

Телефонують зі служби безпеки банку

«Перебуваючи в транспорті, я отримала дзвінок від нібито працівника банку, який повідомив, що з мого рахунку намагаються зняти кошти та переказати їх на сумнівну банківську картку. Співрозмовник наполягав, що для термінового блокування операції необхідно повідомити номер банківської картки, термін її дії та CVV-код. Саме за таким сценарієм найчастіше діють телефонні шахраї».

Телефонують з банку під виглядом працівників і виманюють реквізити карти, код (або від імені державних установ чи операторів мобільного зв'язку).

Пам'ятайте:

✓ Безпека збереження коштів та користування рахунками починається з Вас.

✓ Використовуйте під час будь-яких операцій у мережі "Інтернет" чи онлайн-оплаті послуг лише інтернет-карти, на які переказуйте кошти з основного рахунку в сумі, яка необхідна для оплати або переказу! Не дайте змоги шахраям заволодіти реквізитами до основного рахунку та викрасти кошти.

✓ Ніколи не розміщуйте об'яви в мережі "Інтернет" з вказанням фінансового номеру. Шахраї, отримавши цю інформацію, можуть звернутись до оператора мобільного зв'язку та здійснити його перевипуск, отримати доступ до інтернет-банкінгу та заволодіти коштами. Якщо ви виявили, що сімкартка з якоїсь причини заблокована, мерщій зверніться до найближчого відділення банку та заблокуйте карткові рахунки. Краще їх потім розблокувати, аніж залишитись без коштів.

✓ Використовуйте контрактну основу надання послуг мобільним оператором, тоді шахраям буде важко перевипустити ваш фінансовий номер.

✓ Використовуйте послугу код-пароллю на перевипуск або блокування сімкарт, який знаєте лише ви та мобільний оператор, бо, не маючи цієї інформації, шахрай не досягне злочинної мети.

✗ Працівник банку ніколи не зателефонує до клієнта та не буде випитувати реквізити карти, термін дії, CVV код та 3ds підтвердження, він запросить вас до відділення банку.

✗ Не повідомляйте нікому тимчасові паролі, які приходять в смс-повідомленні. Розголошення цієї інформації призведе до втрати коштів.

✗ Співробітник банку ніколи не буде телефонувати та розповідати про якісь псевдошахрайські операції по рахунку, він просто заблокує картковий рахунок і ви будете змушені звернутись до відділення банку для з'ясування обставин.

✗ Співробітник банку ніколи не запропонує встановити програми для віддаленого керування рахунками (Тімв'ювер, АніДеск та ін...).

✗ Не виконуйте ніяких дій у банкоматах чи терміналах за вказівкою співробітника банку (проведення маніпуляцій у банкоматах чи терміналах)

На замітку:

- Банк не питає секретних даних — це шахрай!
- Телефонний дзвінок — ще не доказ, що це банк!
- Коди й паролі — це твої гроші. Бережи їх!
- Шахрай намагається дізнатися більше — зупини це!
- Банківські дані — це твоє приватне життя. Захисти його!

