BEZPIECZEŃSTWO W SIECI

1.Korzystaj z oprogramowania antywirusowego.

2. Unikaj otwierania wiadomości od nieznajomych osób

3.Uważaj na pliki, które pobierasz w sieci.

4. Pliki należy pobierać tylko z zaufanych witryn.

5. Należy zachować ostrożność w stosunku do pewnych typów plików. Niektóre typy plików są mniej bezpieczne, ponieważ mogą być nośnikami wirusów.

6. Unikaj wchodzenia w nieznane linki. Niektóre maile są fałszwe. Hackerzy stosują dwie metody oszustw internetowych przeprowadzanych za pomocą e-maili – „spoofing" i „phishing". Obie polegają na podszywaniu się pod zaufanego nadawcę, a ich celem jest przechwycenie Twoich osobistych danych lub nakłonienie do wykonania czynności, których nie zamierzałeś. Sfałszowane maile wyglądają jakby pochodziły od znanych instytucji lub Twoich znajomych. Wśród nich możesz natrafić na wiadomość od oszusta.

7. Nie podawaj swoich danych osobowych w sieci. Zgoda na przetwarzanie danych osobowych do celów marketingowych oznacza utratę kontroli nad tym, co się z nimi potem dzieje. Mogą być one wykorzystywane do oferowania towarów i usług, ale też np. do kradzieży tożsamości i wyłudzania kredytów. Dlatego podawanie niektórych swoich danych, np. numeru PESEL, jest bardzo niebezpieczne.

8. Chroń swoje konta na serwisach społecznościowych. Rejestrując się na różnego rodzaju portalach społecznościowych decydujemy się na udostępnianie swoich danych osobowych. Akceptując regulamin danego serwisu, wyrażamy zgodę na przetwarzanie tych danych. Warto jednak zwrócić uwagę na politykę prywatności i kwestie bezpieczeństwa (ochrona danych osobowych), aby nasze dane nie zostały wykorzystane w złym celu.

9. Stosuj skomplikowane, trudne do odgadnięcia hasła i nie podawaj ich nikomu.

10. Nie podawaj numerów konta bankowego. Kody PIN często są zapisywane w telefonach komórkowych, w notesach i innych miejscach w których łatwo je znaleźć, dlatego najlepiej ich nikomu nie pokazywać, zapisywać w trudnych do odgadnięcia miejscach i jeżeli jest taka potrzeba to często zmieniać.

11. Czytaj uważnie regulaminy.

12. Sprawdzaj, czy strona, do której się logujesz, ma zabezpieczenie SSL. Certyfikaty SSL są narzędziem zapewniającym ochronę witryn internetowych, a także gwarantem zachowania poufności danych przesyłanych drogą elektroniczną. Pełne bezpieczeństwo jest efektem zastosowania szyfrowania komunikacji pomiędzy komputerami.

13. Pamiętaj, że nieznajome osoby, które kontaktują się z tobą przez komunikator, czat, e-mail, portal społecznościowy czy inną aplikację mogą mieć wobec ciebie złe intencje. W przypadku znajomości z sieci warto zachować szczególną ostrożność. Nigdy nie wiadomo, kto jest po drugiej stronie.

14. Staraj się zachować umiar w korzystaniu z Sieci czy graniu w gry komputerowe.