Запомните!

Правила сбережения денег



Чтобы обезопасить себя от мошенников, необходимо помнить о следующих основных правилах.

– сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;

– избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;

– внимательно читайте смс от банка;

– никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в смс;

– помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в смс от банка;

– сотрудники банка никогда не попросят вас пройти к банкомату;

– не покупайте в интернет-магазинах товар по явно заниженной стоимости, так как это мошенники;

– никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно, мошенники взломали аккаунт. Сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– в сети интернет не переходите по ссылкам на неизвестные сайты;

– действуйте обдуманно, неторопливо, помните, что «Бесплатный сыр бывает только в мышеловке».

Поделитесь этой информацией с родными и близкими!

Пенсионеры тоже бывают разными

На заметку. Недоверчивость и осторожность – лучшие друзья пожилых людей при подозрительных звонках

Две реальные истории про мошенников и их жертв. Две разные схемы обмана, но обе неудачные для жуликов, потому что две женщины одинаково почтенного возраста смогли вовремя остановиться и не попасться на развод.





Жадность чуть не подвела

Моя мама чуть не попалась на обман мошенников. Хотя казалось, что все звонящие «операторы», «менеджеры», «следователи», благодаря нашим бесконечным напоминаниям, ей не страшны. Слушала, внимала, головой кивала…

А здесь звонок из банка, где у неё находится вклад. Небольшой, 300 тысяч под 18%. Можно и больше открыть безо всяких звонков, до 20%. Но там условия её не устраивают, без снятия и пополнения она не хочет. Вдруг деньги понадобятся.

Звонящий ей обещает 22% со снятием и пополнением, с ежедневным начислением, а «если откроете прямо сейчас, то еще 5% в плюс на 3 месяца». 27% – это ничего себе, знаете ли! Почти +10% к текущей ставке. Вот у мамы осторожность и выключилась. Ведь в том же банке, где вклад. Какие риски?

Она говорит, что сейчас же пойдёт и откроет в приложении сама. Но не тут-то было! Мошенники говорят, мол, сейчас вам ссылка придёт. Это оферта на открытие счёта. Индивидуальная и только для вас, как для нашего клиента. Диктуют маме: сперва выведите деньги с имеющегося вклада на любую карту. Открывайте ссылку, там вводите сумму нового вклада, можете даже добавить, если есть на карте и далее следуйте инструкциям. Всё защищено, ничего сообщать не надо, никому и никогда. По оформлению можете спрашивать.

Мама заходит в приложение, закрывает вклад, выводит деньги на карту. Открывает ссылку, там 100% на вид сайт банка, с её данными ФИО и датой рождения (!!!), вводит сумму вклада и переходит к оплате. Ставит галочки все, что снятие, пополнение, расчёт в конце каждого месяца по процентам.

Вводит сумму, ей предлагают подтвердить операцию через код и….

Тут ей что-то не понравилось. Приходит СМС типа «Никому не сообщайте, списание суммы в 350 тысяч, какой-то Vklad*банк*. Не может так открытие вклада выглядеть – не было у неё ничего подобного! Занервничала мама, с телефоном в руке прибежала ко мне (живём на одной площадке). Я в ужасе ору в трубку, мошенники после моих матов отключаются. Мы быстрее в банк, снимать деньги с карты. Там нас успокоили, что если ничего не ввели и код не отправляли, то всё хорошо. Заново открыли вклад. Испугались жутко. Ссылка, которая была, конечно, пропала. Уже ничего не открывается, страница недоступна.

У знакомых родственница, увы, эту схему завершила в полной мере под диктовку вежливого менеджера из банка. 64 года женщине. Точно так же убедили, что ничего сообщать не надо, ещё и предупредили, чтобы НИКОМУ не говорила, если вдруг кто-то позвонит вместо них! Какие заботливые…

Дальше все по инструкции. Закрыла вклад имеющийся, перешла по ссылке, её вели по шагам: «Там вводите. Тут ставьте галочку». Пришёл код, она его ввела, получила «радостное сообщение», что «Ваш вклад открыт». Менеджер поздравил, сказал, что вклад отобразится в приложении в течение 10 минут, если буду вопросы – звоните по горячей линии. Естественно, что ничего и нигде не появилось…

Банк радостно сообщил, что она сама всё оплатила, а если стала жертвой мошенников, то органы ей в помощь.

