

Urząd Gminy w Rogowie

Zagrożenia i sposoby zabezpieczenia się przed zagrożeniami



Kategoria - Aktualności

Data publikacji -4 lipca 2022 godz. 15:28

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),
- kradzieże tożsamości,
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

- zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym,
- aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie),
- aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki,
- nie otwieraj plików nieznanego pochodzenia,
- nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna,
- nie używaj niesprawdzonych programów zabezpieczających czy też publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony),
- co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować
- sprawdzaj pliki pobrane z internetu za pomocą skanera,
- staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, lub łatwy zarobek przy rozsyłaniu spamu)- często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia,
- nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich,
- nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny,
- pamiętaj o uruchomieniu firewalla,
- wykonuj kopie zapasowe ważnych danych,

- pamiętaj, że żaden bank, czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- nie zapisuj hasłem w przeglądarce
- jeżeli to możliwe, korzystaj z dwuetapowej weryfikacji logowania