СТРАТЕГИЯ ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ
В РОССИЙСКОЙ ФЕДЕРАЦИИ НА 2017-2023 ГОДЫ

ФИНАНСОВОЕ КОНСУЛЬТИРОВАНИЕ

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность банковских карт и средств на банковских счетах.

400 лет назад Швеция была первой страной в Европе, где стали печататься бумажные деньги. Эта страна может оказаться первой в мире, отказавшейся от наличного оборота. Государственный Банк Швеции рассматривает возможность перехода страны на электронные деньги, а хождение бумажных денег может быть полностью запрещено после 2030 года.

Уже сегодня к массовому клиенту пришел совершенно новый цифровой финансовый мир со своими цифровыми валютами и активами, в котором, как и сто, и тысячу лет назад, исчезают физические деньги в прямом и переносном смысле. История неумолима.

Охота за деньгами, кошельками, счётами и активами людей, а теперь цифровыми рублями, цифровым финансовыми активами и криптовалютами со стороны мошенников продолжится в обозримой перспективе. Мошенники прекрасно используют достижения прогресса для актуализации преступных схем и легенд, а иногда снижая себестоимость мошеннического бизнеса.

Да, прогресс активно используется мошенниками, поэтому ассортимент инструментов: интернет, компьютеры и смартфоны, очевидно, расширится.

Страх и интерес людей перед безналичной и цифровой формой денег абсолютно реальный. Все новое и не понятное пугает и привлекает людей. **В 2022 году зафиксирован рост количества киберпреступлений на 45%.** Эти рекордные цифры зафиксированы Банком России. Всего киберпреступлений **в 2022 году выявлено около 500 000**.

Интернет и онлайн-платежные сервисы обеспечивают для населения земного шара доступность широчайшего перечня финансовых услуг. В российском интернете около 300 тысяч сайтов. Среди которых есть мертвые, фейковые, и в меньшинстве, настоящие сайты. **Как среди плохих сайтов выбрать добропорядочный?** Это не простой выбор, но важный.

Признаки фейкового сайта:

1) Вам сразу хотят сделать очень много добра: необычайно высокие скидки, космический кэшбэк, дорогие «подарки» и прочие сказочные бонусы.

2) Адреса интернет ресурсов напоминают известные сайты, но имеется искажение в фейковом адресе по сравнению с настоящим.

3) Косвенный признак — повышенное количество ошибок в текстах, а также вероятны неработающие ссылки.

Лайфхак: В интернет-магазинах важен не столько средний рейтинг, сколько количество отзывов, которые не должны быть однотипными, исключительно восторженными и написанными примерно в один и тот же период времени. Иногда лучше купить товар в магазине по более высокой цене у известного продавца и избежать демпинговых предложений неизвестных проходимцев.

Социальная инженерия — совсем не ругательное слово. Хотя термин в последнее время получил яркую негативную оценку. Родоначальник термина социальной инженерии Карл Поппер. **Социальная инженерия** — это управление политическими и общественными процессами на основе научных знаний при использовании механизмов обратной связи с обществом. В целом ничего плохого. Однако мошенники научились взламывать защиту людей благодаря различным методам манипуляции с их эмоциональным поведением.

Легенд развода с помощью социальной инженерии множество, но суть манипулирования одна. **Создать стрессовое состояние жертвы, чтобы заблокировать логические функции мозга**. В такие моменты люди склонны принимают иррациональные решения. **Самые мощные манипуляции — это манипуляции на чувстве страха и воодушевления**. Вас огорошивают до дрожи или восхваляют до небес.

Психологическое **манипулирование происходит по четкому сценарию:**

1. неожиданно появляется новая проблема для потенциальной жертвы;

2. информация адресована именно жертве;

3. мошенник о вас что-то знает, и это повышает уровень вашего доверия;

4. потом резко создаётся стрессовое состояние. Уровень опасности должен быть намного выше обычного;

5. предлагается быстрый рецепт решения проблемы;

6. жертва получает знаки одобрения, если следует в нужном направлении, и наоборот, если ведёт себя неправильно;

7. жертву подталкивают к быстрым ажиотажным решениям;

8. контакты с другими людьми пресекаются.

