Основные правила безопасного пользования банковскими картами.

1. Необходимо ХРАНИТЬ НОМЕР КАРТЫ И ПИН-КОД ВТАЙНЕ ОТ ДРУГИХ. Помните, ни одно лицо (включая работников банка, выдавшего карту) и ни при каких обстоятельствах не вправе запрашивать по мобильным и стационарным телефонам ПИН-код или код проверки подлинности карты (CVV2 или CVC2).

2. Ни при каких условиях НИКОМУ (даже представителю банка!) НЕ ДАВАЙТЕ ПАРОЛЬ ДОСТУПА к своему счету через Интернет.

3. ПРИ УТЕРЕ ИЛИ ХИЩЕНИИ КАРТЫ немедленно позвоните в службу поддержки банка и попросите ЗАБЛОКИРОВАТЬ ВАШУ КАРТУ. Чем быстрее вы это сделаете, тем больше вероятность того, что мошенники не успеют ею воспользоваться.

4. Необходимо всегда ИМЕТЬ ПРИ СЕБЕ (в записной книжке или в мобильном телефоне) КОНТАКТНЫЕ ТЕЛЕФОНЫ БАНКА И НОМЕР БАНКОВСКОЙ КАРТЫ.

5. SMS-ОПОВЕЩЕНИЕ О ПРОВЕДЕННЫХ ОПЕРАЦИЯХ ПО КАРТЕ позволяет быстрее узнать, что деньги со счета списали без вашего ведома. Чем скорее клиент уведомит банк о несанкционированном списании средств, тем больше у него шансов получить свои деньги обратно.

6. ПРИ РЕШЕНИИ ВСЕХ ПРОБЛЕМНЫХ СИТУАЦИЙ обращайтесь только по ОФИЦИАЛЬНЫМ НОМЕРАМ ТЕЛЕФОНОВ БАНКА. Если вам предлагают позвонить по другому номеру, то это, скорее всего, мошенники, которые пытаются узнать у вас информацию о вас и вашей карте, чтобы украсть деньги.

7. БУДЬТЕ ВНИМАТЕЛЬНЫ К УСЛОВИЯМ ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ БАНКОВСКОЙ КАРТЫ. Не подвергайте ее механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

8. Установленный лимит суточного снятия наличных по карте убережет от снятия мошенниками суммы сверх этого лимита.

Существует немало способов хищения денег с кредитных карт. Основные из них:

1. Копирование информации с карты

Практикуется при оплате картой счета в ресторане, клубе или магазине. Сотрудник под каким-либо предлогом уносит вашу карту и копирует все ее данные, включая секретные цифры (CVV/CVC-код) с обратной стороны. Имея указанные сведения, мошенник сможет расплатиться вашей картой на многих сайтах.

2. Фишинг

Осуществляется с помощью поддельных сайтов банка, отличающихся от настоящих какой-нибудь неприметной мелочью — например, одной буквой в названии. Пользователь карты думает, что он находится на сайте своего банка и собственноручно вводит все необходимые данные карты. Не стоит объяснять, как воспользуется этими данными владельцы сайта.

3. Выяснение пин-кода по телефону или интернету.

Такие способы также называют «социальными», поскольку никаких технических приемов мошенниками не используется - лишь коммуникабельность и знание человеческой психологии. «Вам звонят из банка N. Наш сайт был взломан, данные вашей карты были похищены! Срочно продиктуйте номер карты и пин-код, чтобы мы могли немедленно

заблокировать карту и уберечь ваши деньги от злоумышленников». И пользователь сам диктует свой пин-код, да еще и благодарит мошенников за оказанную «услугу».

Письма с аналогичным содержанием могут приходить и на вашу почту.

Еще раз напоминаем: никогда и ни при каких обстоятельствах сотрудники банка не могут выяснять ваш пин-код. Он должен быть известен только вам.

При получении какой-то смс или звонка с сообщением о «блокировке счета», следует перезвонить в ваше отделение банка по официальному телефонному номеру, указанному на сайте, либо прийти в отделение лично.

4. Хищение карты вместе с пин-кодом либо с телефоном.

При хищении карты вместе с мобильным телефоном, преступники могут снять деньги или воспользоваться Вашей картой для оплаты, используя секретные коды, приходящие на ваш номер. Еще проще будет похитить ваши средства, если вы имеете привычку носить бумажку с пин-кодом вместе с картой.

Будьте бдительны!