Данные по телефону не разглашаю

Изначально звонящий представился сотрудником Пенсионного фонда и сообщил, что у женщины предпенсионного возраста были обнаружены «потерянные» годы стажа, которые теперь нужно зафиксировать и закрепить. Для этого нужно явиться в Пенсионный фонд и представить документы.

Далее – расшифровка разговора читательницы с мошенником.

Ч: – человек, М: – мошенник.

Ч: Так, в пенсионный фонд, вы говорите, да? Ещё раз повторите, какие документы надо?

М: Паспорт, СНИЛС, ИНН и трудовая книжка. Плюс по одной копии каждого документа.

Ч: И когда надо подъехать?

М: Как вам удобно будет, так и подъезжайте. Я сейчас поставлю вас в электронную очередь на определённую дату и время.

Ч: А там ещё очередь?

М: Естественно, все по записям, по электронной очереди.

Ч: Как срочно это надо сделать?

М: Сделайте лучше и забудьте, потому что в дальнейшем могут быть проблемы с начислением пенсионного коэффициента, да и проблемы с выплатами по пенсии, в принципе могут быть.

Ч: А как это получилось вообще?

М: А я откуда знаю? Может кто-то из ваших бывших работодателей чего-то с ведомостями намудрил, я не знаю.

Ч: А как вы это обнаружили тогда?

М: Может системная какая ошибка была.

Ч: Ну как вы обнаружили, что у меня там недосчитанное?

М: Нам письмо пришло из Минтруда, всё. Вы к нам приезжаете, предоставляете документы, пишите заявление по 106-й форме, и вам делается перерасчёт. То есть в систему добавляются те два года, которые вам не учли. Вам или повышают пенсионный коэффициент, либо делают разовую выплату за те два года.

Ч: Слушайте, мне просто сейчас в ближайшее время вообще никак неудобно. М: Я могу вас через месяц записать.

Ч: Я могу забыть потом.

М: Мы можем просто вам сделать электронный талон через госуслуги, и всё. Приедете по талону, пройдёте, и всё. Это недолгая процедура, в принципе.

Ч: Ну так я так понимаю, что я через госуслуги могу потом сама записаться к вам, правильно я понимаю?

М: Вы можете сделать через госуслуги обычную запись, а на перерасчёт вас не пустят…

Ч: Ну слушайте, ну мне сейчас неудобно, правда, я сейчас не могу даже сориентироваться, когда я смогу отпроситься с работы.

М: Не сможете, так не сможете. Я вас просто предупреждаю, что могут потом из-за этого быть проблемы…

Ч: Ну, что делать, у меня в принципе сейчас работодатель очень ответственный и ведёт электронную трудовую книжку, поэтому я не думаю, что….

М: А какая разница тому руководителю, который у вас сейчас, если у вас уже есть два года неучтённого каким-то образом?

Ч: Ну у меня же есть ещё и бумажная трудовая книжка, я всё смогу подтвердить.

М: Вам не подтвердить надо, вы не понимаете. Вам не надо подтверждать тот текущий стаж, который у вас уже есть. Вам нужно сделать перерасчёт, чтобы вам добавили два года неучтённого. У вас где-то два года потерялось попросту!

Ч: Ну так у меня весь мой стаж отражён в трудовой книжке. Если там что-то неучтено, значит…

М: (перебивает) Вы знаете, что такое неучтённый трудовой стаж?

Ч: Вот объясните мне, что такое неучтённый трудовой стаж?

М: У вас есть ваша электронная книжка, в которой есть информация касаемо того, где, сколько вы отработали, на какой должности и так далее. Неучтённый трудовой стаж – это те сроки, те годы, которые в этой трудовой книжке не учтены от слова «совсем». Ни в электронной, ни в бумажной. То есть, их нет. В таком случае это позволяет государству снизить ваш пенсионный коэффициент на законном основании, а вы потом скажете: «Ой, а чего это у меня такая маленькая пенсия?» Либо же у вас начнутся вообще проблемы с выплатами из-за этих двух неучтённых лет, могут вам вообще или неправильно начислять пенсию, или вообще её не начислить, пока вы опять же не подъедете, не сделаете перерасчёт.

Ч: Хорошо, на следующей неделе я готова подъехать, в среду.

М: Обязательно запишите себе тогда 10.00 или 16.10. Я вас тогда сейчас буду ставить в электронную очередь. Номер СНИЛСа мне, пожалуйста, скажите.

Ч: Нет, я никакие свои данные по телефону не называю.

М: У вас перерасчёт по СНИЛСу, по пенсионному, у вас перерасчет пенсионного коэффициента. Я у вас прошу не номер банковской карты, а всего лишь номер свидетельство пенсионного страхования.

