**Bezpieczeństwo w sieci**

Surfowanie w Internecie może być świetną zabawą oraz towarzyską i inspirującą formą spędzania czasu. Zależy nam na tym, abyście naprawdę cieszyli się czasem, który spędzacie na naszych stronach i korzystając z naszych usług. Z tego powodu, przygotowaliśmy zestaw dziesięciu wskazówek dotyczących bezpieczeństwa w sieci.

To ważne, by mieć na uwadze poniższe punkty, gdy czatujecie, używacie komunikatora internetowego, czy też udzielacie się na forach dyskusyjnych:

**1.** Bądźcie dyskretni. Informacje, które publikujecie, stają się publiczne i widoczne dla wszystkich. Nie wstawiajcie informacji lub obrazków, których nie chcecie udostępniać całemu światu. Uważajcie – mogą zostać przekazane dalej!

**2.** Bądźcie anonimowi. Nie dzielcie się prywatnymi lub bardzo osobistymi informacjami. Nigdy nie zamieszczajcie lub wysyłajcie czegokolwiek, co może posłużyć do zlokalizowania was lub innej osoby (na przykład imienia i nazwiska, adresu e-mail, czy też adresu domowego lub numeru telefonu).

**3.** Zachowajcie dystans. Nie organizujcie spotkań z przypadkowymi osobami poznanymi w sieci. Jeśli już musicie, spotykajcie się wyłącznie w bezpiecznych i publicznych miejscach, powiadomcie kogoś o swoich planach i przyprowadźcie ze sobą znajomego. Jeśli nie jesteście pełnoletni, poproście rodziców lub opiekunów o pozwolenie i weźcie ich ze sobą.

**4.** Bądźcie szczerzy. Możliwe, że kusi was udawanie kogoś, kim nie jesteście. Pamiętajcie, że inni ludzie również mogą myśleć w ten sam sposób. Potrafią podawać się za kogoś, kim w rzeczywistości nie są.

**5.** Bądźcie uprzejmi. Nie wdawajcie się w zbędne dyskusje z natrętnymi osobami. Jeśli ktoś was obraża, po prostu odejdźcie od komputera. Powiadomcie dorosłego lub administratora o danej osobie i jej zachowaniu. To ma być przede wszystkim zabawa, czyż nie?

**6.** Uważajcie na wirusy. Nie otwierajcie, nie odpowiadajcie i nie przesyłajcie dalej e-maili, czy też wiadomości z komunikatora, jeśli nie znacie osoby wysyłającej i nie sprawdziliście zawartości programem antywirusowym. Może ona zawierać niebezpieczne oprogramowanie (takie jak spyware, czy wirusy), lub być obraźliwa.

**7.** Zachowajcie bezpieczeństwo. Używajcie oprogramowania zabezpieczającego (np. skanerów antywirusowych). Upewnijcie się, że system operacyjny jest zaktualizowany i zabezpieczony na wypadek, gdyby e-mail nieumyślnie zainfekował wasz komputer.

**8.** Zachowajcie prywatność. Nigdy nie udostępniajcie haseł lub podpowiedzi do nich.

**9.** Bądźcie kreatywni. Upewnijcie się, że wasza tożsamość internetowa nie ujawnia żadnych osobistych informacji. Bądźcie kreatywni i wyjątkowi!

**10**. Uważajcie. Jeśli coś brzmi zbyt dobrze, żeby było prawdą, prawdopodobnie nią nie jest! Sprawdzajcie fakty, jeśli czegoś nie jesteście pewni.

**I pamiętajcie, że wszystko zależy od was. Sami decydujecie, w jakie działalności się zaangażować i jakie informacje udostępnić.**

Gry komputerowe.

Znaki ratingu PEGI znajdują się z przodu i z tyłu opakowania. Wskazują one następujące kategorie wiekowe: 3, 7, 12, 16 i 18. Dostarczają wiarygodnych informacji o stosowności treści gry z punktu widzenia ochrony nieletnich. Rating wiekowy nie uwzględnia poziomu trudności ani umiejętności niezbędnych do danej gry.

