**[Bezpieczeństwo w sieci](http://informatyka.sp2.slupsk.pl/index.php/bezpieczenstwo-w-sieci)**

**Naucz dzieci podstaw związanych z bezpieczeństwem w sieci!**

Jeśli jesteś rodzicem, możesz nauczyć swoje dziecko kilku podstawowych zasad odnośnie bezpiecznego korzystania z Internetu. Oto kilka podstawowych zasad, których rodzice mogą nauczyć swoje dzieci.

**Oto kilka zasad, które dzieci powinny znać i przestrzegać.**

o    **Nie ujawniaj haseł innych osobom.**Nie ujawniaj haseł nawet swoim znajomym.

o  **Zabezpieczaj zachowane hasła.**Uważaj gdzie przechowujesz zapisane hasła. Nie przechowuj haseł w plecaku lub portfelu. Nie zapisuj haseł w miejscach, gdzie nie umieściłbyś informacji, które to hasło zabezpiecza. Nie przechowuj haseł w pliku na swoim komputerze. Przestępcy najpierw szukają właśnie tam.

o    **Nigdy nie wysyłaj swojego hasła przez pocztę elektroniczną.**Jakakolwiek wiadomość e-mail, która prosi o podanie hasła lub prosi o wejście na stronę internetową w celu zweryfikowania hasła, może stanowić oszustwo typu phishing. Dotyczy to również próśb od zaufanych witryn, które często odwiedzasz. Oszuści często podszywają się pod nie i tworzą fałszywe wiadomości e-mail z logo i treścią z prawdziwych stron.

o    **Nie wpisuj haseł na komputerach, nad którymi nie masz kontroli.**Korzystaj z ogólnie dostępnych komputerów w szkole, czytelni, kafejkach Internetowych czy pracowniach komputerowych tylko do anonimowego przeglądania Internetu. Nie korzystaj z tych komputerów w przypadku kont, które wymagają nazwy użytkownika i hasła. Przestępcy mogą nabyć za niewielkie pieniądze keyloggery, urządzenia do wykradania haseł, które można bardzo szybko zainstalować. Wykorzystując te urządzenia, złośliwy użytkownik może zdalnie zebrać informacje wpisane do komputera.

         **Pomóż dzieciom korzystać z sieci społecznościowych w bezpieczny sposób**

Twoje dzieci korzystają z sieci społecznościowych przeznaczonych dla najmłodszych, na przykład Webkinz czy Club Penguin, lub witryn przeznaczonych dla dorosłych na przykład Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook, itp.

Dzieci korzystają z sieci społecznościowych, aby kontaktować się z osobami, które żyją po drugiej stronie globu, jak i z rówieśnikami, z którymi widzą się codziennie w szkole.

Dzieci powinny zdawać sobie sprawę, że niektóre portale społecznościowe mogą być przeglądane przez jakiekolwiek osoby mające dostęp do Internetu. W rezultacie niektóre zamieszczone informacje mogą je narazić na oszustwa typu phishing, cyebrprzemoc, i ataki internetowych pedofilów. Istnieje kilka sposobów na radzenie dzieciom jak korzystać z sieci społecznościowych w bezpieczny sposób.

o    **Rozmawiaj z dziećmi na temat ich doświadczeń.**Zachęcaj swoje dzieci, aby zwracały się do Ciebie, jeśli coś w Internecie sprawiło, że poczuły się niekomfortowo lub jeśli poczuły się zagrożone. Podejdź do tego spokojnie i zapewnij swoje dzieci, że mogą Ci powiedzieć o takich rzeczach. Zapewnij je, że pomożesz im rozwiązać problem.

o    **Ustal zasady korzystania z Internetu.**Ustal zasady korzystania z Internetu kiedy tylko Twoje dzieci zaczną samodzielnie korzystać z Internetu. Zasady powinny mówić czy dzieci mogą korzystać z portali społecznościowych i w jakim wymiarze.

o    **Upewnij się, że Twoje dzieci przestrzegają limitów wiekowych.**Zaleca się, żeby dzieci rejestrujące się na witrynach społecznościowych miały co najmniej 13 lat. Jeśli dzieci nie osiągnęły zalecanego wieku, nie pozwól im korzystać z tych witryn. Nie możesz polegać na serwisach w kwestii powstrzymywania małoletnich dzieci od zarejestrowania się.

o    **Ucz się.** Oceń witryny, z których Twoje dziecko planuje korzystać i upewnij się, że zarówno Ty jak i Twoje dziecko rozumiecie politykę prywatności i zasady zachowania na niej obowiązujące. Sprawdź czy witryna kontroluje zamieszczane przez użytkowników treści. Przeglądaj co jakiś czas stronę swojego dziecka.

o    **Mów swoim dzieciom, aby nie spotykały się z osobami, z którymi miały kontakt tylko przez Internet.**Dzieci, które spotykają się z obcymi osobami, z którymi miały kontakt tylko przez Internet, są narażone na realne zagrożenia. Powiedzenie Twojemu dziecku, żeby nie rozmawiało z obcymi może być nieskuteczne, ponieważ dziecko może nie uznawać osoby poznanej przez Internet za kogoś obcego.

