Заходи безпеки під час використання платіжної картки в Інтернеті:

- Комп'ютерний вірус - комп'ютерна програма (шкідливий код), відмінною рисою якої є здатність збору інформації про дані платіжних карток (номер платіжної картки, CVV2 / CVC2, термін закінчення дії платіжної картки), які зберігаються / вводяться на комп'ютері, ноутбуці, планшеті, смартфоні, телефоні, зараженому вірусом.
- Переконайтеся, що в полі «Адреса» вибраного сайту вказана саме необхідна web-адреса, а не просто схожа на неї. При оплаті або введенні конфіденційної інформації про платіжну картку необхідно звернути увагу, щоб сайт був захищений: в адресному рядку браузера адреса обов'язково повинна починатися з https:// (а не просто http://), а у вікні браузера повинен з'явитися значок «закритий замочок -  ».
- Ніколи не вводьте PIN-код платіжної картки в Інтернеті. Ніколи не вводьте дані платіжної картки в спливаючих (pop-up) вікнах. Зверніть увагу, що для введення CVV2 / CVC2 на захищених сайтах використовується «віртуальна клавіатура», а на шахрайських та незахищених - ні.
- Уникайте проведення оплат за товари, послуги, комунальні платежі з публічного комп'ютера (кафе, бару, ресторану, готелю, бібліотеки, пошти, інших торговельно-сервісних підприємств, що надають послуги доступу до Інтернету), у разі, якщо цього не уникнути, вмикайте в браузері режим «приватного перегляду» (InPrivate Browsing).
- Не зберігайте на платіжній картці суми грошей більше, ніж потрібно для здійснення одноразового платежу в Інтернеті. Поповнюйте рахунок безпосередньо перед проведенням платежу, або блокуйте платіжну картку для онлайн-розрахунків і знімайте це обмеження перед процесом оплати. Ще один варіант - відкрити спеціальну платіжну картку для Інтернет-платежів, яку можна буде в разі необхідності поповнити з основної платіжної картки.
- Обов'язково встановіть на комп'ютері Firewall, ліцензійний антивірус, стежте за його своєчасним оновленням.
- Встановлюйте тільки ліцензійні операційні системи, своєчасно оновлюйте програмне забезпечення.
- Звертайте увагу на папки з випадковими іменами (що складаються з набору символів) в кореневих папках (диску С:), видаляйте їх, а також звертайте увагу на зайві файли при автозавантаженні, якщо Ви їх не обирали, видаляйте їх з вікна завантаження.
- Установіть ліміт на суми / кількість операцій для розрахунків у Інтернеті.