

DZIECKO BEZPIECZNE WŚRÓD NOWYCH TECHNOLOGII

Nowoczesne technologie są nieodłącznym elementem życia młodych ludzi. Nauka, rozrywka, życie społeczne - aktywność młodego pokolenia w XXI wieku toczy się równolegle online i offline. Rozwijanie zainteresowań, rozmowy z rówieśnikami czy odrabianie lekcji to czynności, które dzieci swobodnie realizują w sieci. Dziś trudno znaleźć nastolatka, który potrafiłby obejść się bez Internetu, nie używał komputera, tabletu lub smartfonu.

Nowe technologie dają młodym ludziom wiele możliwości, ale jednocześnie niosą ze sobą nowe wyzwania i zagrożenia. To okno na świat, w którym obok wartościowych treści znaleźć można cały szereg treści niebezpiecznych - dlatego tak bardzo ważne jest, aby rodzice przygotowali dzieci do korzystania z nowych mediów, a aktywność dzieci nie była zupełnie swobodna i pozbawiona nadzoru.

Poniżej zamieszczono zestaw wskazówek dla rodziców, dzięki którym dzieci będą mogły korzystać z ogromnych możliwości nowoczesnych technologii, jednocześnie pozostając bezpiecznymi.

Przede wszystkim:

- Poświęć czas i korzystaj z nowych mediów razem z dzieckiem. Wy tłumacz dziecku, że nie wszystko, co znajduje w sieci jest prawdą i że Internet jest pełen sugestii oraz porad, które mogą być szkodliwe dla jego zdrowia, a nawet życia.
- Zaproponuj bezpieczne i ciekawe strony dostosowane do wieku dziecka.
- Udostępniając dziecku urządzenie z dostępem do Internetu, upewnij się, że jest ono wyposażone w program ochrony rodzicielskiej, kontrolujący dostęp do nieodpowiednich treści. Dostosuj ustawienia narzędzia do wieku dziecka.
- Porozmawiaj z dzieckiem o tym, które dane są wrażliwe i trzeba być szczególnie ostrożnym w ich udostępnianiu. w zależności od wieku dziecka możesz mu wytłumaczyć, do czego mogą być wykorzystywane zbierane przez firmy informacje o nim. Ustal z dzieckiem, że będzie cię informować, jeśli podczas rejestracji w jakimś serwisie wymagane będzie podanie danych osobowych.
- Sprawdź razem z dzieckiem, co można znaleźć o nim w wyszukiwarkach. Jeżeli znajdziecie treści, które mogą mu szkodzić – usuńcie je samodzielnie lub przez administratora danej strony.
- Zainstaluj na komputerze filtr kontroli rodzicielskiej, który ograniczy kontakt dziecka z treściami szkodliwymi, oraz oprogramowanie, które zablokuje wyskakujące okienka.
- Powiedz dziecku o oprogramowaniu do kontroli rodzicielskiej, które jest zainstalowane na urządzeniu. Wy tłumacz dziecku czemu służy dane narzędzie.
- Rozmawiaj z dzieckiem o tym, jakie treści napotyka w Internecie i daj mu możliwość opowiadania o tym, co je niepokoi. Warto wziąć pod uwagę, że dzieci mogą mieć dostęp do Internetu nie tylko w domu, ale też w szkole i miejscach publicz-

nych, gdzie może nie być aktywnych filtrów chroniących przed szkodliwymi informacjami. Dzieci często nie mówią rodzicom o tym, że widziały niepokojące materiały, z powodu obaw przed utratą dostępu do Internetu.

- Zapewnij dziecko, że jeśli coś niepokojącego wydarzy się w trakcie korzystania z urządzeń i Internetu, może zwrócić się do Ciebie z prośbą o pomoc.
- Nie publikuj w sieci wizerunku dziecka nago lub w innych krępujących sytuacjach. Pamiętaj, że materiały, które wrzucasz do sieci pozostaną w niej na długie lata. Zawsze rozważ, czy nie zaszkodzisz nimi w przyszłości swojemu dziecku.
- Nie publikuj w sieci prywatnych informacji na temat swojego dziecka – adresu przedszkola lub szkoły, informacji o trudnościach wychowawczych, przebytych chorobach itp.
- Pamiętaj o ustaleniu z dzieckiem limitu czasu, który może spędzać na używaniu Internetu, tabletu, smartfonu, komputera.

