Альфа-Банк

ОСНОВЫ

ФИНАНСОВОЙ БЕЗОПАСНОСТИ

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

Трапинг

Магазинные мошенники

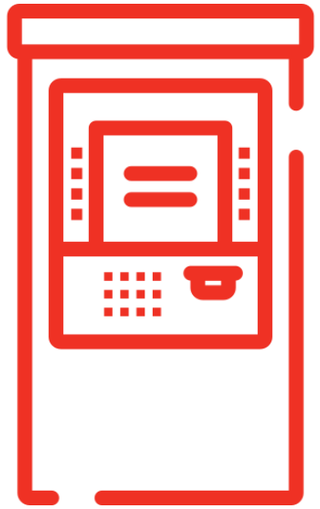
Фишинг

Мошенничество С помощью телефона

Вишинг

Скимминг

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



Таковыми выступают накладная клавиатура (очень похожая на настоящую) и устройство для считывания данных карты, которое устанавливается на картридер. Вместо клавиатуры может быть установлена миниатюрная камера, которая заснимет процесс ввода ПИН-кода.

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

Траппинг

СУТЬ ЭТОГО ВИДА МОШЕННИЧЕСТВА ЗАКЛЮЧАЕТСЯ В УСТАНОВКЕ НА БАНКОМАТ УСТРОЙСТВА, КОТОРОЕ БЛОКИРУЕТ КАРТУ И НЕ ВЫДАЕТ ЕЕ ОБРАТНО.

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.

На помощь человеку приходит «добрый» мошенник, раздавая различные советы. В процессе «помощи» растерянный человек обычно соглашается на введение ПИН-кода, который и запоминает преступник. После чего мошенник «уходит», советуя обратиться в банк. Растерянный человек оставляет карту в банкомате, а мошенник спокойно ее достает и использует по своему усмотрению.

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.

- Не передавайте карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца, CVV/ CVC-код) могут быть использованы для чужих покупок
- Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения (например, официантам или кассирам)

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.

При этом мошенники просят доверчивых пользователей возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код. Сделать это предлагается несколькими способами: либо отправив ответное письмо, либо пройдя на сайт банка-эмитента и заполнив соответствующую анкету. Однако ссылка, прикрепленная к письму, ведет не на ресурс банка, а на поддельный сайт, имитирующий работу настоящего.

! Самая сложная задача для мошенника — узнать ваш ПИН-код. Никому не сообщайте свой ПИН-код.

Мошенничество с помощью телефона

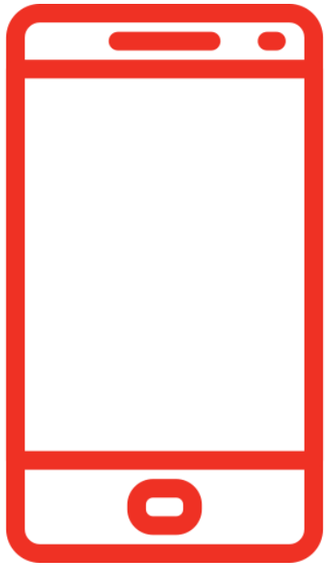
Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту.
Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его пластиковой карты.
В дальнейшем указанная информация используется для инициирования несанкционированных денежных переводов с карточного счета пользователя.

! 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.

Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:



- Автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется вымышленным именем от лица финансовой организации.
- Когда по этому номеру перезванивают, на другом конце провода отвечает типичный компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона.
- Затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как CVV-код, срок действия карты, дата рождения, номер банковского счета и т. п.

Меры безопасности

Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. При его потере или краже -заблокируйте карту

Сохраняйте все документы до окончания проверки правильности списанных сумм

Сообщайте банку актуальные контактные данные

Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки

! В случае мошеннической или ошибочной операции по карте уведомите банк до конца следующего дня, чтобы сумма этой операции была полностью возмещена банком, иначе вернуть деньги будет гораздо сложнее.

Социальная инженерия – как нами манипулируют

Приемы социальной инженерии

Предъявляется «приманка», формирующая положительные (выигрыш в лотерею, оплата выставленного вами на продажу товара), или негативные эмоции (претензия по неоплаченному налогу, взыскание по долгу коллекторским агентством, несанкционированное списание средств со счета, блокировка карты).

