Брифинг «Финансовое мошенничество. Как себя обезопасить»

1. Откуда у мошенников мои данные?

Мошенники получают персональные данные человека с помощью фишинговых сайтов и информационных баз, которые попали в интернет. Они могут знать ваши фамилию, имя и отчество, телефон, адрес, в каких банках у вас открыты счета и их баланс.

Мошенники используют и ту информацию, которую люди сами выкладывают в интернет. Чтобы уменьшить свои шансы на встречу с мошенником, не публикуйте в открытом доступе, в том числе в социальных сетях и мессенджерах, номер телефона, электронный адрес и другие персональные данные, старайтесь избегать публикации фотографий банковских карт. Этой информации недостаточно, чтобы сразу украсть деньги, но хватит для того, чтобы начать общение и усыпить бдительность.

2. Какие виды финансового мошенничества существуют?

Существует большое количество видов финансового мошенничества. К наиболее распространенным сейчас видам относятся:

- телефонные звонки и СМС от мошенников;
- фишинг;
- мошенничество при продаже и покупке через интернет;
- нелегальное кредитование и финансовые пирамиды.

3. Как распознать мошенника?

Несмотря на то что мошеннических схем очень много, распознать мошенника можно по нескольким признакам:

- на вас вышли сами (вам могут позвонить, прислать СМС, электронное письмо или сообщение с сомнительной ссылкой в социальной сети или мессенджере, в том числе от имени вашего знакомого);
- с вами говорят о деньгах (как о подозрительных операциях по вашей карте, так и о внезапном выигрыше, возможности получить компенсацию от государства или вложить деньги в высокодоходный инструмент);
- вас просят сообщить какие-либо данные (номер карты, срок ее действия и баланс, код безопасности (три цифры на обратной стороне карты), код из СМС или пуш-уведомлений, ПИН-код, логин и пароль от банковского приложения, какие карты и вклады у вас открыты, когда вы пользовались онлайн-банком последний раз);
- вас выводят из равновесия: пугают, торопят, не дают права выбора, давят на жалость или на жадность, чтобы у вас не было возможности принять взвешенное решение в спокойной обстановке и чтобы вы действовали импульсивно.
- вам предлагают вложения с высокой доходностью, займы по невероятно низким ставкам и другие, якобы выгодные условия.

Пример 1. Вам звонят из «службы безопасности банка» и сообщают, что по вашей карте прямо сейчас проводится подозрительная операция. Вам предлагают срочно назвать трехзначный код, указанный на обратной стороне карты, чтобы отменить транзакцию, или перевести деньги на якобы безопасный счет.

Пример 2. Вам приходит СМС от банка с текстом: «С вашей карты списаны деньги. Для отмены транзакции позвоните по указанному номеру».

Пример 3. Вам приходит электронное письмо, в котором вам сообщают, что вам положена социальная выплата. Чтобы ее получить, нужно перейти по ссылке и ввести свои данные.

Мошенник может представиться сотрудником какой-либо организации, например банка, государственных или правоохранительных органов, техподдержки, знакомым семьи. Он может подделать идентификатор вызывающего абонента, сайт организации или аккаунт известного вам человека, чтобы не вызвать у вас подозрений. Под каким бы предлогом ни обращались к вам мошенники, всем им нужно одно — ваши деньги.

4. Как реагировать на подозрительный звонок или сообщение?

Возьмите паузу. Если вы получили тревожный звонок или сообщение, главное — не реагируйте сразу. Если речь о деньгах, а вас торопят — это под озрительно.

Если вам звонят, выберите любой удобный повод, который якобы меша ет вам продолжить разговор, например вам нужно закрыть дверь или найти н аушники, потому что вы плохо слышите собеседника. Это даст вам время и н е отпугнет собеседника, если он не мошенник.

Если вам пришло сообщение о неожиданном списании средств, не звон ите по указанному в сообщении телефону и не переходите по ссылке. Обрати тесь в банк по телефону (номер горячей линии указан на обратной стороне ка рты) или через официальное мобильное приложение.

Проанализируйте информацию. Если с вами связались сами, говорят о деньгах, пытаются вывести из равновесия (торопят, пугают, давят на жалос ть или жадность) и просят сообщить конфиденциальные данные, скорее всег о, это мошенники.

Запомните, никому нельзя сообщать:

- срок действия карты;
- код безопасности на обратной стороне (три цифры);
- код из СМС и пуш-уведомлений;
- ПИН-код;
- сколько денег на вашем счете.