Początek formularza

Dół formularza

PEGI 3
Treść gier oznaczonych w ten sposób uznaje się za odpowiednią dla wszystkich grup wiekowych. Dopuszczalna jest pewna ilość przemocy w komicznym kontekście (zwykle podobna do prezentowanej w kreskówkach w rodzaju Królika Bugsa czy Toma i Jerry’ego). Dziecko nie powinno utożsamiać postaci pojawiających się na ekranie z postaciami rzeczywistymi. Powinny one być w całości wytworem fantazji. Gra nie powinna zawierać dźwięków ani obrazów, które mogą przestraszyć dziecko. Nie powinny w niej występować wulgaryzmy.



PEGI 7
Gry, które w innym przypadku zostałyby zakwalifikowane do grupy 3, lecz zawierają dźwięki lub sceny potencjalnie przerażające najmłodszych odbiorców, mogą być uznane za odpowiednie dla tej grupy wiekowej.



PEGI 12
Gry wideo pokazujące przemoc o nieco bardziej realistycznym charakterze, skierowaną przeciw postaciom fantastycznym i/lub nierealistyczną przemoc wobec postaci o ludzkim lub rozpoznawalnych zwierząt, ponadto w tej kategorii wiekowej dopuszczalna jest nieco bardziej dosłowna nagość. Ewentualne wulgaryzmy muszą mieć łagodny charakter i nie mogą zawierać odwołań do seksu.



PEGI 16
Ten symbol jest nadawany, jeżeli przemoc lub aktywność seksualna wyglądają tak jak w rzeczywistości. Młodzież w tym wieku powinna również być odporna na brutalniejsze wulgaryzmy, sceny pokazujące używanie tytoniu lub narkotyków oraz sceny popełniania przestępstw.



PEGI 18
Za gry dla dorosłych uznaje się gry przedstawiające daleko posuniętą przemoc i/lub specyficzne rodzaje przemocy. Daleko posunięta przemoc jest najtrudniejsza do zdefiniowania, ponieważ w wielu przypadkach jest to pojęcie bardzo subiektywne, ale ogólnie można ją określić jako sceny przemocy powodujące u widza uczucie odrazy.

Opisy zamieszczone z tyłu opakowania podają najważniejsze przyczyny przeznaczenia gry dla danej grupy wiekowej. Jest osiem takich opisów: przemoc, wulgaryzmy, lęk, narkotyki, seks, dyskryminacja, hazard i gra w Internecie z innymi ludźmi.



Wulgarny język
W grze jest używany wulgarny język.



Dyskryminacja
Gra pokazuje przypadki dyskryminacji lub zawiera materiały, które mogą do niej zachęcać.



Narkotyki
W grze pojawiają się nawiązania do narkotyków lub jest pokazane zażywanie narkotyków.



Strach
Gra może przestraszyć młodsze dzieci.



Hazard
Gry, które zachęcają do uprawiania hazardu lub go uczą.



Seks
W grze pojawiają się nagość i/lub zachowania seksualne lub nawiązania do zachowań o charakterze seksualnym.



Przemoc
Gra zawiera elementy przemocy.



Online
gra może grać online

## Wiedza w pigułce – o czym muszą wiedzieć dzieci.

Każdego dnia porozumiewamy się z ludźmi. Kiedy robisz zakupy, nie przeszkadza Ci, że ktoś jest świadkiem wymiany zdań ze sprzedawcą. Nie chcesz jednak, aby Twoją poufną rozmowę z przyjaciółką słyszała osoba postronna.

Komunikacja publiczna i komunikacja prywatna znacznie się od siebie różnią. W komunikacji publicznej uczestniczy duża liczba osób, w komunikacji prywatnej — niewielka i ściśle określona grupa. Komunikujemy się publicznie, kiedy bierzemy udział w dyskusji podczas wieczoru autorskiego czy spotkania z politykiem, gdy zamieszczamy posty na forum internetowym, publikujemy artykuł w gazecie, udostępniamy filmy lub zdjęcia na blogu. W przypadku wymiany listów i e-maili, rozmowy z rodziną i przyjaciółmi (np. na przyjęciu urodzinowym), SMS-owania bądź porozumiewania się przez komunikator internetowy lub telefon możemy natomiast mówić o komunikacji prywatnej.

