



КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИЧЕСТВА

Март 2019

Назаров Михаил

Руководитель активных
продаж ПАО «Почта Банк»



Финансовая безопасность

Финансовое мошенничество — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

- **Мошенничества с использованием банковских карт**
- **Интернет-мошенничества**
- **Мобильные мошенничества**
- **Финансовые пирамиды**

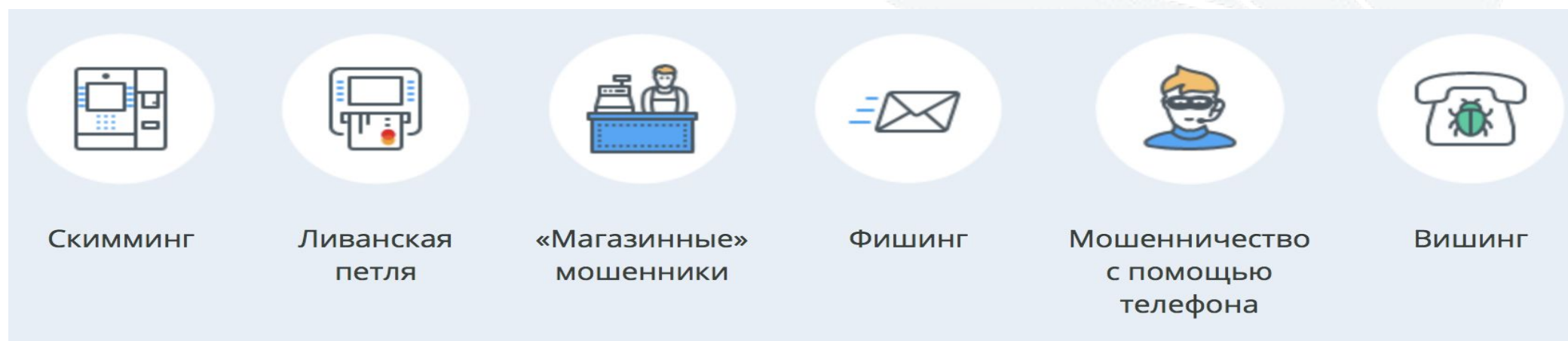
Мошенничества с использованием банковских карт

КАРТА

**7 из 10 совершеннолетних
россиян владеют банковскими
картами***



СХЕМЫ МОШЕННИЧЕСТВ С КАРТАМИ



Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение. При этом преступники постоянно придумывают новые способы хищения денежных средств, по мере того как старые перестают работать. Именно поэтому важно быть в курсе основных приемов, которые используют злоумышленники, и соблюдать базовые правила безопасности.

СКИММИНГ

Предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте.



При использовании банкомата осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних предметов.

ТРАППИНГ (ЛИВАНСКАЯ ПЕТЛЯ) или помощь прохожего.



Отрезок фотопленки (складывается пополам, края загибаются под углом в 90 градусов) вставляется в банкомат. На нижней стороне фотопленки вырезан небольшой лепесток, отогнутый вверх по ходу карты. Пленка располагается в картридере так, чтобы не мешать проведению транзакции. Отогнувшийся лепесток не позволяет банкомату выдать пластиковую карту обратно.

МАГАЗИННЫЕ МОШЕННИЧЕСТВА



От недобросовестных сотрудников в организациях не застрахован никто. Данные карты могут быть считаны и зафиксированы ручным скиммером, а впоследствии использованы для хищения денег.

ФИШИНГ

Цель фишинга — получить данные о пластиковой карте от самого пользователя. В этом случае злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности.

Самая сложная задача мошенника — узнать ваш ПИН-код.

Никому не сообщайте свой ПИН-код!!!

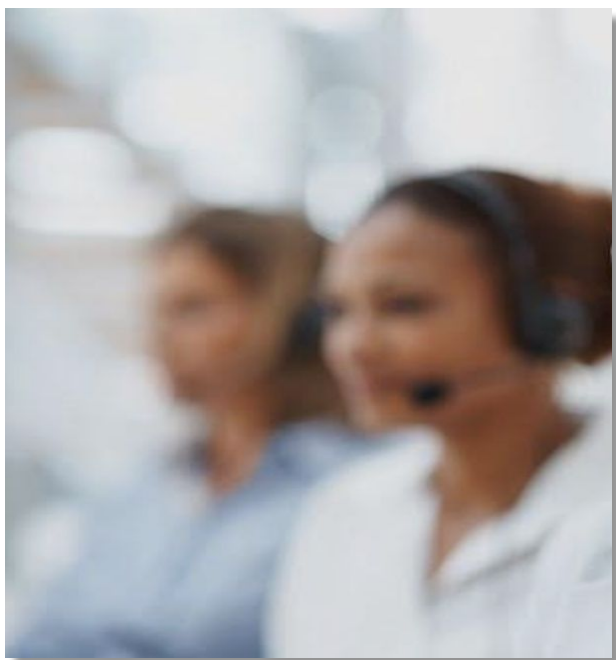
МОШЕННИЧЕСТВО С ПОМОЩЬЮ ТЕЛЕФОНА



Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту.

Банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

ВИШИНГ (ГОЛОСОВОЙ ФИШИНГ)



Новый вид мошенничества, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов.

ИНТЕРНЕТ-МОШЕННИЧЕСТВО

ПОКУПКИ ЧЕРЕЗ ИНТЕРНЕТ

Покупатель (жертва) соглашается купить у продавца (мошенника) товар через интернет. Продавец просит оплатить товар через систему денежных переводов и получает деньги, используя зачастую фальшивое или недействительное удостоверение личности. Обещанный товар не доставляется покупателю.



Такая схема мошенничества обычно имеет один или несколько явных признаков — например, предлагаемый товар продается по удивительно низкой цене.