Korzystanie z aplikacji:

- Przedyskutuj z dzieckiem, które aplikacje warto ściągnąć i na co podczas korzystania z nich należy zwracać uwagę. w przypadku dzieci starszych możesz uzgodnić z nimi, które aplikacje mogą instalować samodzielnie.
- Zanim polecisz daną aplikację dziecku, przeczytaj jej opis i zapoznaj się recenzjami innych użytkowników.
- Zapoznaj się z możliwymi ustawieniami ochrony rodzicielskiej na urządzeniu mobilnym, z którego korzysta dziecko. Rozważ wyłączenie możliwości dokonywania zakupów w aplikacjach. Możesz też poszukać specjalnych aplikacji, które wspomagają rodziców w ochronie rodzicielskiej.
- Nie pozwól dziecku na korzystanie z konta w iTunes, App Store lub Google Play, które jest połączone z twoją kartą kredytową. Stwórz dla dziecka oddzielne konto. Możesz ewentualnie podarować dziecku voucher, który pozwoli mu na ściągnięcie płatnych aplikacji lub dokonywanie mikropłatności tylko do pewnej ustalonej wcześniej kwoty.
- Pozwalając dziecku na jednorazowy zakup w ramach aplikacji z App Store zwróć uwagę, że po wpisaniu hasła i dokonaniu zakupu dane te pozostają zapisane w urządzeniu przez 15 minut. To wystarczająco dużo czasu, aby twoje dziecko mogło narazić cię na dalsze wydatki!
- W szczególności uważaj na aplikacje wymagające podania wielu danych osobowych lub dostępu do wielu zasobów urządzenia mobilnego.
- Raz na jakiś czas zrób przegląd aplikacji zainstalowanych na urządzeniu przenośnym i usuń te nieużywane, gdyż mogą one ciągle pracować w tle i korzystać z danych urządzenia.
- Zabezpiecz urządzenie mobilne hasłem/PIN-em, chroniącym je przed dostępem niepowołanych osób.

- Zainstaluj na urządzeniu przenośnym oprogramowanie antywirusowe, które może wykrywać szkodliwe aplikacje.

Przemoc w Internecie:

- Naucz dziecko szacunku do innych i nieobrażania pozostałych użytkowników Internetu.
- Poinformuj dziecko, że to co publikuje w sieci nigdy nie jest w pełni anonimowe i że można dotrzeć do autora komentarza lub wpisu.
- Naucz dziecko, by krytycznie podchodziło do komentarzy w Internecie. Niektórzy publikują kontrowersyjne komentarze, by wywołać agresję.
- Rozmawiaj z dzieckiem na temat przemocy w sieci, przestrzeż je przed podejmowaniem takich działań i zapewnij, że zawsze w sytuacji zagrożenia oferujesz swoją bezwarunkową pomoc.
- Naucz dziecko, że nie należy odpowiadać przemocą na przemoc online.
- 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.
- Poinformuj dziecko o anonimowej ofercie pomocowej Telefonu Zaufania dla Dzieci i Młodzieży: 116 111

Seksting:

- Ciekawość dotycząca seksualności człowieka jest naturalnym etapem rozwoju młodego człowieka. Należy jednak zadbać, aby internetowe treści pornograficzne nie stanowiły jedyne źródła wiedzy na ten temat. Rozsądna i dopasowana do wieku edukacja seksualna zapobiegnie rozwojowi nieprawidłowych postaw i zachowań związanych z seksem.
- Przestrzeż dziecko przed publikowaniem lub przesyłaniem komukolwiek zdjęć o charakterze seksualnym. Naucz je asertywności w kontaktach z rówieśnikami nalegającymi na przesłanie materiałów o charakterze erotycznym i zwróć jego uwagę na możliwe konsekwencje takich działań.
- Rozmawiaj z dzieckiem o seksualności i naucz je szacunku do swojego ciała. Przestrzeż je przed dowodami miłości wysyłanymi w postaci materiałów o charakterze seksualnym.
- Naucz dziecko zabezpieczania dostępu do prywatnych zasobów cyfrowych. Zwróć jego uwagę na konieczność konfiguracji ustawień prywatności w serwisach społecznościowych, możliwość ograniczania dostępu do prywatnych zdjęć i filmów wybranym osobom oraz zabezpieczenia telefonu lub innych urządzeń mobilnych hasłem dostępu.
- Naucz dziecko dystansu do trendów związanych z erotycznym prezentowaniem się w sieci.

- Poinformuj dziecko, że zawsze może liczyć na twoje zrozumienie i pomoc w sytuacji problemów online, również tych związanych z publikacją wizerunku w sieci.