Poza nadawcą i odbiorcą do wiadomości prywatnej w serwisie społecznościowym oraz na forum ma wgląd administrator. Korzystanie z tej formy komunikacji przypomina zatem podawanie przez koleżankę z ławki liściku — niezłożonego i bez koperty — do kolegi siedzącego pod oknem. Koleżanka, jeśli zechce, jest w stanie zapoznać się z treścią.

W przypadku szkolnego forum wiadomość prywatną może przeczytać nauczyciel.

Jeśli zamieścisz jakieś dane (zdjęcia, pliki tekstowe) na dysku swojego komputera, to dostęp do nich będą miały właściwie tylko osoby korzystające z tego sprzętu. Jeśli udostępniasz określoną informację w Internecie — tracisz nad nią kontrolę. Sieć nie zapomina, zamieszczone materiały pozostają tam na zawsze. Dotyczy to nie tylko serwisów społecznościowych, ale praktycznie każdej aktywności w Internecie.

W sieci — podobnie jak w rzeczywistości poza nią — należy przestrzegać zasad bezpieczeństwa.

Oto 8 wskazówek, które uczestnicy i uczestniczki powinni poznać:

1. Jeśli nie masz pewności, z kim rozmawiasz, nie podawaj żadnych informacji na swój temat.
2. Nie zdradzaj innym swoich haseł. Układaj takie, które będą trudne do odgadnięcia (to nie może być Twoja data urodzenia ani imię!). Zamiast liter możesz wykorzystać cyfry, które są do nich podobne (I = 1, O = 0, A = 4 itp.). Hasło powinno zawierać nie mniej niż 8 znaków, w tym cyfry oraz wielkie litery. W różnych serwisach posługuj się różnymi hasłami.
3. Nie pozwalaj na zapamiętywanie przez przeglądarkę haseł do poczty elektronicznej i serwisów, z których korzystasz — w przeciwnym razie każda osoba pracująca na tym komputerze będzie mogła zalogować się na Twoje konto. Po skończonej pracy wyloguj się — inaczej ktoś może się pod Ciebie podszyć.
4. Jeśli korzystasz z serwisów społecznościowych, zadbaj o odpowiednie ustawienia prywatności. Im mniej informacji udostępniasz osobom postronnym, tym lepiej. Zastanów się, czy na pewno warto z tych serwisów korzystać. Pamiętaj, że zgodnie z regulaminem Facebooka możesz założyć tam konto dopiero po ukończeniu 13. roku życia.
5. Na forach dyskusyjnych czy blogach posługuj się nickiem (pseudonimem), a nie swoim imieniem i nazwiskiem. Unikaj publikowania informacji o sobie w sieci.
6. Nie korzystaj z możliwości automatycznego „oznaczania się” w miejscu pobytu. Geolokalizacja ma swoje zalety (np. można pochwalić się zwiedzaniem ciekawego miasta), ale i wady — jeżeli ktoś planuje złożenie bliskiej osobie niezapowiedzianej wizyty, przez przypadek może zepsuć efekt niespodzianki. Ponadto ujawnianie swojego miejsca pobytu umożliwia śledzenie, a niekiedy może być nawet niebezpieczne.
7. Zwracaj uwagę na komunikaty pojawiające się w trakcie ściągania gier i aplikacji na telefony komórkowe i smartfony. Możesz się z nich dowiedzieć, do jakich Twoich danych żąda dostępu pobierana usługa. Uważaj, na co wyrażasz zgodę.
8. W razie wątpliwości odnośnie do tego, jak w danej sytuacji postąpić, poproś o radę swoich rodziców lub innych dorosłych, którym ufasz.