Злоумышленник представляется сотрудником государственных органов, банка, страховой компании, электронного магазина и т.д

Создается дефицит времени для принятия решения: «чтобы приз не ушел к другому, перезвонить или сообщить свои данные нужно в ближайшие пять минут», «чтобы избежать повестки суд, необходимо оплатить задолженность в течение 24 часов» и т.д.

Результат

В условиях необходимости быстрого реагирования наш мозг автоматически переводится в режим стресса. Мы следуем инструкциям мошенников

Социальная инженерия – что делать в ответ

1 **Необходимо осознать, что тебя ставят в условия немедленного принятия решения**, и зажечь «красную лампочку». Покупки-продажи финансовых продуктов и услуг не должны совершаться в течение ближайших 5 минут.

2 **Необходимо любыми способами убрать влияние дефицита времени, взять паузу**. Если собеседник говорит вам «Сейчас или никогда!», смотри пункт первый.

3 **Успокоиться и трезво оценить ситуацию:**

- медленно подышать – это один из способов снизить частоту пульса и перевести свой организм и мозг из режима быстрого реагирования в спокойный режим;
- проверить информацию, которую вы успели получить от звонившего (посмотреть в сети Интернет информацию об аналогичных ситуациях или позвонить по официальному номеру в компанию от имени которой вас ожидают призы или угрозы;
- позвонить родным, другу, кому-то, кто мог бы посмотреть на ситуацию взглядом, не замутненным эмоциями, и указать вам на риск мошенничества.

Виды интернет-мошенничеств

Мошенничество в интернете включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Этот перечень обширен, поскольку мошенники по максимуму используют все преимущества интернет-коммуникаций: массовый охват, возможность выбора целевой группы, оперативность.

Покупки через интернет

Составляем гороскоп

Письма от платежных систем, судебных приставов и др.

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.

Составление гороскопа

Объявлений, предлагающих заказать персональный гороскоп, очень много во всемирной паутине. Авторы обещают выслать его быстро и бесплатно. Пользователю предлагается заполнить стандартную анкету (имя, фамилия, дата рождения), оставить свой электронный адрес.

Любитель астрологии указывает все эти данные, но вместо гороскопа в его ящик попадает письмо с еще одним условием: чтобы получить заказ, надо отправить по указанному номеру СМС-сообщение с набором тех или иных цифр. При этом забывают добавить, что стоимость этого сообщения может составлять несколько сотен рублей. В лучшем случае ему, действительно, пришлют гороскоп. Причем сразу же, что уже вызывает сомнения в его уникальности. В худшем — ничего не пришлют.

Письма платежных систем

Вы можете обнаружить в своем почтовом ящике письмо от администрации платежной системы (e-gold, Moneybookers, Paypal), судебных приставов и других… В послании, например, говорится, что у вас есть долг по кредиту и вам нужно срочно сверить данные в файле. К письму прилагается вложение — файл, который нужно скачать и открыть. Или же в письме есть ссылка, по которой нужно перейти «для скачивания программы».

! На самом деле часто вас поджидает вирус, задача которого - собрать данные о ваших аккаунтах в платежных системах, данные банковской карты, которые вы вводите на своем компьютере.

Способы защиты

Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой URL стоит в адресной строке, или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от настоящего сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные и они станут известны мошенникам.

Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах

Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров, но никак не на других ресурсах.

Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.

Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку. Настоящие работодатели никогда не просят денег с соискателей, они сами платят за работу!

Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, отправляйте в корзину, не открывая. Техническая поддержка платежных систем никогда не рассылает таких писем.
В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

Виды мобильных мошенничеств

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.

Вы выиграли приз

Мама, я попал в аварию

Ваша карта заблокирована

Вирус

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

Виды мобильных мошенничеств

«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.

Виды мобильных мошенничеств

«Ваша карта заблокирована»

На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону…». «Жертва» перезванивает по указанному номеру и «сотрудник банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.

Вирус

Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.
В 2014 г. сотрудники компании Tele2 приняли от абонентов и обработали 17 640 обращений с жалобами на разные виды мошенничества. На диаграмме представлены основные виды мошеннических схем.

Способы защиты

Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки. С вашего счета могут списать деньги.

При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию. Банк никогда не сообщает подобным образом информацию.

Не отправляете СМС на короткие номера, заранее не узнав стоимости подобного сообщения. Это можно сделать на сайте своего оператора мобильной связи.

