

## Serwisy społecznościowe – przewodnik dla rodziców

Coraz więcej dzieci spędza znaczną ilość czasu w Internecie, korzystając z witryn takich, jak Facebook czy MySpace. Są to jedne z popularniejszych portali stanowiących świetny sposób na utrzymywanie kontaktów z przyjaciółmi. Dzieci jednak często ujawniają zbyt dużo informacji, narażając się na ryzyko.

Niniejszy przewodnik zawiera porady, w jaki sposób radzić sobie z wyzwaniem stawianymi przez witryny społecznościowe. Pozwoli to zachować pewność, że korzystając z Internetu dzieci pozostają bezpieczne.

### **Pięć lekcji dla rodziców, których dzieci korzystają z portali społecznościowych.**

#### **Lekcja 1**

##### **Czym są portale społecznościowe?**

Portale społecznościowe, to witryny tworzące wirtualną społeczność ludzi interesujących się określonym zagadnieniem lub chcących po prostu „przebywać” ze sobą. Dzieci i młodzież uwielbiają portale społecznościowe, gdyż platformy te umożliwiają im rozmowy z przyjaciółmi i rodziną, wysyłanie wiadomości e-mail, udostępnianie zdjęć itp.

- Porozmawiaj z dziećmi o tym, co robią, gdy korzystają z Internetu
- Załóż własny profil Facebook lub stronę MySpace - poproś dzieci o pomoc
- Bądź na bieżąco z korzyściami i wyzwaniami związanymi z portalami społecznościowymi - np. dzięki McAfee® Security Advice Centre

#### **Lekcja 2**

##### **Ryzyko związane z portalami społecznościowymi**

Największym problemem wynikającym z korzystania z portali społecznościowych jest ryzyko ujawnienia zbyt dużej ilości informacji. Twoje dzieci powinny zrozumieć, że udostępnianie zbyt dużej ilości informacji o sobie i swoim życiu osobistym może oznaczać narażenie się na ataki.

- Ustal ograniczenia i zasady zachowania podczas korzystania z Internetu
- Ogranicz ilość czasu, który Twoje dzieci spędzają przy komputerze, korzystając z Internetu
- Porozmawiaj o tym, czym można, a czym nie należy dzielić się podczas korzystania z Internetu
- Doradź dzieciom, aby były ostrożne w stosunku do nieznanym im osób, które chcą dołączyć do kręgu ich znajomych
- Powiedz dzieciom, aby nie spotykały się osobiście z ludźmi poznanymi za pośrednictwem Internetu
- Nalegaj, aby dzieci informowały Cię, gdy zauważą coś nietypowego, poczują się niekomfortowo lub się wystraszą
- Naucz swoje dzieci ostrożności podczas odpowiadania na wiadomości e-mail zawierające pytania, oferty lub odnośniki do witryn internetowych

#### **FAKTY DOTYCZĄCE PORTALI SPOŁECZNOŚCIOWYCH**

67% młodzieży w Europie większość czasu w internecie spędza na serwisach portali społecznościowych. <sup>1</sup>

Najczęstszym zagrożeniem dla europejskiej młodzieży jest ujawnianie osobistych informacji. <sup>2</sup>



### Lekcja 3

#### Zastraszanie przez Internet

Cyberbullying, to wykorzystanie Internetu, lub innych technologii, do wysyłania lub publikowania tekstów lub obrazów mających na celu zawstydzenie lub zranienie innej osoby.

**Nauč się szybko rozpoznawać objawy i porozmawiaj o nich z dziećmi.**

#### Znaki ostrzegawcze mogące świadczyć o tym, że dziecko padło ofiarą zastraszania:

- Brak komfortu podczas odbierania wiadomości e-mail, wiadomości w komunikatorze lub wiadomości tekstowej na telefonie
- Pogorszenie samopoczucia po skorzystaniu z komputera
- Niechęć do wychodzenia z domu lub uczęszczania do szkoły
- Odsunięcie się od przyjaciół i rodziny

#### Znaki ostrzegawcze mogące świadczyć o tym, że dziecko zastrasza kogoś innego:

- Przełączanie pomiędzy oknami lub zamykanie programów, gdy tylko przechodzisz obok komputera
- Korzystanie z komputera późno w nocy
- Wybuchy gniewu w przypadku braku możliwości skorzystania z komputera
- Korzystanie z wielu kont internetowych lub korzystanie z konta należącego do kogoś innego

**Jeśli zauważysz którykolwiek z powyższych objawów, porozmawiaj z dziećmi o kwestii zastraszania przez Internet. Rozważ problem zarówno ze strony ofiary, jak i sprawcy.**

### Lekcja 4

#### Przestępcy internetowi

Internet jest doskonałym miejscem dla przestępców, gdyż pozwala łatwo ukryć tożsamość i uzyskać dostęp do potencjalnych ofiar. Dlatego też bardzo ważne jest, aby omówić z dziećmi odpowiednie zachowanie podczas korzystania z Internetu oraz to, jakie informacje wolno, a jakich nie wolno ujawniać w Internecie.

