Bądź bezpieczny w sieci

Grupa I

1) Zwracanie uwagi na protokół SSL podczas korzystania z e-mailów
2) Posiadanie cały czas aktualnego antywirusa
3) Posiadanie włączonego firewalla
4) Posiadanie aktualnej przeglądarki
5) Nie otwieraj podejrzanych lików z e-mailów
6) Posiadanie wtyczki poprzez którą społeczność ocenia bezpieczeństwo strony.
7) Posiadanie wtyczki blokującej wyskakujące okna i reklamy np. noscript
8) Zwracanie uwagi na pliki cookie
9) Zaznaczenie opcji o nieśledzeniu użytkownika przez witryny
10) Nieuruchamianie ważnych stron np. kont bankowych ze smartphone'a lub tabletu itp
11) Zainstalowanie na urządzeniach mobilnych, programów chroniących

Grupa II

1) Nie udostępniaj swoich prywatnych danych nieznanym osobom.
2) Nigdy nie podawaj komuś swojego hasła (do poczty czy choćby dziennika elektronicznego).
3) Używaj programów antywirusowych, antyspamowych oraz rozszerzeń blokujących reklamy.
4) Pamiętaj, że surfując po Internecie nie jesteś anonimowy.
5) Surfując po internecie, udostępniasz też administratorom hostując serwery wiele informacji o używanej przeglądarce. Informacji tych może być tak wiele, że dzięki nim można będzie zidentyfikować Cię w sieci.
6) Nie korzystaj z portalów społecznościowych jeśli nie jesteś do tego zmuszony. Przynoszą one więcej szkód niż pożytku.
7) Staraj się chronić swoje dane osobowe (korzystać ze sprawdzonych witryn).
8) Dokonuj rozsądnie zakupów przez Internet (nie daj się nabrać na niesamowite promocje).
9) Nie wchodź w nieznane Ci linki.
10) Korzystaj z komputerów szkolnych tak jak nakazuje nauczyciel / regulamin pracowni. Nie używaj go do „spraw prywatnych”.
11) Uważaj przy kontaktach z nieznajomymi, nigdy nie mamy pewności kto siedzi po tej „drugiej stronie”.
12) Dane na dyskach szkolnych powinny być szyfrowane, ponieważ mogą one przechowywać dane osobowe uczniów i nauczycieli. Mogą poważnie zaszkodzić osobom korzystającym ze sprzętów szkolnych.