В каждом из нас, в большей или в меньшей степени, встроена система критического мышления. Она включится сразу, как только у вас будет достаточно времени. **Ваша цель — это время получить.** Надо остановить ажиотаж и стремительное развитие криминального сценария. У всех людей есть **3 функции врожденной защиты**:

- Эмоциональная — боязнь всего не известного.
- Рациональная — кругом мошенники и доверять никому нельзя.
- Социальная — возможность общения с другими людьми и коллективный разум. Убедить одного человека намного легче, чем группу людей.

Манипуляции, основанные на страхе и счастье, прекрасно работают с любым типом людей. Схема работы мошенника обычно не изменяется. Жертве сообщают о якобы краже ее денег, утрате близких или измене родине. Или сообщается о огромном выигрыше, компенсации от государства, сказочном наследстве.

Например, **мошенническая схема нигерийского письма**. Обычно это просьба от незнакомца из далекой страны помочь в получении огромной суммы денег. Платить ничего не надо, достаточно только предоставить свой банковский счет. История разыгрывается поэтапно. В какой-то момент для зачисления нескольких миллионов долларов на ваш счет понадобится заплатить. Бывали случаи, когда манипуляции длились годами и задействовалось целое преступное сообщество. Использование

в мошеннических звонках криминального коллцентра уже стало почти нормой для качественного развода.

Лайфхак: при совершении мошеннического звонка используется посторонний шум (фоновый шум работы коллцентра, разговоры и звонки телефонов). Этот шум мешает жертве сконцентрироваться на разговоре с жуликом, и она быстрее вовлекается в манипуляцию.

По данным опросов Национального института финансовых исследований (НАФИ), почти **80% россиян осведомлены о рисках пользования банковскими картами в связи с мошенничеством**. Источником информации о карточных рисках, как правило, выступают СМИ и социальные сети. Сама по себе информированность населения об опасностях способствует более осторожному, внимательному отношению к картам. Однако излишне красочная, утрированная подача новостей на карточные темы формируют в обществе чрезмерные страхи.

В 2022 году количество операций по картам без согласия клиентов **уменьшилось на 15% и достигло 877 тысяч операций**, а объём операций, наоборот, увеличился и достиг рекордной суммы — более 14 миллиардов рублей. В свою очередь, **банки вернули клиентам всего около 4,4% средств**. Возврат денег от банков снизился почти в 2 раза. Так ка в 2021 году банки вернули около 7%.

Методы злоумышленников — это хорошо знакомые нам приемы социальной инженерии. Люди, благодаря психологическому воздействию, добровольно переводят деньги злодеям. Средний чек операции без согласия физических лиц — **около 15 тысяч рублей.**

Почему у людей массово складывается впечатление, что карты опаснее наличных? Полагаем, что основных причин три:

1) СМИ, блоггеры очень часто говорят о случаях карточного мошенничества и значительно реже — о повседневном, уличном и домашнем воровстве. Это объяснимо, поскольку, в отличие от «уличной» преступности, которая мало изменилась со времен Древнего Рима, карточные мошенники меняют свои «технологии» и эволюционируют в постоянном режиме. Во многом их к технологическому развитию

подталкивают банки, которые также развивают системы защиты карточных расчетов.

2) Потери по банковским картам в некоторых случаях оказываются очень большими. Связано это с тем, что если преступнику становятся известны ваши персональные данные и контрольная информация карточного счета, то в зоне опасности могут оказаться все средства на ваших счетах, а иногда и кредитный лимит, предоставленный банком.

3) Сильное впечатление на граждан производят случаи массовой дискредитации банковских карт, когда преступники одномоментно получают доступ к сотням тысяч, а иногда и миллионам счетов физических лиц. Подобные громкие случаи мошенничества практически никогда не влекут финансовых потерь клиентов, поскольку являются очевидными проколами работы в безопасности банков. Однако это катастрофически подрывает доверие населения к электронным карточным расчетам.