- Poproś dzieci, aby informowały Cię, gdy natrafią na coś nietypowego podczas korzystania z Internetu
- Zachęcaj dzieci, aby poprosiły o pomoc Ciebie, lub inną zaufaną osobę, gdy padną ofiarą zastraszania lub natrafią na przestępców internetowych
- Upewnij się, że młodzież wie, jak zgłosić nadużycie lub nieodpowiednie zachowanie na witrynach portali społecznościowych

<sup>1</sup> Europejskie badanie bezpieczeństwa w Internecie. Cross Tab Media

<sup>2</sup> Dzieci w krajach Unii, a Internet – Porównanie możliwości i zagrożeń płynących z Internetu w Europie, czerwiec 2008



## Lekcja 5

### Naruszenie prywatności, podszywanie się i kradzież tożsamości

Bardzo ważne jest, aby dzieci uważały na to, jakie informacje udostępniają i z kim się nimi dzielą, oraz by rozumiały, że po zamieszczeniu w Internecie wszystko traci charakter prywatny. Portale społecznościowe mogą być dla hakerów ogromnym źródłem prywatnych informacji. Oszuści często wykorzystują nieprawdziwe, lecz sprawiające wrażenie pochodzących z autoryzowanego źródła prośby, by uzyskać hasła, numery telefonu lub numery kart płatniczych.

- Ucz dzieci kierować się zdrowym rozsądkiem
- Rozmawiaj z dziećmi i stawiaj im granice
- Sprawdź, czy ktoś nie wykorzystuje tożsamości Twojego dziecka
- Stwórz własny profil i korzystaj z serwisów społecznościowych razem z dziećmi
- Wykorzystaj ustawienia zabezpieczeń na serwisach społecznościowych takie jak prywatne profile, blokowanie komentarzy lub ich akceptowanie
- Upewnij się, że posiadasz aktualne oprogramowanie zabezpieczające
- Rozważ korzystanie z oprogramowania pozwalającego monitorować aktywność dziecka w Internecie, co umożliwi jego ochronę

### Ważne informacje

#### Co robić, gdy dziecko padnie ofiarą działań w Internecie:

- Zignoruj sprawcę lub nie loguj się na witrynie, na której doszło do incydentu
- Zablokuj nazwę użytkownika i adres e-mail sprawcy
- Zmień udostępnione dane dziecka lub, jeśli to konieczne, usuń profil.
- Skontaktuj się z witryną, na której doszło do incydentu i, jeśli to konieczne, zażądaj, by usunięto z niej dane dziecka
- Zgłoś zajście swojemu dostawcy usług internetowych oraz dostawcy usług internetowych sprawcy
- Zgłoś zajście na policji
- Zachowaj wszystkie wiadomości od sprawcy
- Zapisz nazwę użytkownika, adres e-mail oraz, jeśli to możliwe, nazwę dostawcy usług internetowych sprawcy



McAfee® Family Protection pozwoli Ci chronić dzieci przed nieodpowiednimi treściami, zagrożeniami ze strony portali społecznościowych i innymi zagrożeniami internetowymi, a ponadto dostarczy Ci informacji o aktywności dziecka w Internecie.



McAfee Polska sp. z o.o.  
ul. Bitwy Warszawskiej  
1920r. 7B  
02-366 Warszawa  
<http://www.mcafee.com/pl>  
<http://service.mcafee.com>



Więcej informacji można znaleźć w publikacji „Portale społecznościowe – przewodnik dla rodziców”.

**Pobierz poradnik:**  
[www.mcafee.com/advice](http://www.mcafee.com/advice)

McAfee oraz inne nazwy produktów firmy McAfee wymienione w niniejszym dokumencie są zarejestrowanymi znakami towarowymi lub znakami towarowymi należącymi do firmy McAfee, Inc. lub firm od niej zależnych w USA i/lub innych państwach. Czerwień McAfee w połączeniu z bezpieczeństwem jest cechą wyróżniającą produktów marki McAfee. Wszystkie inne produkty niezwiązane z McAfee, zastrzeżone lub nie zastrzeżone, zostały w niniejszym dokumencie jedynie wzmiankowane i są własnością innych podmiotów. © 2009 McAfee, Inc. Wszystkie prawa zastrzeżone.