystanie z Internetu może być kosztowne**
  Jeżeli nie chcesz być zaskoczony ogromnym rachunkiem telefonicznym, to pamiętaj o wytłumaczeniu swojemu dziecku, w jaki sposób są rozliczane połączenia internetowe z telefonu komórkowego. Wytłumacz mu też zasady pobierania gier z serwisów, których reklamy najczęściej można spotkać w pismach dziecięco-młodzieżowych.
- **Zdjęcia i filmy tylko za zgodą**
  Poucz dziecko, aby nigdy nie robiło zdjęć czy nie nagrywało filmów z udziałem innych osób w sytuacjach, w których mogą one sobie tego nie życzyć. Powiedz, aby głośno i aktywnie protestowało, jeżeli same znajdzie się w takiej sytuacji. Wytłumacz też, że przed zamieszczeniem w sieci zdjęć czy filmów z udziałem innych osób należy wcześniej poprosić je o zgodę.
- **Konkursy sms-owe są dla dorosłych**
  Upewnij się, czy Twoje dziecko wie, że udział we wszystkich konkursach związanych z wysyłaniem wiadomości SMS dotyczy wyłącznie osób dorosłych. Wytłumacz mechanizmy działania takich konkursów i ryzyko z nimi związane. Szczera rozmowa pozwoli zaoszczędzić mnóstwo kłopotów.
- **W sytuacji bez wyjścia lepiej oddać telefon**
  Chcąc pozostawać w ciągłym kontakcie ze swoim dzieckiem godzimy się niestety na podwyższenie ryzyka dla jego bezpieczeństwa. Naucz dziecko, że jeżeli zostałoby kiedyś ofiarą napadu i nie mogłoby liczyć na natychmiastową pomoc, to dla ratowania zdrowia i życia lepiej by było, aby zdecydowało się oddać napastnikowi telefon komórkowy i inne wartościowe rzeczy, a dopiero niezwłocznie po odejściu sprawcy zaczęło wołanie o pomoc.

## Serwisy społecznościowe i komunikatory

- **Czy na pewno warto tam być?**
  Porozmawiaj z dzieckiem o tym, jakie przesłanki kierują jego chęcią do uczestnictwa w portalu społecznościowym. Wytłumacz mu zasady działania takiego portalu. Nie warto kierować się wyłącznie modą.

- **Pseudonim zamiast imienia i nazwiska**
  Jeżeli zakładasz jednak dziecku jego własne konto w serwisie społecznościowym lub w komunikatorze, to nie używaj prawdziwego imienia i nazwiska. Twoje dziecko nie szuka przecież kontaktów biznesowych, a swoich znajomych z łatwością odnajdzie, korzystając z pseudonimu, który wspólnie wymyślicie.

- **Bez danych osobowych i kontaktowych**
  Pamiętaj o tym, że profil Twojego dziecka w serwisie społecznościowym może być przeglądany także przez osoby postronne. Wytłumacz zatem dziecku, aby nie podawało Waszych danych osobowych i kontaktowych. Do kontaktów ze znajomymi w zupełności wystarczą usługi udostępniane przez portal.

- **Akceptujcie wspólnie publikowane zdjęcia**
  Ustal ze swoim dzieckiem, jakich zdjęć nie powinno zamieszczać w serwisie społecznościowym. Przestrzeż je przede wszystkim przed umieszczaniem zdjęć mogących ośmieszyć Twoje dziecko wśród jego znajomych lub ich prowokować. Akceptujcie wspólnie zdjęcia przed ich opublikowaniem i pamiętajcie, aby w miarę możliwości tło zdjęć nie pozwalało na identyfikację Waszych danych czy miejsca zamieszkania.

- **Nieznajomym mówimy „nie”!**
  Naucz swoje dziecko, aby nie dodawało do grona swoich znajomych osób, których nie zna. Poproś, aby powiadamiało Cię o każdej wątpliwości i o każdej podejrzanej próbie kontaktu.

- **Po drugiej stronie jest człowiek**
  Przypominaj dziecku, że kontakty ze znajomymi poprzez serwisy społecznościowe, czaty czy komunikatory to nie gra, tylko prawdziwa rozmowa. Słowa wysłane w sieć mogą ranić tak samo, jak przy osobistym kontakcie. Naucz dziecko nie obrażać i nie naśmiewać się z innych, aby pozostało w dobrych stosunkach ze swoimi znajomymi.

## Email

- **Stwórz fikcyjną skrzynkę**
  Jeżeli zgadzasz się, aby Twoje dziecko posiadało własny adres email i używało go np. do rejestrowania się w portalach przeznaczonych dla dzieci, to najlepiej załóż mu konto, w którego adresie zamiast imienia i nazwiska użyjesz pseudonimu lub jakiegoś określenia, z którym dziecku będzie miło się utożsamiać. Im mniej bowiem danych osobowych umieścicie w sieci, tym lepiej...