Вероятность реальной потери денежных средств при соблюдении самых простых правил финансовой безопасности значительно меньше. Единственным неудобством оказывается необходимость блокирования карты и ее перевыпуск.

Основные виды мошенничества с банковскими картами:

1. Воровство карт. Как правило, карты воруют вместе с кошельками. Попытки использовать обнаруженные в кошельках карты довольно редки, поскольку в большинстве случаев владелец карты блокирует ее сразу после обнаружения пропажи.

Есть целенаправленное воровство карт, как правило, вблизи банкоматов. Карта уличному воришке интересна тогда, когда он знает ее ПИН-код. Код он может подсмотреть у банкомата. Или установить миниатюрную видеокамеру и отследить, какой номер вы набираете. Поэтому прикрывайте рукой цифры, когда набираете пин-код в банкомате.

2. Фальшивые терминалы. Установка в многолюдных местах «банкоматов», «платежных терминалов» используется мошенниками для того, чтобы получить информацию о банковской карте, включая пин-код. Правда, это большая редкость в наше время.

3. Скимминг — установка на банкоматы специальных устройств, позволяющих скопировать информацию с карты. Как правило, устанавливается специальная накладка на картоприемник или клавиатуру для фиксации пин-кода, который вводит владелец карты.

Скимминг в последние годы теряет свою популярность, что связано с массовым внедрением карт с микропроцессором (чипом). Наличие чужеродных устройств на банкоматах можно обнаружить визуально. Обычно их просто приклеивают. Если видите на картоприемнике следы клея, то лучше воздержаться от пользования этим банкоматом. И об этом нужно сообщить сотрудникам банка.

4. «Ливанская петля». Мошенники устанавливают в картоприемник кусок пластика или пленки, который позволяет карте свободно войти в банкомат, но не пускает ее обратно. Банкомат «отказывается» отдавать карту владельцу. В этот момент появляется

«добрый помощник», который посоветует еще раз ввести ПИН-код, ведь он якобы «вчера попал в точно такую же ситуацию, и это помогло». После безуспешных попыток жертвы «помощник» рекомендует срочно обратиться в банк и непременно написать заявление. В течение 10-15 минут после того, как расстроенный человек пойдет в банк, счет его будет обнулен в соседнем банкомате. Так ка мошенник не только завладел картой, но и узнал ее пин-код.

При возникновении проблем с банкоматом не покидайте его до момента, пока вы не проинформируете по телефону о случившемся службу поддержки. Телефоны технической поддержки должны быть у каждого терминального устройства. И, конечно, не набирайте пин-код перед незнакомыми людьми.

5. Фишинг — выуживание контрольной информации и персональных данных владельца карты. Мошенничество, связанное с получением персональных данных и контрольной информации по счетам от самих владельцев карт. Этот вид мошенничества стал массово распространяться именно сейчас, поскольку для дистанционных операций через интернет сама карта теперь уже не нужна.

В подавляющем большинстве случаев потери денег с платежных карт являются следствием мошеннических рассылок и особенно звонков. Люди сами передают мошенникам реквизиты карт или переводят преступникам деньги. Основная проблема опять — «социальная инженерия».

В 2022 году Банк России заблокировал более пол миллиона мобильных телефонных номеров. И ещё четверть миллиона городских стационарных телефонных номера.

Стандартная схема мошенничества выглядит примерно так.

- Все начинается со звонка с неизвестного номера.
- **Жертву сразу пытаются «огорошить»:** «за вами числится большой долг»; «ваш перевод на миллион долларов с Островов Кука пришлось заблокировать»; «транзакция террористической организации» т.п.). Чем нелепее выглядит обвинение, тем оно

оказывается более действенным. **Цель — возбудить желание тут же «оправдаться» по абсурдным претензиям.**

- Владелец карты готов выложить всю контрольную информацию по карте. Давление ослабевает при получении мошенниками контрольной информации. И в конце потребителя успокаивают, что все нормально, что, по всей видимости, произошла «техническая ошибка», которая в самое ближайшее время будет исправлена.
- Человек расслабляется, считает, что очень удачно решил неожиданную проблему, а вскоре получает сообщение о том, что с его счета списана крупная сумма.
- **Выигрыш призов.** Это разновидность фишинга, но вместо шокирующего сообщения **человек получает «радостное»** — он выиграл в лотерею приз (как правило, денежный). Но для того, чтобы перевести деньги на карту, организаторы игры **уточняют реквизиты счетов, персональные данные, а под конец и контрольную информацию счастливого победителя**. Итог — исчезновение денег со счета.