МОБИЛЬНЫЕ МОШЕННИЧЕСТВА

ВИДЫ МОБИЛЬНЫХ МОШЕННИЧЕСТВ



«Вы выиграли
приз...»



«Мама, я попал
в аварию...»



«Ваша банковская
карта
заблокирована...»



Вирус

Основных видов мобильного мошенничества немного, но их вариаций достаточно много, причем все они выгодны для мошенников и приносят им огромные суммы денег. Даже при небольших финансовых потерях конкретного человека (15-150 рублей) срабатывает эффект масштаба, когда жертвами становятся тысячи людей.

По данным международной статистики, совокупные потери операторов связи и абонентов от мобильного мошенничества ежегодно составляют примерно 25 млрд долларов.

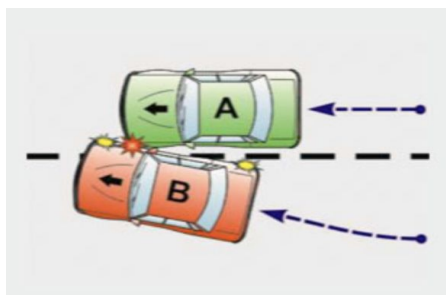
«ВЫ ВЫИГРАЛИ ПРИЗ...»



Мошенник привлекает «жертву» дорогим подарком, который выиграл абонент, но при этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код.

Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.

«МАМА, Я ПОПАЛ В АВАРИЮ...»



Эта схема направлена на воздействие на психику человека. Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.

«ВАША КАРТА ЗАБЛОКИРОВАНА»



ВИРУС



На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону...».

Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

КАК НЕ СТАТЬ ЖЕРТВОЙ ФИНАНСОВОЙ ПИРАМИДЫ

ФИНАНСОВАЯ ПИРАМИДА



Если говорить о деньгах, то нами движут два основных чувства: страх потерять заработанное и желание максимально преумножить то, что уже есть. К сожалению, часто именно второе чувство притупляет осторожность и приводит к плачевным финансовым результатам.

Финансовая пирамида – схема инвестиционного мошенничества, в которой доход по привлеченным денежным средствам образуется не за счет вложения их в прибыльные активы, а за счет поступления денежных средств от привлечения новых инвесторов.

ПРИНЦИП РАБОТЫ

Инвесторов побуждают вкладывать денежные средства обещанием получения высокой гарантированной доходности. Поскольку нет возможности обеспечить в течение длительного времени постоянный приток денежных средств новых инвесторов, ресурсы финансовой пирамиды начинают сокращаться, а финансовые обязательства растут. Возможность возврата вложенных средств с течением времени становится всё меньше.

Закономерным итогом такой ситуации становится крах финансовой пирамиды, в результате которого инвесторы теряют вложенные средства.





Одна из главных задач нашего общества – обеспечение безопасности пожилых граждан. Приведенные ниже рекомендации помогут Вам обезопасить себя и своих близких от неприятностей.

ВНИМАНИЕ!

Чтобы не стать жертвой мошенников:

- **никогда не открывайте двери незнакомым Вам людям, кем бы они ни представлялись, если вы предварительно не вызывали их к себе домой;**
- **узнайте заранее телефоны полиции, социальных служб, пенсионного фонда и если незнакомый Вам человек представляется служащим государственной организации, узнайте его фамилию, имя, отчество, должность и причину посещения;**
- **если человек представился сотрудником социальной службы, попросите поднести к глазку двери служебное удостоверение;**
- **если Вы открыли дверь, не впускайте незнакомца в квартиру или дом;**
- **если человек настойчиво просится в квартиру, позовите соседей по лестничной площадке присоединиться к Вам;**
- **позвоните родным и сообщите о «непрошенном госте»;**
- **не отдавайте документы (паспорт, пенсионное, ветеранское удостоверение и другие документы);**
- **ничего не подписывайте;**
- **не оставляйте незнакомца одного в комнате;**

- **если человек представился сотрудником социальной службы, попросите поднести к глазку двери служебное удостоверение;**
- **если Вы открыли дверь, не впускайте незнакомца в квартиру или дом;**
- **если человек настойчиво просится в квартиру, позовите соседей по лестничной площадке присоединиться к Вам;**
- **позвоните родным и сообщите о «непрошенном госте»;**
- **не отдавайте документы (паспорт, пенсионное, ветеранское удостоверение и другие документы);**
- **не давайте денег и не меняйте незнакомым Вам людям деньги;**
- **ничего не подписывайте;**
- **не оставляйте незнакомца одного в комнате;**
- **не приобретайте у людей, представившихся представителями торговых фирм продукты, мелкую бытовую технику, лекарства;**
- **сообщайте в полицию о подозрительных лицах, появившихся в Вашем подъезде;**
- **если же случилось, что Вас обокрали или обманули, немедленно звоните в полицию.**

РЕЗЮМЕ



- Проявляйте бдительность и внимательность к своим ежедневным финансовым операциям.
- Никогда никому не сообщайте ваши пароли, ПИН-код, CVV.
- Используйте антивирусное программное обеспечение.
- При совершении платежей в интернете обязательно проверяйте, какой URL стоит в адресной строке
- Не передавайте банковскую карту третьим лицам.
- Обязательно установите пароль для разблокировки телефона, особенно если на нем установлено банковское мобильное приложение.
- Гарантирование доходности по инвестициям, в несколько раз превышающей рыночный уровень, является признаком финансовой пирамиды.
- При получении сомнительных СМС от банков или лиц, представившихся родственниками, позвоните в банк или родственникам, уточните информацию. Не отвечайте на сомнительные СМС.
- Если Вы стали жертвой финансовых мошенников, сообщите в полицию.



СПАСИБО ЗА ВНИМАНИЕ!