- **Ważne informacje przesyłaj zaszyfrowane**
  Trzeba mieć świadomość tego, że wiadomości email mogą być przechwytywane przez osoby postronne. Pamiętaj więc i naucz tego swoje dziecko, aby wszystkie ważne, zawierające istotne dla naszego bezpieczeństwa wiadomości (hasła, dane osobowe itp..) przesyłać w postaci zaszyfrowanej. Najprościej zapisać taką wiadomość w pliku tekstowym, po czym skompresować go programem typu ZIP z użyciem bezpiecznego hasła, które podamy odbiorcy np. przez telefon. Zastanówmy się też, czy naprawdę warto wysyłać za pomocą poczty elektronicznej inne pozornie niegroźne informacje, np. o naszej nieobecności w domu, o problemach z systemem alarmowym czy też dołączać fotografie nowego samochodu wraz ze skanami jego dokumentów.

- **Usuwaj podejrzane wiadomości z załącznikami przed ich otworzeniem**
  Pomimo posiadania oprogramowania antywirusowego, zwróć uwagę dziecka na konieczność usuwania podejrzanych wiadomości (czasami mogą one nawet udawać wiadomości od osób, które znamy), zwłaszcza takich, które zawierają załączniki. Wiadomości takie należy kasować nawet przed podejrzeniem ich zawartości.

- **Ostrzegaj o fałszywych emailach**
  Ponieważ najsłabszym ogniwem w każdym systemie bezpieczeństwa jest człowiek, stąd też najwięcej skutecznych ataków na bezpieczeństwo danych wykorzystuje elementy inżynierii społecznej. Przestrzeż swoje dziecko o tym, że wiadomości email mogą być w łatwy sposób fałszowane. Naucz je potwierdzać dodatkowo (np. przez telefon) niecodzienne prośby wyrażone przez znajomych w wiadomościach email, np. prośba siostry o podanie kodu do alarmu, który zapomniała czy też prośba taty o pozostawienie kluczy pod wycieraczką.

## Przeglądarki internetowe

- **Ochrona przed nieodpowiednimi treściami**
  Pomimo faktu, że przypomina to nieco walkę z wiatrakami, warto zrobić jak najwięcej, aby chronić swoje dziecko przed treściami dla niego nieprzeznaczonymi. Zainstaluj oprogramowanie ochrony rodzicielskiej lub skorzystaj z takich funkcji oferowanych przez przeglądarki internetowe. Pamiętaj jednak, że automatyczne działanie takiego oprogramowania jest mocno przereklamowane i częstokroć odnosi się tylko do stron angielskojęzycznych. Musisz wziąć sprawy w swoje ręce - przyglądaj się, jakich fraz poszukuje w sieci Twoje dziecko i sprawdź, jakie to daje rezultaty. Jeżeli trafisz na stronę, której Twoje dziecko nie powinno oglądać, dodaj jej adres do listy stron blokowanych. Im dłuższa taka lista, tym większa szansa, że Twoje dziecko będzie bezpieczne.

- **Phishing**
  Fałszywe wiadomości email mogą kierować niekiedy do fałszywych stron internetowych, udających prawdziwe serwisy (np. bankowe) w celu przechwycenia naszych danych logowania. Być może nie dotyczy to w dużym stopniu dzieci, ale warto porozmawiać z nimi o tym i wyczulić je na sprawdzanie poprawności adresu strony www, na którą zostaną przekierowane za pomocą łącza z wiadomości email.

- **Nie używaj pirackiego oprogramowania/cracków**
  Koniecznie poinformuj swoje dziecko, że ściąganie i instalowanie pirackiego oprogramowania jest formą kradzieży. Ale to nie wszystko! Mafie na świecie coraz więcej inwestują w tworzenie wirusów, za pomocą których mogą np. przejąć komputer nieświadomego tego użytkownika i wykorzystywać go wielokrotnie do przestępczych operacji. A najłatwiej rozprowadzać takie wirusy wraz z pirackimi wersjami gier i aplikacji oraz tzw. crackami, czyli programami usuwającymi zabezpieczenia licencyjne pożądanego oprogramowania. Korzystanie zatem z takich rozwiązań wiąże się z olbrzymim ryzykiem.

- **Wyszukiwarki i serwisy dla dzieci**
  W internecie można z łatwością znaleźć wyszukiwarki treści przeznaczonych specjalnie dla dzieci - zwłaszcza tych mniejszych. Jest też kilka działających w ten sposób serwisów w Polsce. Ustawienie takiego serwisu jako strony startowej w profilu dziecka oraz dodanie do ulubionych stron kilku sprawdzonych portali z grami i zabawami dla dzieci pomoże dziecku samodzielnie poruszać się po sieci, a Tobie da pewność, że nie spotka tam treści dla niego nieodpowiednich.

- **Nie udostępniaj ważnych serwisów**
  Pamiętaj o tym, że jeżeli umożliwisz dziecku korzystanie z Twojego konta w ważnym serwisie (np. w banku czy serwisie aukcyjnym), to możesz liczyć się z tym, że w Twoim imieniu zostaną dokonane (nawet przypadkowo) nieplanowane operacje finansowe, których być może nie da się anulować. Zastanów się nad tym, zanim pozwolisz dziecku np. skorzystać z Twojego laptopa.