Ч: Ну так и что? Я никакие данные по телефону не разглашаю.

М: Я в таком случае вас записать не смогу. Записывайте себя самостоятельно.

Ч: Хорошо, запишусь самостоятельно.

И всё. Жулик слился. С явной досадой о потраченном времени. Собеседнице – почёт и уважение, так качественно держать персонажа на линии надо уметь. Финалом этого диалога, при развитии сценария мошенника, стало бы получение «жертвой» кода на восстановление доступа к госуслугам, сообщение его жулику и «угон» учётной записи.

Будьте начеку

Несостоявшийся инвестор



Челябинец перевёл мошенникам около двух миллионов рублей, пытаясь заработать на инвестициях.

В полицию с заявлением о мошенничестве обратился 59-летний мужчина. Он рассказал, что увидел на одном из сайтов рекламу с информацией об инвестировании денежных средств. Житель Челябинска оставил свой номер телефона, вскоре ему позвонил незнакомец и стал объяснять суть работы на бирже и заработка на криптовалюте.

Звонивший предложил инвестировать денежные средства с последующим доходом. Потерпевший согласился, после чего ему велели скачать приложение, посредством которого осуществлялось дальнейшее общение. С заявителем связался якобы трейдер, который контролировал процесс «инвестирования». Челябинцу были даны инструкции включить демонстрацию экрана и скачать платёжное приложение, посредством которого он перевёл денежные средства в сумме более 1,8 миллиона рублей на неизвестные счета.

После того, как мужчина не получил обещанный доход и не смог вывести свои денежные средства, он понял, что стал жертвой мошенников и обратился в полицию.

Возбуждено уголовное дело по статье «Мошенничество».

Полиция напоминает гражданам о необходимости быть бдительными при выборе брокерских компаний и инвестировании денежных средств. Необходимо внимательно изучать официальную информацию о брокере, либо о компании, куда гражданин планирует вложить денежные средства. Следует помнить, что для мошенников характерно обещание высоких процентов и стабильной прибыли новичкам, отсутствие регистрации. Если противоправное деяние всё-таки произошло и вы лишились денежных средств вследствие мошеннических действий, незамедлительно обращайтесь в полицию.

Учитесь на чужих ошибках

Три миллиона проходимцам

Мошенники смогли украсть у жителя Кусы более трёх миллионов рублей.

Новой жертвой дистанционных мошенников стал 22-летний южноуралец. Для его обмана злоумышленники использовали распространённую схему с начальным звонком от имени сотового оператора. Кусинцу предложили продлить срок действия сим-карты, для чего попросили назвать пришедший в смс код.

Далее ему последовали звонки якобы с сайта госуслуг, из банка и от правоохранительных органов. Молодому человеку сообщили, что под видом сотового оператора ему звонили мошенники, благодаря полученному коду они вошли в личный кабинет на портале и получили доступ к его счетам, а также подали заявки на несколько кредитов. Чтобы этого не допустить, кусинцу рекомендовали самому оформить несколько займов и вместе с собственными средствами перевести на «безопасный счёт».

В течение недели он брал кредиты, одалживал крупные суммы у родных и переводил их на указанные счета. Для этого молодой человек даже ездил в Златоуст, чтобы использовать банковский терминал. В результате мужчина отдал мошенникам три миллиона десять тысяч рублей. А понял, что стал жертвой аферистов, когда те потребовали перевести им ещё 230 тысяч.

Следственным отделом по Златоустовскому городскому округу возбуждено уголовное дело по статье «Мошенничество, совершённое организованной группой либо в особо крупном размере».

Сотрудники полиции вновь напоминают, что никому ни под каким предлогом не следует сообщать коды из телефона и немедленно прекращать разговор, если неизвестные сообщают об оформляемых на вас кредитах, взломе банковского счёта и прочих финансовых операциях. Помните, что так поступают только мошенники.

«Золотой» счётчик

Мошенники убедили пенсионерку перечислить им 830 тысяч рублей после сообщения о проверке счётчиков.



75-летняя жительница рассказала полицейским, что ей позвонил неизвестный, представился сотрудником энергоснабжающей компании и убедил её в необходимости замены счётчиков электроэнергии. Для начала процедуры необходимо было назвать данные СНИЛС и четырёхзначный код из смс, что она и сделала.

