Платіжна безпека: основні поради від Кіберполіції

Не розголошуйте всі реквізити платіжної картки та контролюйте рух коштів на рахунку Банк по телефону може запитати перші 6 та останні 4 цифри платіжної картки. **Для отримання платежу на картку достатньо повідомити лише16-значний номер картки.**

- Тримайте в секреті три цифри на звороті картки (CVV/CVC код), коди (одноразові паролі) банків та мобільних операторів, 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 в Інтернет.

Перераховуйте необхідну суму з основної картки на віртуальну перед здійсненням покупки. Віртуальну картку також можливо додати і до гаманців Apple Pay, Google Pay. Не переходьте за посиланнями від незнайомців! Шахраї розсилають шкідливі посилання в месенджери, смс, e-mail для зараження пристроїв вірусом, викрадення персональних даних, секретних карткових реквізитів, для переходу на фішингові або інші шахрайські ресурси.

Отримали посилання від друга – не поспішайте на нього клікати. Шахраї могли отримати доступ до акаунта друга. Спершу зателефонуйте другу та запитайте, чи справді посилання від нього.

Не вводьте реквізитів платіжних карток на незнайомих та підозрілих сайтах

- Перш ніж ввести в будь-яку форму дані своєї платіжної картки або паролі до онлайн
- банкінгу, перевірте адресу необхідного ресурсу, адже будь-які відмінності можуть свідчити про те, що ви опинилися на фішинговому сайті.
- Якщо необхідно перейти на сайт компанії, адресу якого ви отримали в посиланні, введіть у пошуковій системі назву необхідного сайту і лише тоді переходьте на вебресурс.

Звертайте увагу на протокол сайту http – це ненадійний протокол, це означає, що сайтом користуватися не можна **https** – потрібно продовжити перевірку сайту Також рекомендується додатково перевірити посилання сумнівних сайтів:

- на сайті Кіберполіції в розділі "Стоп фрауд". Також у цьому розділі можна перевірити на шахрайство номер телефону та банківську картку;
- через сервіс Асоціації "ЄМА" CheckMyLink ВАЖЛИВО!

Схема шахрайства може бути абсолютно новою або добре прихованою. Тому, крім перевірки сайту на сайті Кіберполіції в розділі "Стоп фрауд" та сервісі Асоціації "ЄМА" CheckMyLink, проводьте також власну перевірку. Якщо ви випадково розкрили дані платіжної картки на підозрілому сайті, негайно

телефонуйте до банку за номером, зазначеним на звороті картки. Якщо ви стали жертвою шахраїв, напишіть заяву до Кіберполіції за цим посиланням або повідомте про ваш випадок за номером телефону – 0 800 505 170. Захистіть свої акаунти двічі

1. Створіть складний пароль до електронної пошти, соціальних мереж та інтернетбанкінгу. Складний пароль може містити:

- 8 і більше символів,
- Великі та малі літери,
- Цифри та спеціальні знаки/символи. Створюйте унікальний пароль для кожного інтернет-банкінгу, електронної пошти, соціальних мереж тощо. Під час створення пароля не використовуйте: • особисту персональну інформацію (дата народження, адреса, номер телефону тощо);
- загальновідомі комбінації паролів **(наприклад, Qwerty12, Password123456, Admin1234 тощо);**
- послідовне/зворотне написання символів або цифр.

2. Установіть багатофакторну автентифікацію.

Багатофакторна автентифікація – це, коли для входу до акаунта, крім логіна та пароля, потрібно ввести код підтвердження, що приходить на смартфон,

електронну скриньку або у відповідний додаток. Налаштування багатофакторної автентифікації на прикладі інстаграму за посиланням.

Надійно зберігайте та не розголошуйте свій пін-код! Змінюйте пін-код до картки:

- регулярно: 1 раз на 3 місяці,
- ситуативно: якщо виникла підозра, що ще хтось його може знати.

#ШахрайГудбай! #Кіберполіція #БезпекаДаних