

Особи, які користуються послугами, що надаються в електронному вигляді, можуть наражатися, зокрема, на такі ризики:

Спам	Отримання небажаної рекламної (комерційної) інформації за допомогою електронних засобів.
Шкідливе програмний засіб	Програмне забезпечення, яке під час запуску здатне заражати файли шляхом самовідтворення, зазвичай це все відбувається непомітно для користувача. Вони мають різні дії та ефекти, займають оперативну пам'ять, місце на процесорі та жорсткому диску.
Черв'яки	Програмне забезпечення, що самовідтворюється. Черв'як електронної пошти - це руйнівна атака на мережу, яка збирає всі адреси електронної пошти в локальній адресі електронної пошти та надсилає їм сотні електронних листів із невидимим вкладенням із хробаком.
Шпигунство	Програмне забезпечення, яке стежить за діями користувача в Інтернеті, встановлюється без його відома, згоди та контролю.
Шкідливе програмне забезпечення	Небажане та "шкідливе" програмне забезпечення, яке виконує дії, не контрольовані напередбачені користувачем, наприклад такі як: троян, wabbit, руткіт, кілоггер, бекдор, експлойт.
Взлом/фішинг („перехоплення паролів“)	Дії, спрямовані на зламання запобіжних методів (злом) і отримання особистої інформації, напр. з метою крадіжки особистих даних шляхом надсилання фальшивих нагадувань електронною поштою для омани.
Сніфер	Незаконне прослуховування, що полягає у використанні сніфера - комп'ютерної програми, завдання якого полягає в перехопленні та аналізі даних, що надходять у мережу.
Криптоаналіз	Пошук слабких місць у криптографічній системі з метою її зламу або обдурення.
Перегляд з нелегальних пристроїв	Введення іншими особами в ІКТ-систему та/або телекомунікаційну мережу незаконних пристроїв, що мають несанкціонований доступ до захищених послуг.

Щоб уникнути зазначених вище ризиків, Клієнт повинен перш за все мати в своєму пристрої, який підключається до Інтернету, оновлену антивірусну програму та фаєрвол. Крім того, Клієнт повинен мати на своїй електронній пошті програму, яка визначає наявність вірусів у електронних повідомленнях та перевіряє імпортовані дані перед їх відкриттям (запуском) за допомогою модуля сканування файлів антивірусної програми.