Настоящий сотрудник банка и службы безопасности знает ваши фамилию, имя и отчество, последние четыре цифры вашей карты, сколько денег на вашем счете. Он не попросит снять деньги в банкомате, перевести их на другой счет или сообщить данные карты кому-то еще.

В некоторых банках деньги можно обналичить через QR-код, созданный в мобильном приложении. Мошенники, под предлогом отмены операции, просят сгенерировать такой код и переслать им в один из мессенджеров. После этого ваши деньги снимают в банкомате.

Когда банк замечает сомнительный платеж или перевод с вашего счета, с вами могут связаться, только чтобы подтвердить или отклонить операцию. Конфиденциальные данные для этого не нужны. Если о них спрашивают — вас пытаются обмануть.

Вешайте трубку. Если вы пришли к выводу, что общаетесь с мошенником, сразу вешайте трубку. После этого позвоните в банк или другую организацию, сотрудником которой представился мошенник, и расскажите о ситуации. Так вы поможете организации усилить меры безопасности и узнаете, все ли в порядке с вашим счетом.

Установите на телефон определитель номера. Он распознает подозрительные звонки, и вы снизите вероятность общения с мошенниками.

5. Что такое фишинг и как от него защититься?

Фишинг — это вид интернет-мошенничества, который используется для кражи конфиденциальных данных человека. Для этого злоумышленники рассылают сообщения с вредоносными ссылками. По ссылке вас может ждать вирус, троянская программа, фишинговый сайт, с помощью которых мошенники украдут ваши логин и пароль, реквизиты банковской карты, информацию об устройстве и другие личные данные.

Мошенники могут прислать фишинговую ссылку:

- в сообщении в социальных сетях или мессенджере от имени незнакомого человека или знакомого, взломав его аккаунт;
- в электронном письме от имени якобы реального интернет-магазина, банка, государственного учреждения или другой организации. В письме вам могут предложить подтвердить аккаунт, чтобы воспользоваться бонусами, сообщить о полагающейся вам социальной выплате или одобренном кредите. Перейдя по ссылке, вы попадете на поддельный сайт, интерфейс и адрес которого будут максимально похожи на настоящие;
- в электронном письме от имени вымышленных организаций. Часто в таких письмах обещают деньги. Вам могут сообщить о положенной компенсации или выигрыше в лотерею, предложить вложить деньги в высокодоходный инструмент и заработать много денег за 10 минут. Только, чтобы получить деньги, вам нужно сначала перейти по ссылке и заплатить самим, например оплатить доставку, комиссию за выигрыш, взнос или налог на подарок. Если, чтобы получить деньги, вам нужно заплатить — это мошенничество.

Обычно злоумышленники формулируют тему письма так, что на него хочется отреагировать, например: «Ваш аккаунт заблокирован», «Срочное сообщение от банка», «Привет! Отправляю обещанные фотографии».

Еще один вариант мошенничества с вредоносными ссылками — поддельные QR-коды. Их могут размещать:

- на упаковке и этикетках товаров;
- в электронных письмах, бумажных объявлениях, на рекламных баннерах;
- на поддельных квитанциях от имени государственных учреждений и официальных организаций, например управляющих компаний.

Чтобы защититься от фишинга:

- не открывайте сомнительные письма о крупных выигрышах, легких викторинах, лотереях и одобренных кредитах;
- не загружайте вложенные файлы из сообщений, которых вы не ожидали;
- не переходите по ссылкам от незнакомых людей, а если ссылку прислал человек, которого вы знаете, позвоните ему и убедитесь, что это он отправил вам сообщение;
- если пришло письмо о том, что вам положена какая-то выплата, возьмите паузу и проверьте информацию в официальных источниках;
- внимательно проверяйте адресную строку сайта, на котором просят ввести ваши данные, — название поддельного сайта может отличаться от настоящего на один-два символа;
- не вводите свои персональные данные и данные вашей банковской карты на сомнительных сайтах;
- всегда проверяйте электронный адрес, с которого пришло письмо. Если он отличается от известного вам адреса магазина, банка или другой организации хотя бы одним символом, не открывайте письмо. Если адрес вам не знаком и вы не ждете сообщений от новых адресатов, письмо лучше удалить;
- помните, что ошибки и плохой дизайн — это признаки поддельного письма, но будьте внимательны, даже если все выглядит идеально;
- следите, чтобы QR-код был напечатан вместе с этикеткой или упаковкой. Если на месте оригинального кода приклеен другой, не сканируйте такой QR-код и сообщите о нем сотруднику магазина;
- при оплате с помощью QR-кода проверяйте, правильно ли указаны реквизиты организации, сумма, которую нужно оплатить, и другие данные в документе и на странице, открывшейся после сканирования кода. Если данные не совпадают, обратитесь в

организацию, которая прислала документ, чтобы подтвердить его подлинность.

