

## Jak zachować bezpieczeństwo w sieci?

### Drodzy Rodzice, drodzy Uczniowie

W trosce o Wasze bezpieczeństwo chcę zwrócić Wam uwagę na pojawianie się coraz większej liczby niepokojących informacji na temat zagrożeń związanych z korzystaniem z zasobów internetowych, w tym: mediów społecznościowych, gier, itp.

Poniżej podaje kilka, godnych uwagi, informacji, jak ustrzec się przed cyberprzemocą.

Udostępniając różne informacje w Internecie — tracisz nad nimi 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 — 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 załogować się na Twoje konto. Po skończonej pracy wyloguj się — inaczej ktoś może się pod Ciebie podszyc.
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.
8. Uważaj, na co wyrażasz zgodę. W razie wątpliwości odnośnie do tego, jak w danej sytuacji postąpić, poproś o radę swoich rodziców lub innych dorosłych, którym ufasz.

W celu uzyskania porad lub informacji można zadzwonić pod bezpłatny numer: 800 100 100

Aby otrzymać więcej informacji zachęcam do odwiedzenia stron:

[www.dyzurnet.pl](http://www.dyzurnet.pl)

[www.akademia.nask.pl](http://www.akademia.nask.pl)

[www.sieciaki.pl](http://www.sieciaki.pl)

[www.kursor.edukator.pl](http://www.kursor.edukator.pl)

[www.saferinternet.pl](http://www.saferinternet.pl)

[www.plikifolder.pl](http://www.plikifolder.pl)

[www.bezpiecznaszkola.men.gov.pl](http://www.bezpiecznaszkola.men.gov.pl)

pedagog szkolny – Agnieszka Czerniawska