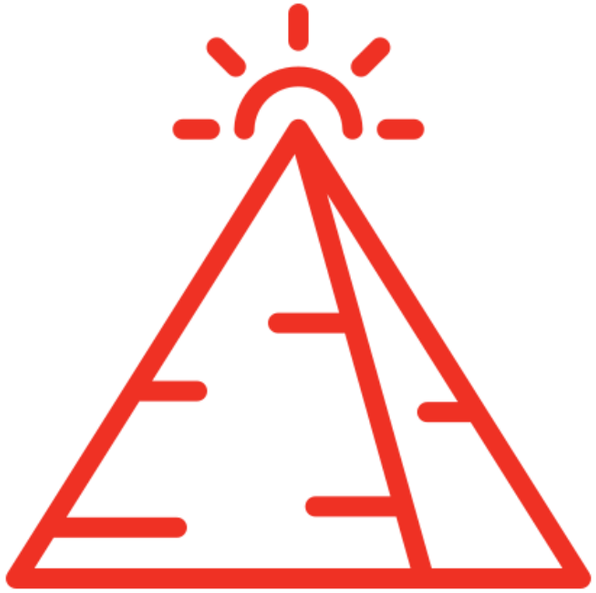
Никогда не сообщайте никаких персональных данных (дату рождения, ФИО, данные о родственниках и т. д.), даже если вам звонят и представляются сотрудником банка, полиции, мобильных операторов и т. д. Попросите представиться, назвать ФИО, звание-должность, поинтересуйтесь, какой адрес у отделения, офиса, уточните наименование организации. Затем узнайте телефон этой организации в справочных базах и перезвоните. Помните: мошенники могут использовать ваши персональные данные в разнообразных преступных схемах, вплоть до открытия на ваше имя фирмы.

Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, за решетку, в больницу и за него нужно внести залог, штраф, взятку — откупиться. Не верьте! Позвоните вашему родственнику.

Ценную информацию никогда не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

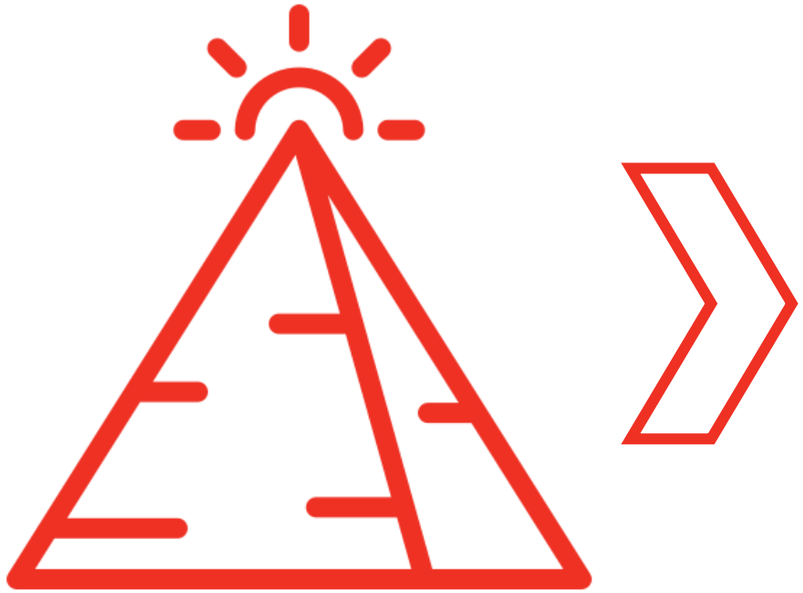
Финансовая пирамида

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.



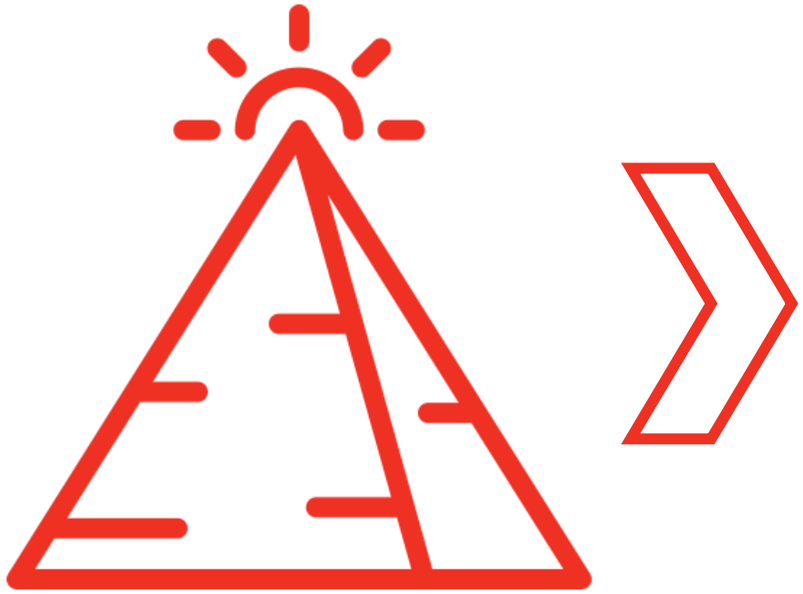
Финансовая пирамида – схема инвестиционного мошенничества, в которой доход по привлеченным денежным средствам образуется не за счет вложения их в прибыльные активы, а за счет поступления денежных средств от привлечения новых инвесторов.

