РЕКОМЕНДОВАНІ ЗАХОДИ БЕЗПЕКИ
ПРИ ВИКОРИСТАННІ ПЛАТІЖНИХ ІНСТРУМЕНТІВ

1. **Будьте уважні!**

   Шахраї можуть скористатися будь-яким доступним способом взаємодії з Вами: телефон, інтернет, пошта, банкомати.

   Як правило, шахраї застосовують методи соціальної інженерії та намагаються збити Вас з пантелику шляхом нав'язування, тиску, залякування, обіцянок швидкої вигоди, надання допомоги тощо.

   Ось декілька прикладів, як розпізнати шахрайські дії:

   - якщо Вам телефонують та просять повідомити конфіденційні дані, такі як: номер та термін дії карти, її ПІН-код, баланс, три цифри на звороті карти (CVV2/CVC2-код), одноразові коди з SMS, пароль до інтернет-банкінгу і т.п.,
   - якщо Вам телефонують від імені Банку та повідомляють про блокування або операції з Вашою карткою (наприклад, помилкове надходження коштів, списання, перерахунки і т.п.) та пропонують допомогу у вирішенні проблеми,
   - якщо надходять повідомлення sms або у месенджерах, наприклад, щодо виграшів авто або великої грошової суми та які містять номери телефонів для зворотного зв'язку або посилання на веб-сторінки,

   – припиняйте такі розмови негайно! Їх продовження може привести до втрати грошей!

   Зверніть увагу! Банк ніколи не запитує у клієнтів паролі, одноразові коди, копії криптографічних ключів, ПІН-коди та інформацію про строки дії платіжних карт, коди CVV2 ні телефонними дзвінками, ні в sms-повідомленнях, ні електронною поштою!

2. Не розголошуйте Ваші фінансові дані та дані Вашої платіжної карти:
   - фінансовий номер телефону,
   - кодове слово,
   - логін та пароль для входу до інтернет-банкінгу,
   - термін дії карти,
   - ПІН-код карти,
   - три цифри на звороті карти (CVV2/CVC2-код),
   - коди підтвердження з sms-повідомлень.

   Зверніть увагу! Для здійснення переказу на Вашу картку достатньо повідомити 16-значний номер, зазначений на лицевій стороні Вашої карти:

   

   Якщо у Вас запитують більше даних – можливо Ви маєте справу із шахраями.

3. При знятті готівки в банкоматах (АТМ):
   - не здійснюйте операцію, якщо щось навколо Вас викликає підозру, наприклад, дивна людина біля банкомату, незвичне розташування відеокамери на банкоматі, наявність накладок на клавіатурі/отворі для картки/отворі для видачі грошей, зовнішній вигляд клавіатури та/або картоприймача не відповідає зображенню на екрані банкомату тощо;
   - при вводі ПІН-коду прикривайте рукою клавіатуру, щоб запобігти підгляданню або запису коду на камеру, встановлену шахраєм;
   - якщо банкомат «відрахував» купюри, але вони не «вийшли» з банкомату – не відходьте від банкомату і негайно **зверніться до контакт-центру Банку за телефонами**: **0-800-50-70-80 або (044) 428-61-28**, після чого зверніться до поліції.

4. Оплата карткою та розрахунки в Інтернеті:

- використовуйте мобільний або веб додаток Банку для управління своїми платіжними картами! Не завантажуйте на телефон неперевірене програмне забезпечення (наприклад, «Універсальний мобільний банкінг», яке пропонує користуватися мобільними послугами декількох банків одночасно) – з великою ймовірністю це може виявитися шахрайським додатком!
- користуйтеся послугою GSM-banking для відстеження активності по карті;
- якщо це можливо, активуйте протокол 3DSecure для додаткового захисту операцій;
- встановлюйте ліміти на операції в Інтернеті;
- блокуйте можливість оплати картою в Інтернеті на постійній основі та активуйте її безпосередньо на момент оплати;
- надавайте перевагу способу оплати по факту отримання товару;
- робіть замовлення/покупки на перевірених інтернет-ресурсах, не здійснюйте оплату на випадкових/невідомих ресурсах.

  Зверніть увагу! Як правило, фішингові сайти, створені шахраями, мають дуже подібні до оригіналу адресу та зовнішній вигляд сторінок! Завжди звертайте увагу чи правильно зазначено адресу сайту та чи є у вікні браузера поряд з адресним рядком ознака захищеного з'єднання - значок у вигляді замкнутого замка.

- додатково перевірити, чи не внесений інтернет-сайт до «бази шахрайських сайтів» Української міжбанківської асоціації членів платіжних систем ЄМА, можна за посиланням https://ema.com.ua/report-an-incident/black-list/.
- додатково перевірити інформацію про банк та його відокремлені підрозділи можна у довіднику банків, розміщеному на офіційній сторінці НБУ, за посиланням https://bank.gov.ua/ua/supervision/institutions/.

5. У випадках

- втрати карти,
- виявлення спроби проведення несанкціонованої оплати з використанням Вашої карти;
- підозри, що дані Вашої карти стали відомі сторонній особі;
- підозри, що Ви стали «жертвою» шахраїв;
- виявлення підробленої сторінки банку (фішингового сайту)

для блокування карти та/або отримання рекомендацій щодо подальших дій негайно **зверніться до контакт-центру Банку за телефонами**: **0-800-50-70-80 або (044) 428-61-28 !**