o    **Zachęcaj dzieci, żeby kontaktowały się z osobami, które już znają.**Możesz zadbać o bezpieczeństwo swoich dzieci przez zachęcanie ich, aby wykorzystywały witryny do kontaktowania się ze znajomymi, nie z osobami, których nigdy na żywo nie widziały.

o    **Upewnij się, że Twoje dzieci nie używają swojego imienia i nazwiska.**Mów swoim dzieciom, żeby używały tylko pierwszego imienia lub pseudonimu, który nie przyciąga uwagi niepożądanych osób. Nie zezwalaj również dzieciom na zamieszczanie imion i nazwisk ich znajomych.

o **Zwracaj uwagę na zawarte w profilu dziecka informacje, które ułatwiają identyfikację.**Wiele stron społecznościowych umożliwia dzieciom dołączenie do publicznych grup, do których należą wszystkie osoby, które uczęszczają do danej szkoły.

Zwróć uwagę czy Twoje dziecko nie ujawnia informacji, które mogą ułatwić ich identyfikację, na przykład szkolna maskotka, miejsce pracy lub nazwa miasta, w którym mieszkają. Udostępnienie zbyt wielu informacji może sprawić, że Twoje dziecko będzie narażone na cyberprzemoc, ataki internetowych pedofilów, oszustwa internetowe lub kradzież tożsamości. Więcej informacji: [Jak rozpoznać oszustwa typu phishing i fałszywe wiadomości e-mail](http://www.microsoft.com/pl-pl/security/online-privacy/phishing-symptoms.aspx).

o    **Rozważ korzystanie ze strony, która nie jest dostępna dla wszystkich.** Niektóre witryny sieci web pozwalają na zabezpieczenie Twojej strony hasłem lub skorzystanie z innych sposobów na ograniczenie dostępu osób odwiedzających tylko do tych, które Twoje dziecko zna. Korzystając z Windows Live Spaces, można na przykład ustawić, które osoby są uprawnione do przeglądania Twojej witryny; mogą to być wszystkie osoby w Internecie lub wybrane przez Ciebie osoby.

o    **Zwracaj uwagę na szczegóły widoczne na zdjęciach.** Wyjaśnij swoim dzieciom, że zdjęcia mogą ujawniać dane osobowe. Zachęcaj dzieci, aby nie zamieszczały swoich zdjęć lub zdjęć znajomych, które zawierają łatwo rozpoznawalne szczegóły jak znaki drogowe, rejestracje samochodowe lub nazwa szkoły nadrukowana na ubraniach.

o    **Ostrzegaj swoje dziecko przez ujawnianiem emocji obcym osobom.**Prawdopodobnie już zachęciliście swoje dzieci, aby nie komunikowały się bezpośrednio z obcymi osobami za pomocą Internetu. Jednak dzieci korzystają z portali społecznościowych, aby pisać pamiętniki i wiersze, które często wyrażają silne emocje. Wyjaśnij dzieciom, że każda osoba z dostępem do Internetu może to przeczytać i że pedofile często szukają wrażliwych emocjonalnie dzieci.

o    **Rozmawiaj ze swoim dzieckiem na temat cyberprzemocy.** Jeśli Twoje dzieci są w wieku pozwalającym im na korzystanie z portali społecznościowych, rozmawiaj z nimi na temat [cyberprzemocy](http://www.microsoft.com/pl-pl/security/family-safety/cyberbullying.aspx). Powiedz im, że jeśli czują, że są ofiarami cyberprzemocy, to powinny od razu porozmawiać o tym z rodzicem, nauczycielem lub inną osobą dorosłą, której ufają. Ważne jest również to, aby zachęcać dzieci do komunikowania się z innymi osobami za pomocą Internetu w ten sam sposób, w jaki zrobiłyby to podczas bezpośredniego kontaktu twarzą w twarz. Poproś dzieci, aby traktowały inne osoby w taki sam sposób, w jaki same chciałyby być traktowane.

o    **Usunięcie strony dziecka.**Jeśli Twoje dziecko nie chce dostosować się do ustalonych zasad mających na celu zwiększenie jego bezpieczeństwa w sieci jeśli nie powiodły się Twoje próby zmiany ich zachowania, możesz skontaktować się z portalem społecznościowym, z którego korzysta dziecko i poprosić go o usunięcie strony dziecka. Dowiedz się więcej na temat narzędzi filtrujących zawartość Internetu (takich jak [Kontrola rodzicielska w Windows Live](http://windows.microsoft.com/pl-pl/windows-vista/Protecting-your-kids-with-Family-Safety)) jako element uzupełniający, a nie zastępujący nadzór rodzicielski.