Проверить безопасность сайта можно с помощью сервисов «Яндекс» и Google, а

финансовую организацию — на сайте Центрального банка Российской Федерации.

6. Как продавать и покупать через интернет?

Если вы продаете или покупаете что-либо в интернете, важно знать о распространенных мошеннических схемах в этой сфере.

Мошенники могут:

- предлагать дорогой товар, который пользуется повышенным спросом, по более низкой цене. Например, средняя рыночная стоимость новой модели телефона — 30 000 рублей. Вы нашли сайт, на котором он стоит 10 000 рублей, при этом предыдущая модель этого телефона у продавца стоит столько же. Скорее всего, после оплаты товара продавец исчезнет;
- присылать сообщение с поддельной ссылкой для оплаты. Например, вашим объявлением о продаже заинтересовался покупатель. Он говорит, что готов купить ваш товар, отвлекает внимание вопросами о нем и отправляет вам ссылку, по которой вы должны пройти и ввести данные своей карты, чтобы он смог сразу оплатить покупку. Если вы введете данные карты, он спишет с нее деньги. Поддельную ссылку для оплаты может отправить и продавец, попросив вас внести предоплату. Когда вы введете данные карты, мошенник спишет с нее больше, чем должен был.

Чтобы не стать жертвой мошенника:

- оформите виртуальную карту для покупок в интернете и установите по ней лимит, например 100 рублей в месяц, — в таком случае снять с нее больше не получится. Перед покупкой можно вручную увеличить лимит на нужную сумму, а потом снова уменьшить. Также можно оформить отдельную карту и счет для онлайн-покупок и пополнять их перед оплатой;
- общайтесь с продавцами и покупателями только на том сайте, где продается товар, не переходите в другие мессенджеры;
- попросите у продавца, если он просит предоплату, номер карты и отправьте предоплату по номеру карты. Внимательно проверяйте реквизиты получателя денежных средств. Помните: внося предоплату, вы действуете на свой страх и риск;
- пользуйтесь доставкой с оплатой при получении;
- внимательно проверяйте ссылки для оплаты;

- не отдавайте товар раньше, чем вам его оплатили, или воспользуйтесь специальной услугой доставки интернет-сервисов;
- не открывайте сомнительные ссылки;
- в случае каких-либо подозрений обращайтесь в службу поддержки сайта.

7. Как уберечься от нелегальных финансовых организаций и финансовых пирамид?

Вклады и финансовые услуги. Если вам от лица компании предлагают финансовые услуги, проверьте есть ли у этой компании лицензия либо другая информация в справочнике финансовых организаций Центробанка России. Если лицензии нет, и компания не состоит в реестре, скорее всего, она работает нелегально. Велик риск потерять деньги. Если вы планируете купить финансовую услугу или доверить свои деньги какой-либо организации, проверьте ее в списке компаний с признаками нелегальной деятельности.

Кредиты и займы. Нелегальный кредитор — компания, индивидуальный предприниматель (ИП), физическое лицо или интернет-проект, выдающий потребительские займы, не обладающий законным на то правом. Нелегальный кредитор:

- собирает различные комиссии, предоплаты за кредит/заем, вознаграждения за проверку кредитной истории или страховку. Выставляет необоснованные штрафы. Получив деньги, компания может исчезнуть;
- подделывает или подменяет документы, препятствует оплате долга. В результате клиент может потерять залоговое имущество;
- запугивает должников;
- не выполняет условий договоров, заявленных в рекламе и обещаниях представителей компании;
- оформляет займы с использованием других видов договоров (купли-продажи, хранения, комиссии и прочих).

Обратите внимание: выдавать кредиты и займы могут только кредитные организации и микрофинансовые институты, и всегда только на основании лицензии Банка России. Все микрофинансовые организации, кредитные и сельскохозяйственные потребительские кооперативы, жилищно-накопительные кооперативы и ломбарды включены в реестр.