6. Мошенничество с картами в точках продажи товаров и услуг. В первую очередь речь идет о копировании данных при приеме карт в ресторанах и других точках продажи услуг.

Одной из самых проблемных зон в плане безопасности карточных расчетов были и в определенной степени остаются рестораны, где при оплате заказа официант уносил карту. За время, которое карта находится вне контроля владельца, с нее можно скопировать всю информацию, включая ту, которая записана на магнитной полосе. Но без оборудования официант может сфотографировать или просто переписать всю буквенную и цифровую информацию с карты, что позволит ему оплачивать с вашего счета покупки на многих интернет-сайтах.

Но иногда (в нашей стране достаточно редко) применяются специальные терминалы, которые позволяют мошенникам просканировать всю информацию, нанесенную на карту. Если вам предлагают воспользоваться терминалом, в который карта погружается почти полностью, рекомендуем отказаться от транзакции.

При неожиданной пропаже денег с карточного счета, независимо от причин списания, **порядок действий владельца карты должен быть единым, и он определяется в Федеральном законе «О национальной платежной системе».**

1) Банк обязан проинформировать владельца карты обо всех совершенных по счету операциях (как, правило, применяется СМС-оповещение).

2) Если банк не проинформирует клиента о транзакции, то он будет «обязан возместить клиенту сумму операции, о которой клиент не был проинформирован и которая была совершена без согласия клиента».

3) Клиент, получив сообщение о «неправильной» или несанкционированной им операции, должен незамедлительно сообщить об этом в банк («не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции»).

4) Закон также требует сообщить в банк о потере, пропаже карты.

5) Если клиент сообщил в указанные сроки о том, что списание денег было инициировано не им, то банк «**обязан возместить сумму операции**, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа,

что повлекло совершение операции без согласия клиента-физического лица».

6) Если клиент не сообщает банку о том, что операция не была им санкционирована, то банк «**не обязан возместить клиенту сумму операции,** совершенной без согласия клиента».

Следует также иметь ввиду, что существует **процедура возврата платежей (ошибочных, мошеннических) Chargeback в самих платежных системах**. Не всегда она работает, но попытаться ею воспользоваться при возникновении проблем необходимо.

Массовый переход на дистанционное банковское обслуживание мошенники используют в своих интересах, пытаясь вторгнуться во взаимодействие клиента и банка, перенаправив денежные средства в свою сторону.

В системах дистанционного банковского облуживания есть две стороны — банк и клиент. Сегодня мошенники сосредоточились на клиенте. Именно мы являемся слабым звеном во взаимодействии Клиент-Банк, и, к сожалению, чаще всего из-за нашей собственной беспечности.

Основные способы проникновения мошенников в системы интернет и мобильного банкинга — это:

- вирусное программное обеспечение на компьютеры или гаджеты клиента;
- использование потерянных или украденных средств мобильной связи;
- фишинг — выведывание у человека конфиденциальной, контрольной информации, необходимой для вторжения на ваш счет.

На 99% избавить себя от мошеннических звонков можно через соответствующий **сервис вашего Банка по блокированию мошеннических звонков**. Однако эта услуга, как правило, платная.

Защитить себя, сохранить душевное равновесие, и свои деньги можно соблюдая простые **правила финансовой гигиены**.

- Не пользуйтесь ссылками, полученными с неизвестных адресов, а также из «неожиданных» посланий от знакомых.
- Внимательно проверять адреса сайтов.
- Не пользуйтесь мобильным банком в общественных местах.
- При пользовании мобильным банком закрывайте другие приложения на смартфоне.
- Не записывайте пароли для входа в мобильный банк на том же устройстве, через какое вы в него входите.
- Антивирусные программы должны быть свежих версий.

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