Мошенничество с картами в сети Интернет

Не сообщайте данные карты и не передавайте SMS-коды неизвестным людям

1. **Человек размещает объявление о продаже чего-нибудь в интернете**
   Диван, телевизор — всё, что угодно
2. **Мошенники звонят по указанному номеру и прикидываются покупателями**
   В разговоре они узнают данные карт, якобы для того, чтобы перечислить деньги за покупку.
3. **Мошенник подключаются к мобильному приложению и списывает со счёта деньги**

Мошенники просят внести предоплату, после получения суммы больше не выходят на связь

- **Никому не говорите номер карты или счёта и, что важнее, трехзначный код,**
- **расположенный на оборотной стороне карты, а также никогда никому**
- **не передавайте SMS-код, который приходит к вам от номера 900.**

Телефонные мошенничества

Социальная инженерия: не переводите деньги незнакомым людям

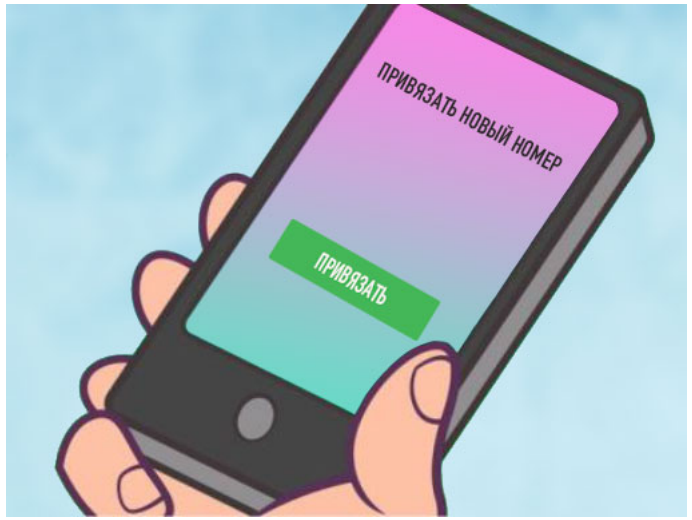
Использование социальной инженерии— один из самых распространённых способов мошенничества

1. Обычно человеку звонит мошенник, представляется полицейским или, к примеру, следователем и говорит, что ваш родственник или друг устроил аварию, кого-то избил или как-то ещё нарушил закон.

2. Чтобы уладить вопрос «по-хорошему», мошенники просят перечислить с карты определённую сумму денег.

Будьте бдительны: если попадёте на такой звонок, обязательно свяжитесь для начала с человеком, которого пытаетесь спасти. Вероятно, с ним всё в порядке, а вас просто кто-то пытается обмануть

Мобильный банк



Социальная инженерия: Не привязывайте чужой номер телефона к своему мобильному банку

Под различными предлогами (в первую очередь компенсации) злоумышленники выуживают у клиента информацию, необходимую для проведения операции, дополнительно клиенты под воздействием злоумышленников подключают телефон злоумышленников к сервису «Мобильный банк».

После получения доступа, мошенник может перевести все деньги с вашего счета на чужой

Будьте бдительны: всегда внимательно относитесь к звонкам с незнакомых номеров. Нередки случаи, когда мошенники представляются сотрудниками банка или государственных служб. Звонить в банк только по номерам, указанным на карте.

Воровство данных кредитных карт с помощью вирусов и троянов на компьютере

Не устанавливайте неофициальные версии мобильных приложений

1. Мошенники через интернет или смс-сообщения распространяют вирус.

2. Припопытке открыть приложение банка, вирус перенаправляет вас на сайт-ловушку, который внешне мало чем отличается от настоящего сайта банка.

3. На этом сайте клиента просят ввести свой логин от личного кабинета. И вирус получает и отсылает мошенникам пароли для входа.

Не пользуйтесь сомнительными приложениями и регулярно обновляйте антивирусы на своих смартфонах

Обман владельца банковской карты по телефону/SMS

Не доверяйте сомнительным сообщениям о блокировке карты

Мошенники могут присылать SMS-сообщения о том, что банковская карта заблокирована. **На самом деле — нет.**

Чтобы разблокировать карту, человека просят прислать персональные данные, PIN-код или набрать цифры, с помощью которых активируют услугу перевода средств на чужой номер.

Запомните: никто не имеет права узнавать у вас такую информацию. И уж тем более никому вы не должны сообщать свой PIN-код. Держите его только при себе.

Мошенничество при оплате безналичных счетов в гостиницах, кафе и ресторанах

Никогда не давайте людям «подержать» свою карту

Информации, которая указана на карте, достаточно для того, чтобы совершить с её помощью покупку в интернете. Поэтому **карту лучше вообще никому не давать в руки**

Даже в кафе опасно расплачиваться картами, когда, к примеру, официант её уносит, чтобы провести платёж. В идеале — не давать официанту карту, а самому вставлять её в устройство и вводить пароль.

И обязательно — использовать карту, которая связана с вашим номером телефона.

Если кто-то другой захочет что-то оплатить вашей картой, вам придёт код-подтверждение. Игнорируйте этот код и не сообщайте его другим людям

Информация на карте

Никогда не пишите PIN-код карты на самой карте

Карту можно где-то забыть или потерять. Или, к примеру, при оплате в магазине карта попадает в руки продавцов

Написанный на карте **PIN-код является большим соблазном** для того, чтобы без труда воспользоваться ею

Выход простой — никогда не указывайте на карте PIN-код

Информация из чеков

Не выбрасывайте в урну чек, который печатает банкомат

При оформлении новой карты и её активации прямо в банке люди обычно выбрасывают в ведро чек, выданный банкоматом.

Мошенники могут подобрать выброшенную бумагу, где указана информация с логинами и паролями для входа в онлайн-банк, и перевести деньги на свой счёт

Забирайте чек с собой

Сбербанк сегодня

СБЕРБАНК
Всегда рядом

Может направлять e-mail – сообщения со ссылкой для входа в Личный кабинет или сервис саморегистрации системы Сбербанк Онлайн при этом ссылка ведет на официальный сайт Банка.

При рассылке СМС/MMS/e-mail – сообщений всегда обращаться адресно, в сообщении от имени Сбербанка. Всегда указываются имя и отчество клиента либо последние цифры номера карты держателя

Отправляет СМС – сообщения только с номера «900»
для ряда регионов 9000, 9001, 8632, 6470, SBERBANK

Правила безопасности

Для телефона, планшета и компьютера

1. **Используйте антивирус** или установите приложение «Сбербанк Онлайн» с бесплатным антивирусом для телефонов Android
2. **Не переходите по ссылкам с незнакомых ресурсов** в целях исключения вирусного заражения ваших устройств
3. **Используйте только официальные приложения Банка** из магазинов **AppStore, Google Play, WindowsStore**
4. **Информируйте Банк** о смене номера Вашего мобильного телефона, подключенного к услуге Мобильный банк
5. **Не сообщайте третьим лицам,** включая сотрудников Банка, свои конфиденциальные данные: подтверждающие пароли, PIN/CVV коды от банковских карт
6. **Проверяйте реквизиты** операции в СМС от Банка с подтверждающим паролем