Zestawienie szczególnych zagrożeń związanych z korzystaniem z usługi świadczonej drogą elektroniczną, na które mogą być narażone osoby korzystające z usług świadczonych drogą elektroniczną:

1. Spam – otrzymywanie niezamówionej informacji reklamowej lub handlowej drogą elektroniczną.
2. Malware – oprogramowanie, które jest w stanie, po uruchomieniu, zarazić pliki w sposób samopowielający, zazwyczaj nie będąc zauważonym przez użytkownika. Mają różne działanie i skutki, zajmują pamięć RAM, CPU i miejsce na twardym dysku.
3. Worm – oprogramowanie zdolne do samopowielania. E-mail wrom jest niszczącym atakiem przeciwko sieci, polegającym na zebraniu wszystkich adresów e-mail znajdujących się w lokalnym programie do obsługi poczty i wysłaniu na nie setek e-maili zawierających robaka w niewidocznym załączniku.
4. Spyware – oprogramowanie szpiegujące działania użytkownika w Internecie, instalujące się bez jego wiedzy, zgody i kontroli.
5. Złośliwe oprogramowanie – niechciane lub „złośliwe" oprogramowanie, wykonujące czynności niezamierzone przez użytkownika, min: trojan, rootkit, keylogger, backdoor, exploit.
6. Cracking/phishing („łowienie haseł") – działania mające na celu złamanie zabezpieczeń (cracking) i pozyskanie osobistych informacji min. w celu kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne.
7. Sniffing – niedozwolony podsłuch, polegający na wykorzystaniu sniffera – programu komputerowego, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci.
8. Kryptoanaliza – wyszukiwanie słabości systemu kryptograficznego w celu umożliwienia jego złamania lub obejścia.
9. Korzystanie z nielegalnych urządzeń – wprowadzanie przez inne osoby do systemu teleinformatycznego i/lub sieci telekomunikacyjnej nielegalnych urządzeń, dających nieuprawniony dostęp do usług podlegających ochronie.

W celu uniknięcia powyższych zagrożeń zaleca się:

1. Zaopatrzyć swoje urządzenie, które łączy się z Internetem w aktualny program antywirusowy.
2. Stosować zaporę sieciową firewall.
3. Zaopatrzyć pocztę elektroniczną w program wykrywający wirusy w wiadomościach e-mail.
4. Sprawdzać importowane dane przed ich otwarciem (uruchomieniem) za pomocą modułu skanowania pliku programu antywirusowego.
5. Wykonywać regularne aktualizacje systemu i oprogramowania.
6. Cykliczne wykonywać kopie zapasowe ważnych danych.
7. Nie otwierać plików nieznanego pochodzenia.
8. Logować się za pomocą unikatowego hasła i loginu i nie używać go do różnych kont i urządzeń.
9. Chronić swój login i hasło i nie podawać go innych osobom.
10. Sprawdzać, czy adres strony logowania poprzedzony jest zapisem „https" i czy certyfikat został prawidłowo wystawiony.
11. Nie pobierać aplikacji z nieznanych źródeł. Aplikację na urządzenia mobilne należy zawsze pobierać z autoryzowanego serwisu.