Биржевые схемы. Нелегальный профессиональный участник рынка ценных бумаг (в том числе нелегальный форекс-дилер) — компания, предоставляющая без лицензии Банка России брокерские, дилерские и другие финансовые услуги. Основные признаки мошеннических схем, когда вам:

- предлагают услуги на рынке Форекс, включая торги криптовалютой;

- настойчиво рекомендуют срочно увеличить сумму вложений на торговом счете, при отсутствии средств подталкивают на оформление кредита для пополнения торгового счета, например, чтобы отыграть потери;
- предлагают помочь с покупкой высокодоходных ценных бумаг через ответы на заявки, оставленные на сайте, телефонные звонки, сообщения в мессенджерах;
- привлекают под видом трудоустройства, обязательное условие — пройти обучение и начать торговать;
- предлагают зачислить деньги в «личный кабинет» через перевод на карту физического лица;
- обнуляют счет в личном кабинете, ссылаясь на рыночную конъюнктуру.

Нелегалы уверяют, что имеют лицензию зарубежного регулятора, но часто это невозможно проверить. А при появлении проблем, решать их придется в иностранной юрисдикции, по «месту прописки» компании.

Финансовая пирамида — это схема по привлечению денег граждан, при которой «прибыль» от вложенных средств выплачивается за счет новых участников. Вам обещают сверхвысокую доходность вложений, но часто для участия требуется первоначальный взнос. Пирамиды ведут агрессивные рекламные кампании, используя современные технологии и популярные темы — криптовалюта, кешбэк за покупки. Одни маскируются под экономические игры, другие действуют исключительно в мессенджере Телеграм, не имея собственных сайтов. Еще один признак пирамиды — анонимность. Невозможно найти конкретной информации о руководителе проекта, а также сведений о финансовом положении организации.

Подробнее о том, как защититься от финансовых мошенников, читайте на портале «Открытый бюджет города Москвы», а также в материалах «Финансовой культуры» (проект Центробанка России) о рисках торговли на Форекс, о том, как не стать жертвой нелегальных кредиторов, о финансовых пирамидах, о том, что делать, если вы стали их жертвой, и о многом другом.

8. Что еще можно сделать, чтобы защититься от мошенничества в интернете?

Чтобы защититься от мошенничества в интернете:

- создавайте сложные пароли, храните их в недоступном месте и регулярно меняйте. О том, как придумать сложный пароль, можно узнать из нашей инструкции;
- сравнивайте реквизиты операции и сумму оплаты, полученные в СМС или пуш-уведомлениях банка с информацией на сайте, где происходит оплата. Если данные не совпадают, не вводите пароль;

- никогда не вводите пароли для отмены операции — об этом могут просить только мошенники. Если вы с этим столкнулись, покиньте сайт и срочно обратитесь в банк по телефону горячей линии или через официальное мобильное приложение;
- пользуйтесь защищенным соединением: адресная строка должна начинаться с префикса https://. Помните, что официальные сайты финансовых организаций в поисковых системах («Яндекс», Mail.ru) отмечены цветным кружком с галочкой;
- используйте на мобильном телефоне мобильное приложение банка вместо его веб-версии;
- держите на обычном счете немного денег и в случае необходимости переводите на него нужную сумму с накопительного счета, не привязанного к карте и основному счету, — с него деньги украсть сложнее;
- защитите свои устройства, установите и регулярно обновляйте антивирусную программу.

9. Что делать, если я стал жертвой мошенников?

Если вы стали жертвой мошенников, немедленно обратитесь в банк по телефону (номер горячей линии банка указан на обратной стороне карты) или через официальное мобильное приложение и заблокируйте карту.

Не позднее дня, следующего за днем поступления информации о совершении подозрительной операции, подайте в банк заявление о несогласии с операцией. Банк проверит, сообщали ли вы ПИН-код, код безопасности или срок действия карты посторонним. Если вы нарушили правила безопасности, банк не компенсирует потери.

Подайте заявление в полицию. Чем быстрее вы это сделаете, тем выше вероятность того, что преступников найдут и привлекут к ответственности, поэтому выберите самый быстрый в вашем случае способ.

Вы можете подать заявление:

- по телефону 102 или 112;
- с помощью специальной формы на официальном сайте МВД России (обращение нужно отправить в управление «К» МВД России);
- в ближайшем отделении полиции по месту жительства.
-