Czaty i komunikatory:

- Czaty i komunikatory to narzędzia pozwalające twojemu dziecku szybko i bezpłatnie kontaktować się z ważnymi dla niego osobami. Pamiętaj jednak, by uczulić dziecko, aby nie dzieliło się online wszystkimi informacjami, o jakie proszą je rozmówcy.
- Sprawdź właściwości czatu i komunikatorów, z których korzysta twoje dziecko: czy czat jest moderowany, czy ma ograniczenia wiekowe, czy usługi te dają możliwość zgłaszania niepokojących sytuacji i blokowania agresywnych użytkowników.
- Porozmawiaj z dzieckiem o tym, dlaczego ważne jest, by przestrzegało regulaminu w przypadku czatów mających ograniczenia wiekowe. Jego łamanie może się wiązać z sytuacjami nieprzyjemnymi, trudnymi i niebezpiecznymi, które na długo mogą pozostać w pamięci dziecka.
- Ostrzeż dziecko, by nie dało się namówić na zachowanie, które może spowodować niekłopoty (np. rozebranie się przed kamerką internetową). Po drugiej stronie mogą być osoby, które mogą mieć zupełnie inne intencje niż sądzi dziecko.

Portale społecznościowe:

- Poznaj portale z których korzysta twoje dziecko. Wtedy będziesz mógł szybciej pomóc mu w razie ewentualnego zagrożenia. Możesz też poprosić dziecko, by samo wprowadziło cię do tego świata – tym sposobem dowiesz się o wiele więcej niż podczas samodzielnego zwiedzania serwisu.
- Sprawdźcie wspólnie ustawienia prywatności. Poproś dziecko, aby ograniczyło dostęp do swojego profilu wszystkim tym, których dobrze nie zna.
- Ucz dziecko, aby kontrolowało to, co samo publikuje i to, co publikują o nim inni. Niech regularnie sprawdza informacje na swój temat w Internecie i na bieżąco kasuje ze swojego profilu wszystkie nieodpowiednie komentarze i linki umieszczone przez inne osoby. Niektóre wyszukiwarki (np. Google) pozwalają na ustawienie alertów z wybranymi hasłami (np. naszym imieniem i nazwiskiem), które automatycznie wyślą do nas e-mail, gdy coś na nasz temat pojawi się w sieci.
- Uczul dziecko, że każdy wpis świadczy o nim. Jeśli pisze coś pod wpływem np. silnych emocji to powinno przeczytać post dwa razy zanim go opublikuje.
- Zobacz jakie informacje twoje dziecko ujawnia na profilu i wyjaśnij mu, dlaczego prywatność w Internecie jest bardzo cenna.
- Zwróć uwagę na to, jakie treści umieszcza na portalu twoje dziecko – czasami młodzi internauci nie myślą o ewentualnych przykrych konsekwencjach swoich

czynów. Przypomnij dziecku, że przed oznaczeniem innych osób na publikowanych zdjęciach należy zapytać o ich zgodę.

- Zapytaj dziecko, ilu spośród portalowych „znajomych” zna naprawdę. Wyjaśnij mu, jakie zagrożenia wiążą się z dzieleniem się prywatnymi informacjami z nieznanymi osobami. Przypomnij dziecku, że nie ma obowiązku przyjmowania do grona znajomych wszystkich osób, które je zapraszają.
- Upewnij się, że dziecko wie, jak w danym portalu zgłaszać niepokojące sytuacje lub treści.

Geolokalizacja:

- Uczul dziecko na możliwe konsekwencje podawania swojej fizycznej lokalizacji.
- Zapoznaj się z funkcjami lokalizacyjnymi, oferowanymi przez urządzenie, z którego korzysta dziecko (np. GPS, wifi), i w zależności od wieku dziecka rozważ ich wyłączenie.
- Przejrzyj jakie aplikacje odwołujące się do lokalizacji dziecko ma zainstalowane w telefonie. Zadbaj, aby korzystając z nich przestrzegało granicy dozwolonego wieku. Wyłumacz, dlaczego jest to ważne dla jego bezpieczeństwa i jakie zagrożenia mogą wiązać się z ujawnianiem lokalizacji.
- Jeśli dziecko korzysta z aplikacji społecznościowych, aby logować się do różnych miejsc, upewnij się, że jego profil nie jest otwarty i informacje widoczne są jedynie dla znajomych. Przy okazji przejrzyj razem z dzieckiem jego listę kontaktów, aby upewnić się, że nie ma tam osób przypadkowych.
- Jeśli zdecydujesz się na aplikację śledzącą dziecko, poinformuj je o tym, wytłumacz, jak ona działa i upewnij się, że masz zgodę dziecka. Pamiętaj, że nie jest to narzędzie zastępujące ochronę rodzicielską.

Dodatkowe informacje na temat bezpieczeństwa wśród nowych technologii można znaleźć na stronach:

www.bezpieczneinterneciaki.pl

www.safeinternet.pl

www.best.fdn.pl

Opracowanie: Pedagog SP nr 25,
Katarzyna Piontek