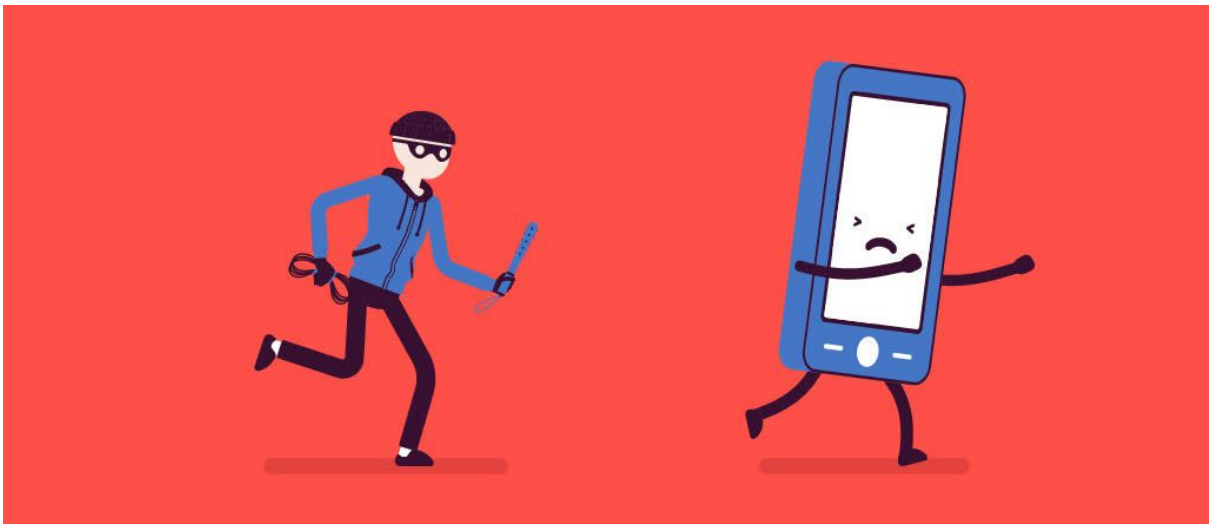
Що робити, якщо телефонують з номера банку й просять надати конфіденційні дані?

Кіберзлочинці все частіше маскують свій номер під офіційні номери банків. Розбираємося, як не стати жертвою підступів шахраїв.



Для початку перевірте, чи точно це співробітник банку. Покладіть слухавку, зателефонуйте на офіційний номер банку й уточніть, чи все в порядку з вашими рахунком і карткою.

Чому варто покласти слухавку й набрати офіційний номер банку самому?

Навіть якщо у вас на телефоні засвітився знайомий номер банку, у жодному разі не робіть на нього зворотний дзвінок. Наберіть номер гарячої лінії банку вручну. Телефон гарячої лінії можна знайти на зворотному боці банківської картки чи на офіційному сайті банку.

Така пильність може здатися параноїдальною. Але останнім часом кіберзлочинці все частіше підробляють офіційні телефонні номери банків, щоб обдурити їхніх клієнтів.

Шахраї використовують спеціальне програмне забезпечення, що допомагає приховати справжній номер абонента, при цьому на телефоні людини відображається офіційний номер банку. Зазвичай злочинець звертається до співрозмовника на ім’я та по батькові, може назвати прізвище й навіть номер і термін дії картки. Ці відомості шахраї, як правило, отримують заздалегідь з відкритих джерел, наприклад із соціальних мереж, та за допомогою фішингу.

Навіть якщо інформація звучить дуже правдоподібно, краще перестрахуватися й зателефонувати в банк самому, щоб спілкуватися точно з його співробітником, а не зі злочинцем.

Найчастіше шахраї телефонують пізно ввечері, вночі чи рано вранці у вихідні, коли людина спить і не може швидко зорієнтуватися. Злочинець представляється співробітником банку й повідомляє про підозрілу операцію, що вимагає негайних дій з боку клієнта. Шахраї добре знайомі з психологією: кажуть швидко й упевнено, використовують професійні терміни, нерідко фоном включають звуки, що імітують роботу пожвавленого контакт-центру. Усе це допомагає їм втертися в довіру до клієнта банку й зробити так, що він втратить пильність.

При цьому вони кваплять і залякують клієнта, тиснуть на його емоції та запевняють, що трапиться щось непоправне.

Наприклад, обманщики кажуть, що за карткою проводиться підозрілий платіж на велику суму й, щоб його зупинити, потрібно терміново повідомити дані картки, ПІН-код або одноразовий пароль із SMS-повідомлення. Якщо людина вагається або відмовляється їх назвати, їй погрожують, що гроші з її картки просто зараз відійдуть шахраям.

Якщо злочинцям вдається дізнатися потрібну їм інформацію, вони отримують доступ до рахунку й знімають з нього всі гроші.

Як захистити свої гроші від шахраїв?

Якщо клієнт сам повідомить злочинцям секретну інформацію, яку не можна розголошувати, повернути гроші через банк не вийде. Тому варто дотримуватися основних правил безпеки, щоб не потрапити в пастку до шахраїв і не втратити гроші:

1. Завжди телефонуйте тільки на офіційний номер банку. Його зазначено на зворотному боці картки й на офіційному сайті банку.

2. Не телефонуйте й не надсилайте SMS на незнайомі номери, не поспішайте переходити за посиланнями з повідомлень «від банку». У будь-якій незрозумілій ситуації телефонуйте в банк на офіційний номер і уточнюйте інформацію в оператора.

3. Якщо вам телефонують з банку, фінансової організації чи держоргану, уточніть П. І. Б. і посаду того, хто телефонує, після чого скажіть, що зателефонуєте йому самі. Покладіть слухавку й зателефонуйте на офіційний номер організації або на гарячу лінію банку. Номер потрібно набрати вручну.

4. Не варто панікувати й поспішати. Якщо банк виявить підозрілу транзакцію, він відразу призупинить її на строк до двох діб. За цей час ви можете або підтвердити цю операцію банку, або скасувати її. Це рішення треба ухвалити

протягом 48 годин – цього часу достатньо, щоб добре все обміркувати й без поспіху самостійно зателефонувати в банк. Якщо ж ви нічого не зробите, то через дві доби банк автоматично зніме блокування й операція пройде.

5. За жодних умов нікому не повідомляйте особисті дані, реквізити картки та секретну інформацію: CVC/CVV-код на зворотному боці картки, коди із SMS і ПІН-коди. Називати кодове слово можна, тільки якщо ви самі телефонуєте на гарячу лінію банку.