# Bezpieczne korzystanie z internetu

* Przestrzegaj netykiety – pisz kulturalnie, na temat, poprawnie, bez błędów; używaj polskich znaków; NIE KRZYCZ (czyli nie pisz wielkimi literami).
* Nie rozsyłaj spamu, niechcianych odnośników do stron ani „łańcuszków szczęścia” – prawdziwość informacji możesz sprawdzić w internecie, np. w serwisie www.atrapa.net.
* Używaj programów antywirusowych i zapór ogniowych (*firewall*).
* Stosuj zabezpieczenie swojej sieci WiFi (najlepiej używając protokół WPA-2 i ustawiając niestandardowe hasło do zmian konfiguracji sieci).
* Dbaj o bezpieczeństwo swoich haseł. Ważne usługi (dostęp do banku, portalu aukcyjnego) zabezpieczaj hasłami o wysokiej złożoności, tzn. co najmniej 8 znaków, w tym duże i małe litery, cyfry, znaki niealfanumeryczne. Jako haseł nie używaj imion, dat urodzenia i popularnych ciągów tekstowych typu *qwerty*. Staraj się, by hasła w ogóle nie tworzyły zrozumiałych słów. Jeżeli masz problem z zapamiętaniem skomplikowanych wyrażeń, możesz zastosować metodę zamieniania wybranych liter hasła na znaki specjalne i cyfry, np. łatwe do zapamiętania słowo *licealista* przekształcić do *l!c3alisTa*. Innym sposobem tworzenia hasła łatwego do zapamiętania może być użycie pierwszych liter wyrazów przysłowia czy tytułu piosenki, np. z przysłowia „Jak Kuba Bogu, tak Bóg Kubie!” można utworzyć hasło jKBtBK!
* W przypadku ujawnienia lub jedynie podejrzenia ujawnienia hasła należy je niezwłocznie zmienić.

*Powyższe zasady powinny dotyczyć także haseł do poczty elektronicznej i portali społecznościowych. Kradzież tożsamości może być bowiem równie dotkliwa jak utrata pieniędzy.*

* Jeżeli kupujesz towary i usługi w internecie, zawsze dokładnie zapoznaj się z ich opisem. Przeczytaj regulamin sklepu lub aukcji, sprawdź koszty przesyłki, możliwości zwrotu lub reklamacji produktu. Poszukaj też opinii internautów o sprzedawcy.
* Konto bankowe (lub kartę kredytową), które wykorzystujesz do płatności online zasilaj niewielkimi kwotami (niezbędnymi do zrealizowania pojedynczej transakcji).
* Nie ujawniaj nikomu haseł, loginów, kodów PIN i CVV2, numerów kart, zwłaszcza gdy byłbyś proszony o te informacje drogą e-mailową.
* W czasie nawiązywania internetowych znajomości zachowuj ostrożność. Nie zawsze rozmówca z chatu czy komunikatora musi mieć wobec ciebie dobre zamiary. Nie obdarzaj go bezgranicznym zaufaniem. Postaraj się zweryfikować swoją wiedzę na jego temat u innych źródeł. Na spotkania umawiaj się w miejscach publicznych, w towarzystwie innych osób.

Szczególnym problemem związanym z rozwojem nowoczesnej technologii jest cyberprzemoc. To wszelkiego rodzaju wyśmiewanie innych, kompromitowanie i poniżanie ich, znieważanie, nękanie, zastraszanie i tym podobne czynności dokonywane z wykorzystaniem usług internetowych (np. poczta elektroniczna, fora dyskusyjne, portale społecznościowe) oraz telekomunikacyjnych (np. SMS, MMS). Osoby dokonujące cyberprzemocy muszą sobie zdawać sprawę z konsekwencji swoich czynów. Groźby, pomówienia, znieważanie, a od niedawna również nękanie (*stalking*) są czynami karalnymi według polskiego prawodawstwa. Naprawienie wyrządzonej szkody poprzez usunięcie krzywdzących treści jest przeważnie bardzo trudne do zrealizowania – w globalnej sieci będą one już powielone w setkach egzemplarzy i przechowywane na dziesiątkach serwerów na całym świecie.

Jeżeli czujesz, że problem cyberprzemocy dotyczy również ciebie – zwróć się o pomoc do organizacji helpline.org.pl, pedagoga szkolnego lub wychowawcy.