Следующий звонивший сообщил пенсионерке о взломе личного кабинета на сайте госуслуг и доступе мошенников ко всем личным данным. Якобы для того, чтобы обезопасить собственные средства, их необходимо было перевести на «безопасный счёт».

Испуганная женщина отправила мошенникам все накопленные средства – 830 тысяч рублей. Однако после перевода денежных средств аферисты прекратили общение. Осознав, что её обманули, потерпевшая обратилась в полицию.

Возбуждено уголовное дело.

Сотрудники полиции вновь призывают граждан к рассудительности и настоятельно рекомендуют не верить посторонним по телефону, если речь заходит об угрозе сбережениям или попытках оформления кредитов. Если вы получили сомнительный телефонный звонок, поделитесь сомнениями с родственниками, обратитесь в отдел внутренних дел по телефону 102, но никогда не принимайте поспешных финансовых решений и не переводите деньги под диктовку незнакомцев по телефону. Помните, любые сообщения от кого-либо с предупреждениями об оформляемых кредитах, взломанных счетах и предложения «обезопасить» их исходят только от мошенников.

Учитесь на чужих ошибках

Приёмы-«ловушки»

Полицейские раскрыли психологические приёмы, которые используют мошенники.

Сотрудники подразделения по борьбе с киберпреступлениями Главного управления МВД России по Челябинской области раскрыли психологические приёмы, которые используют мошенники для обмана граждан.

Срочность (эффект ограниченного времени). Мошенники создают ощущение срочности: «Срочно подтвердите код, иначе ваш аккаунт заблокируют». Срочность вредит способности человека к критическому мышлению. Человек действует эмоционально, а не разумно.

Авторитет (эффект Милгрэма). Мошенники представляются сотрудниками банка, полиции или ФСБ, потому что в природе большинства людей подчиняться авторитету. Уверенный, возможно, чуть-чуть грубоватый тон также способствует этому эффекту.

Эмоциональное давление (страх или вина). Вас пугают (например, «ваши родственники в беде») или пытаются вызвать чувство вины («из-за вашей ошибки система заблокирована»). Страх и вина также подавляют способность логически мыслить и приводят к подчинению.

Иллюзия доверия (социальное доказательство). Социальное доказательство – это психологический принцип, согласно которому люди выбирают, как им поступить, с оглядкой на поведение других людей. Мошенники говорят: «Все так делают», «Ваши друзья уже зарегистрировались».

Комплименты и лестные отзывы. Мошенники могут хвалить вашу «проницательность» или упоминать некий «уникальный статус», чтобы получить расположение. Например, представившись сотрудником правоохранительных органов, могут попросить помочь выявить преступника. Жертва, попавшаяся на эту удочку, будет пытаться соответствовать статусу и завоевать доверие.

Манипуляция недостатком знаний. Злоумышленник может использовать сложную терминологию, чтобы подтвердить свою экспертность, кроме того непонимание вызывает страх показаться некомпетентным, и человек соглашается на предложение.

Ложная персонализация. Это маркетинговый приём, когда алгоритмы искусственного интеллекта пытаются создать иллюзию индивидуализированного опыта для пользователя, но на самом деле используют стандартные шаблоны и данные. Аферисты обратятся к вам по имени-отчеству, чтобы показать, что знают о вас всё.

Микрошаги к большой уступке (техника «нога в двери»). Эффект приёма «нога в двери» объясняют тем, что, оказав необременительную помощь при первой просьбе, индивид начинает осознавать себя отзывчивым человеком, готовым помочь другим в хорошем деле. Это повышает самооценку индивида, и человек бессознательно или осознанно налагает на себя моральные обязательства – быть таким же (нужным, отзывчивым) и впредь. Злоумышленники начинают с маленькой просьбы, например, «Назовите имя», а затем требуют большего.

Доигралась!

Внучка озерчанки по указанию мошенников потратила на покупку игровой валюты около 60 тысяч рублей.

В дежурную часть озёрской полиции обратилась 71-летняя жительница города с заявлением о хищении с её расчетных счетов около 60 тысяч рублей.

Полицейские выяснили, что девятилетняя внучка потерпевшей в одном из приложений хотела приобрести игровую валюту. Для этого она выполняла указания неизвестного, который просил делать фото экрана. Таким образом, в ходе манипуляций по указанию злоумышленников она совершила пять переводов денежных средств на общую сумму около 60 тысяч рублей, но игровую валюту получить так и не смогла.

После поступления денежных средств злоумышленник удалил диалог и больше на связь не выходил.

Возбуждено уголовное дело по статье «Мошенничество».