Как мошенники получают реквизиты банковских карт.

В настоящее время существует множество схем обмана держателей банковских карт. Расскажем про самые популярные как в Беларуси, так и за рубежом.

В последние месяцы зафиксирован резкий подъем несанкционированных операций со счетами клиентов банков. В подавляющем большинстве случаев они происходят через подменные телефонные номера с использованием социальной инженерии. В конце 2019 года данный вид мошенничества усилился в Беларуси, причем злоумышленники при звонках потенциальным жертвам стали чаще использовать технологию подмены телефонного номера банка (так называемый А-номер) при использовании звонков через Интернет. При таких звонках на экране телефона потерпевшего высвечивается реальный номер банка, а клиенту сообщают о попытке несанкционированного списания средств. Для защиты средств клиенту предлагают перевести их на специальный счет, сообщить полную информацию по карте, кодовое слово или данные из СМС. Нередко клиент, сбитый с толку информацией, которую может знать только банк, рассказывает незнакомцу на другом конце провода, о чем его просят. И после этого происходит хищение. Для совершения подобных звонков злоумышленники используют IP-телефонию. Применяя один из протоколов такой связи (SIP-протокол), звонки можно проводить с помощью компьютера, установив специальную программу; через сети Wi-Fi или 3G/4G с помощью SIP-программ для планшетов и мобильных телефонов; используя специальный стационарный SIP-телефон, который включаются в роутер; через обычный телефон, подключив его к VoIP-шлюзу, а сам шлюз — к роутеру.

Блокировка карты.

Клиент банка получает сообщение "Ваша карта будет заблокирована". Также в сообщение говорится, что нужно обратиться по номеру телефона из SMS-сообщения, чтобы избежать блокировки карты.

При звонке по указанному номеру, человеку сообщают, что его карта действительно заблокирована и для решения проблемы надо сверить данные карты. Таким образом, владелец карты выдает всю информацию: ее номер, срок действия и CVV-код.

Если Вам вдруг пришло такое SMS, то лучше обратиться в отделение банка или позвонить в банк по телефону, указанному на официальном сайте!

Неожиданный перевод от неизвестного отправителя.

На телефон держателя карты поступает SMS-уведомление о поступлении денежного перевода. В сообщении также указано, что деньги заморожены и чтобы их разблокировать - нужно позвонить по номеру из сообщения. Дальше все по такой же схеме, как и в первом случае. Мошенники просят подтвердить данные, запросив Ваши ФИО, номер карты и т.д. Стоит отметить, что в первой и второй схеме мошенникам также может потребоваться SMS-подтверждение. Во время звонка держателя карты просят продиктовать проверочный код, который приходит в SMS, чтобы якобы удостовериться в личности звонящего. Надо ли говорить, что диктуя код из сообщения, человек собственноручно подтверждает мошенническую операцию – переводит деньги на чужую карту.

Многие считают, что без CVV-кода (три цифры на обратной стороне карты) преступники не смогут снять средства с их счета, но это ошибочное мнение. Даже если введен неверный CVV, но код подтверждения из SMS верный – транзакция все равно будет совершена.

Фишинговые сайты

Суть фишинговых сайтов заключается в том, что мошенник создает интернет-страницу внешне не отличимую, либо слабо отличимую от настоящей страницы, на которой у пользователя запрашивается конфиденциальная информация. Это может быть не только данные банковской карты, но и любая другая информация: логины, пароли от соцсетей, почты и т.д.

Следует обратить внимание, что фишинговый сайт может копировать любые сайты в интернете, начиная от страниц социальных сетей и заканчивая почтовыми сервисами, сайтами банковских организаций и платежных систем.

У современного человека должны быть минимум три карты: сберегательная, на которой деньги просто хранят, зарплатная – для совершения всевозможных оплат и виртуальная, на которую можно всегда перевести ограниченную сумму для расчетов и покупок в сети Интернет.

Помните: Ваша беспечность - в Ваших руках. Будьте бдительными!