Наша финансовая безопасность напрямую зависит от принимаемых ежедневно решений. Банковские карты - удобный инструмент повседневных расчетов. При этом, способы обмана людей и кражи денежных средств с их банковских карт очень разнообразны. В наших силах избежать негативных последствий от мошеннических действий, соблюдая простые меры безопасности, направленные на предупреждение таких последствий.

Причины хищения денежных средств:

- незащищенность компьютеров от современных вирусов (антивирусное программное обеспечение не эффективно);
- массовое заражение крупнейших легальных сайтов вирусами;
- возможность удаленно управлять зараженным компьютером через сеть Интернет;

- низкая компьютерная грамотность.

Примеры схем финансового мошенничества:

- внедрение на компьютер жертвы вредоносной троянской программы либо манипулирование по телефону методами социальной инженерии;
- получение информации о персональных данных, номерах счетов и карт;
- получение дубликата SIM-карты в офисе оператора по поддельному паспорту, водительскому удостоверению, нотариальной доверенности;
- мониторинг финансовых потоков жертвы, выбор момента совершения преступления;
- использование дубликата SIM-карты в телефоне мошенников, перехват сообщений;

- хищение средств и перевод их на банковские счета, карты, счета мобильных телефонов или электронные кошельки, контролируемые мошенниками;
- снятие наличных денежных средств либо покупка товаров и услуг для последующей перепродажи.

Пример содержания мошеннической рассылки:

- «Ваша карта заблокирована, информация по телефону +7 (903) ###-11-11»;
- «По Вашей карте запланирован платеж на сумму 33500 рублей. Для отмены позвоните по телефону +7 (903) ###-11-11»;
- «Вам поступил платеж на сумму 5768 фунтов стерлингов. Подтвердите получение, иначе платеж будет возвращен отправителю. Телефон для справок 8(800) ###-11-11»;

- «Поздравляем! Вы выиграли компьютер! Информация по телефону 8(800) ###-11-11».

Цель сообщения – инициировать звонок держателя карты мошенникам.

Во время звонка клиента убеждают подойти к банкомату и выполнить ряд процедур либо выясняют конфиденциальную информацию о карте. Системе ДБО, кодовые слова.

Способы защиты. Инструкция для потребителя.

- Использовать сложные пароли;
- Никому не передавать данные для входа в систему, в т.ч. сотруднику банка;
- При использовании одноразовых паролей по SMS, с особым вниманием отнеситесь к тому, что доступ третьих лиц к телефону невозможен;
- Перед вводом кода подтверждения операции из SMS всегда проверяйте параметры операции, содержащиеся в сообщении;
- Вход в систему с чужого компьютера не является безопасным;
- Установите и настройте антивирусное программное обеспечение;
- Регулярно устанавливайте обновление безопасности;
- При подозрении, что Ваши данные для входа в систему стали известны третьим лицам, при утере телефона, устройства, которые Вы используете для подтверждения операции в системе, или обнаружении несанкционированных операций в системе, незамедлительно обратитесь в банк;
- Установите лимиты.

Угрозы при использовании банковских карт:

- Физические: хищение банкомата, взлом банкомата, вандализм;
- Интеллектуальные: скимминг, фальшивый банкомат, траппинг (захват карты или

наличных), кибератаки (вредоносное ПО и др.), получение наличных денежных средств по поддельным, утраченным картам.

Угрозы нападения у банкомата:

- Неподобающее место;
- Ночное время суток;
- Поступки, провоцирующие грабеж;
- Невнимательность, беспечное поведение держателя;
- Проведение операций если рядом находятся какие-то посторонние люди.

Как избежать:

- Осмотреться перед снятием денег;
- Использовать зеркала на банкомате, чтобы видеть, что происходит сзади Вас;
- При снятии крупной суммы договориться о сопровождении.

«Бытовые звонки»:

Мошенники используют украденные базы данных с информацией об адресах, номерах телефонов, истории болезни в поликлинике.

- Мошенники звонят на домашний телефон и сообщают о некотором событии;
- Методами социальной инженерии побуждают жертву перевести средства либо впустить в квартиру «представителя» для общения;
- Жертва переводит средства на счет мобильного телефона либо карты мошенников, для «подтверждения кода» или «участия в социальной программе» либо приобретают бесполезные предметы по завышенным ценам, либо подвергается ограблению в квартире.

Цель – путем сообщения о якобы «важной» информации добиться от жертвы исполнения инструкций мошенников либо допустить в квартиру.

Меры безопасности:

- Не открывайте неизвестные вложения в письмах;
- Не нажимайте, не подумав, на короткие ссылки;
- Осмотрительно используйте публичный Wi-Fi;
- Устанавливайте обновления безопасности;
- Используйте разные пароли для различных аккаунтов;
- Устанавливайте и обновляйте антивирус;
- Создавайте и обновляйте резервные копии документов;
- Обращайте внимание на сообщения браузера о безопасности;
- С осторожностью публикуйте в социальных сетях персональную информацию;
- Скачивайте только необходимые приложения и из известных источников;
- С осторожностью подходите к любым финансовым сервисам, требующих ввода данных Вашей карты, счета, персональных данных, телефонов, адресов.

Правила поведения:

- При любой операции с картой или с денежными средствами продумывайте свои действия и учитывайте возможные зловредные действия мошенников;
- Используйте только банкоматы, установленные в безопасном месте;
- Внимательно относитесь к компьютерной безопасности;
- Не оставляйте карту без присмотра, не передавайте ее никому;
- Никому и никогда не сообщайте ПИН-код, одноразовые пароли и другую информацию, пришедшую из банка по СМС;
- Сотрудник банка никогда не может запросить номер карты, ПИН-код, пароли, пришедшие по СМС;
- При любой проблеме с картой, сомнениях, подозрении о компрометации карты, срочно свяжитесь с банком исключительно по телефонам, указанным на обороте карты или на сайте банка.

В случае необходимости получения дополнительной информации по вопросам финансовой безопасности, защите прав потребителей финансовых услуг потребители могут обратиться в Единый Консультационный Центр Роспотребнадзора (ЕКЦ) по телефону 8(800)555-49-43, а также в отдел защиты прав потребителей Управления Роспотребнадзора по Республике Алтай по телефону 8(38822) 6-42-41, или к специалистам консультационного центра по защите прав потребителей тел. 8 (38822) 6-36-22.