Признаки пирамиды



- 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.

Признаки пирамиды



- Призыв не раздумывать и вкладывать быстро
- Обещание сверхвысокой доходности больше 20% годовых
- Объяснение такой доходности непрозрачными сверхприбыльными проектами
- Обещание вознаграждения за приведенных клиентов
- Анонимность организаторов и отсутствие защиты прав вкладчика в договоре
- Отсутствие информации о возможны рисках
- Требование , например, оплатить «вступительный взнос», «обучение», «участие в семинаре»
- Отсутствие лицензии/ указание номера чужой лицензии, или собственной, но не позволяющей работать с денежными средствами

Чтобы не стать жертвой пирамиды

Во-первых

не поддавайтесь на агрессивную рекламу «легких и быстрых денег», гарантированная доходность выше ставки банковского депозита – повод задуматься о целесообразности таких вложений.

Во-вторых

обратите внимание на следующие признаки, которые могут характеризовать организацию как «финансовую пирамиду»:
Вам объясняют высокую доходность непрозрачными сверхприбыльными проектами, при этом не раскрывают информацию о потенциальных рисках. Проекты, как правило, находятся в другой стране, что затрудняет выяснение текущего положения дел.
Организаторы скрывают информацию о себе, о наличии лицензий на ведение соответствующей деятельности и действуют через посредников. Часто компания зарегистрирована не в России.
Вам обещают высокое вознаграждения за приведенных друзей, знакомых или родственников. Предлагают построить систему привлечения клиентов и зарабатывать на ней. Агрессивно рекламируют свои услуги

В-третьих

старайтесь принимать взвешенные финансовые решения, не поддавайтесь эмоциям, повышайте свои знания в области финансовой грамотности.

Что делать?

Перед тем, как отдать деньги:

- Проверьте наличие лицензии Центрального банка на ведение деятельности (банковская, страховая, инвестиционная).
- Внимательно изучите договор на предмет условий инвестирования и возврата средств.
- Найдите в Интернете информацию о данной организации, ее историю, отзывы клиентов, рейтинги в соответствующей отрасли.

Финансовая пирамида

! Если деньги уже вложены в сомнительные проекты, постарайтесь максимально оперативно изъять не только полученную прибыль, но и основные вложения. Не ждите, когда пирамида развалится, и не старайтесь компенсировать убытки, вкладывая новые средства.

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.

Альфа-Банк

Уважаемые сотрудники,
Для Вас специальное предложение по зарплатному проекту от Альфа-Банка

Зарплатная карта «Альфа-Карта МИР»

0 ₽

- Обслуживание карты
- SMS-уведомления
- Перевод в рублях в другой банк по номеру телефона
- Снятие наличных в банкомате любого банка без комиссии
- Перевыпуск карты по любой причине
- Оплата коммунальных услуг, мобильной связи, штрафов ГИБДД, налогов, ЖКХ

до 2%
кэшбэк от Альфа-Банка за все покупки реальными деньгами, а не бонусами

до 33%
кэшбэк от платежной системы МИР за покупки в магазинах партнёров с privetmir.ru

Для выпуска зарплатной карты и присоединения к зарплатному проекту необходимо обратиться к нашему сотруднику!

По вопросам присоединения к зарплатному обращаться обращаться:
Ильченко Александр Андреевич, менеджер по развитию зарплатного проекта в Альфа-Банке
Тел: +7 (968) 196 34 58, +7 (812) 329 80 50 доб. 012 7523
Эл.адрес: Aailchenko@alfabank.ru