Czy chcesz dowiedzieć się więcej na temat sposobów zapewnienia bezpieczeństwa dziecka w Internecie? Więcej dowiesz się z publikacji [Bezpieczeństwo dzieci w Internecie: 4 rzeczy, które może zrobić rodzic](http://www.microsoft.com/pl-pl/security/family-safety/childsafety-steps.aspx).

         **Jeśli Twoje dziecko prowadzi bloga, upewnij się, że nie ujawnia za dużo informacji**

Pisanie bloga lub pamiętników internetowych stało się niezwykle popularne zwłaszcza wśród nastoletniej młodzieży, która prowadzi blogi bez wiedzy swoich rodziców lub opiekunów. Nastolatki wybierają portale społecznościowe zamiast blogów jako formę spędzania wolnego czasu w sieci, chociaż wiele osób nadal prowadzi blogi na portalach społecznościowych. Badania wykazują, że połowę działających dziś blogów prowadzą nastolatki. Dwie trzecie z nich ujawnia swój wiek, trzy piąte ujawniają swoją lokalizację i dane kontaktowe, a jedna piąta swoje pełne imię i nazwisko. Ujawnianie tego rodzaju informacji może się wiązać z pewnym ryzykiem. Choć prowadzenie bloga może przynosić korzyści, takie jak rozwijanie zdolności komunikacyjnych i umiejętności pisania, ważne jest, aby dzieci nauczyły się czegoś na temat Internetu i blogów, zanim zaczną je prowadzić. Można to porównać do ukończenia kursu jazdy przed samodzielną jazdą samochodem. Poniżej przedstawiamy kilka sugestii na początek:

o    **Ustal z dziećmi zasady korzystania z Internetu**i konsekwentnie je egzekwuj.

o    **Sprawdzaj, co Twoje dzieci chcą zamieścić, zanim to zrobią.**Pozornie nieszkodliwe rzeczy, takie jak zdjęcie maskotki szkolnej, albo miasta, mogą zdradzić, do jakiej szkoły uczęszcza jego autor.

o    **Zadaj sobie pytanie (i niech Twoje dzieci zrobią to samo), czy nie masz nic przeciwko pokazywaniu danej treści nieznajomym.**Jeśli masz wątpliwości, usuń tę treść.

o    **oSprawdź serwis, na którym umieszczony będzie blog,** aby upewnić się, czy umożliwia prowadzenie prywatnego, chronionego hasłem bloga.

o    **Zapisz adres strony z blogiem swojego dziecka**i systematycznie go odwiedzaj.

o    **Obejrzyj inne blogi i znajdź pozytywne przykłady,** które mogłoby naśladować Twoje dziecko.

$1         **Uważaj na internetowe oszustwa**

Według Federalnej Komisji Handlu 31 procent ofiar kradzieży tożsamości to młode osoby. Nastolatki stanowią łatwy cel, ponieważ nie mają problemów finansowych i wiedzą mniej niż dorośli na temat ochrony danych osobowych.

Oto kilka kwestii, o których powinny wiedzieć dzieci, aby zachować bezpieczeństwo i nie stać się ofiarą oszustw internetowych.

o    **Nigdy nie ujawniał osobistych informacji.**Nie ujawniaj danych osobowych, takich jak imię i nazwisko lub miasto rodzinne, jak korzystasz z komunikatora internetowego lub pokojów rozmów dopóki nie masz pewności co do tożsamości rozmówcy.

o  **Wyloguj się z konta,**jeśli korzystasz z publicznych komputerów. Jeśli korzystasz z komputerów w czytelni lub kafejce internetowej, pamiętaj, żeby wylogować się z konta. Nie wiesz, jakie oprogramowanie zainstalowano na komputerach, co ono robi i czy nie zainstalowano na nich sprzętu służącego do wykradania haseł.

o    **Używaj silnych haseł i nikomu ich nie ujawniaj.** Więcej informacji w punkcie 1 powyżej.

o    **Odwiedzaj tylko bezpieczne witryny.**Jeśli Twoje dziecko robi zakupy w Internecie, ważne jest aby upewniło się, że adres URL witryny, na której podają informacje finansowe zaczynał się od https:// i miał ikonkę z żółtą kłódką w prawym dolnym rogu lub, żeby pasek adresu był zielony. Mogą kliknąć ikonkę lub pasek adresu, żeby sprawdzić certyfikat bezpieczeństwa dla konkretnej witryny.

o    **Rozpoznawaj i powiadamiaj o oszustwach.**Powiedz swoim dzieciom o sygnałach, które mogą świadczyć o ryzyku kradzieży tożsamości: oferty karty kredytowej dostępnej od ręki, telefony od agencji windykacyjnych lub nieznane sprawozdania finansowe. Jeśli Twoje dziecko podejrzewa, że doszło do kradzieży tożsamości, od razu podejmij działania, żeby ograniczyć szkody. Skontaktuj się z firmą obsługującą ich kartę kredytową, bankiem, biurami informacji kredytowej i policją. Zamknij wszystkie fałszywe konta i powiedz, żeby zmieniły hasła do wszystkich pozostałych kont internetowych. Zapisz wszystkie swoje działania.