Національний банк України

#ШахрайГудбай

ШУКАЧІ СЕКРЕТІВ ПЛАТІЖНОЇ БЕЗПЕКИ:

Хелловінська місія проти шахраїв

Поради з платіжної безпеки
для проведення гри

Тримайте в секреті три цифри на звороті платіжної картки.
Тримайте в секреті коди (одноразові паролі) банків.
Тримайте в секреті коди (одноразові паролі) мобільних операторів.
Тримайте в секреті ПІН-код до картки.
Підключіть смс-інформування стосовно операцій з платіжною карткою.
Установіть індивідуальні ліміти на операції з вашою платіжною карткою.
Використовуйте віртуальну картку для розрахунків у мережі Інтернет.
Не переходьте за посиланнями від незнайомців!
Отримали посилання від друга – не поспішайте на нього клікати. Шахраї могли отримати доступ до акаунту друга. Спершу зателефонуйте другу та запитайте, чи справді посилання від нього.

Не вводьте реквізити платіжних карток на незнайомих та підозрілих сайтах.
Перевіряйте посилання на сумнівні сайти на сайті Кіберполіції в розділі "Стоп фрауд".
Перевіряйте посилання на сумнівні сайти на сайті Кіберполіції в розділі "Стоп фрауд".
Створюйте складні паролі до електронної пошти, соціальних мереж та інтернет-банкінгу.
Створюйте різні паролі до електронної пошти, соціальних мереж та інтернет-банкінгу.
Не використовуйте під час створення паролів особисту персональну інформацію (дату народження, адресу, номер телефону тощо).
Не використовуйте під час створення паролів загальновідомі комбінації паролів (наприклад, Qwerty12, Password123456, Admin1234 тощо).
Не використовуйте під час створення паролів послідовне/ зворотне написання символів або цифр.
Захистіть свої акаунти – установіть багатофакторну автентифікацію.

Якщо телефонує працівник банку, скажіть, що ви зараз перетелефонуєте самостійно на офіційний номер банку, зазначений на платіжній картці.
Негайно заблокуйте картку, якщо випадково повідомили шахраю реквізити картки та паролі.
Тримайте в секреті логін та пароль до онлайн-кабінету мобільного оператора.
Купуєте в інтернеті – надавайте перевагу післяплаті!
Коли купуєте на торговельному майданчику (наприклад, OLX), обговорюйте деталі угоди виключно в чаті торговельного майданчика або використовуючи його додаток!
Якщо ввели реквізити картки і зрозуміли, що сайт шахрайський, негайно заблокуйте картку!
Захистіть свій фінансовий номер телефону – "прив’яжіть" фінансовий номер телефону до своїх паспортних даних або перейдіть на контракт з мобільним оператором.
Відключіть послугу віддаленої заміни сім-карти у свого мобільного оператора.