Cyberbezpieczeństwo

1. Zabezpiecz hasłem dostęp do systemu BIOS komputera,
2. Nie zostawiaj odblokowanego urządzenia bez nadzoru, zablokuj dostęp, aby nikt niepowołany nie mógł z niego korzystać,
3. Regularnie aktualizuj system operacyjny i oprogramowanie na komputerze (np. przeglądarkę internetową),
4. Stosuj unikatowe hasła o odpowiednim poziomie skomplikowania (zawierające duże i małe litery, liczby, znaki specjalne) oraz nie udostępniaj ich nikomu,
5. Korzystaj z bezpiecznych połączeń internetowych lub używaj połączeń VPN gdy łączysz się z nieznaną siecią np. ogólnodostępną siecią Wi-Fi,
6. Używaj zapory sieciowej firewall oraz aktualnego oprogramowania antywirusowego uruchomionego na swoim komputerze,
7. Pracuj na koncie zwykłego użytkownika z ograniczonymi uprawnieniami (załóż konto nie posiadające uprawnień administratora),
8. Zachowaj ostrożność przy uruchamianiu linków i załączników w poczcie elektronicznej,
9. Nie podłączaj do komputera nieznanych urządzeń np. znalezionych dysków USB, mogą być celowo zainfekowane złośliwym oprogramowaniem,
10. Podobne zasady stosuj przy korzystaniu z urządzeń mobilnych,
11. Uważnie czytaj komunikaty i powiadomienia pojawiające się w trakcie logowania. Pamiętaj, że przestępcy potrafią podrabiać strony w Internecie. Jeśli zaskoczyło Cię coś w widoku naszej strony lub miałeś do czynienia z nietypowym jej działaniem, skontaktuj się z nami,
12. Uważaj na phishing, są to próby wyłudzenia od użytkowników ich danych osobowych i uprawnień do logowania się na strony www. Najczęściej ma on formę specjalnie spreparowanych wiadomości przesyłanych pocztą elektroniczną.