

## Правила финансовой безопасности

Люди старшего поколения не успевают адаптироваться к финансовым инструментам, из-за чего зачастую становятся жертвами мошенников. Способы хищений разные – от кражи данных банковских карт до продажи несуществующих лекарств. Разберёмся, какие схемы используют мошенники и как им противостоять.

### Общие принципы использования карты

Распространённый способ получить доступ к деньгам – узнать данные карты. Банки постоянно предупреждают клиентов от передачи пластика, а также сообщения кодов и паролей третьим лицам. Но пенсионеры не всегда идентифицируют случаи мошенничества, несмотря на эти предупреждения.

Распространённая схема обмана – использование СМС-сообщений с целью получить доступ к счёту клиента.

Присланная информация может быть разной: списаны деньги, счёт заблокирован, выигрыш приза, получение компенсации и т.д. Главное – не предпринимать никаких действий после получения такого сообщения: не перезванивать по указанному номеру, не переходить по ссылке, не сообщать никакие сведения. Так, вирусная ссылка опасна тем, что мошенники получают доступ к мобильным банкам на телефонах и снимают или переводят деньги.

Это касается и телефонных звонков. Конечно, сотрудники банка могут общаться с клиентами, но никогда не попросят предоставить данные карты, ПИН-код и пароли из СМС. Уточните у собеседника имя, фамилию и должность, и, если сомневаетесь, попрощайтесь и перезвоните в банк по номеру, указанному на карте или официальном сайте организации. Спросите, работает ли в банке такой сотрудник, может ли он звонить клиентам, если да – с какой целью.

Общеизвестный совет, но нельзя об этом не сказать – не записывайте пароли на бумажках! Преступники могут поджидать у банкомата, следя за действиями держателя карты. Эта бумажка или кошелек с ней затем и похищаются. Таких прецедентов множество, поэтому не стоит надеяться на то, что злоумышленники не пойдут на столь

открытые действия. Это касается и хранения пароля в телефоне – вместе с его потерей рискуете лишиться и сбережений.

## **Конкретные схемы мошенничества**

Даже зная общие правила использования карты, не всегда получается избежать потери денег из-за преступных посягательств. Это связано с тем, что мошенники используют разные способы психологического воздействия на жертву. Пенсионеры входят в группу риска из-за своей доверчивости, поэтому стоит ознакомить родителей, бабушек и дедушек с самыми распространёнными преступными схемами.

### ***«Ваша карта заблокирована»***

Излюбленный приём преступников – представиться сотрудником банка. Это может быть как звонок, так и СМС с информацией о том, что деньги списаны, карта заблокирована или есть угроза хищения. В процессе разговора злоумышленники выясняют, сколько средств на счету. Затем сообщают, что для разблокировки или предотвращения хищения нужны данные карты, в том числе информация, необходимая для списания денег (CVV/CVC-код, срок действия пластика). На пенсионера начинают психологически давить, пугая тем, что эти сведения нужны для срочной блокировки карты. Конечно, настоящие сотрудники банка не будут просить предоставить эту информацию.

### ***«Вам положена компенсация»***

Преступники представляются судебными приставами и сообщают, что пенсионер признан потерпевшим, которому положена компенсация. Так, реальный случай – злоумышленники сообщали, что деньги вернут тем, кто покупал БАДы (а таких было много). После этого человеку называют внушительную сумму, для получения которой нужно оплатить пошлину. Преступники дают реквизиты счёта, на который необходимо перевести деньги. Другой вариант – спрашивают данные карты, чтобы перевести сумму компенсации, но вместо этого списывают средства. Например, несколько лет назад действовала схема «дети войны», когда злоумышленники обещали пенсионерам компенсации за участие в действиях в тылу или на фронте.

### ***«По ошибке отправили код»***

Это схема с созданием сайта, на который устанавливается платный вход по коду и номеру телефона. На номер приходит код, как при покупке в интернет-магазине, а преступники звонят и просят его сообщить, так как без этого «не могут завершить операцию». Упор здесь делают на том, чтобы разжалобить человека, но это обман. Во-первых, такой код приходит только на номер, привязанный к мобильному банку. Во-вторых, даже если код не прислали, можно запросить повтор. Если же человек сообщает присланные цифры, с номера списываются деньги. Похожая схема с платным звонком. На телефон поступает звонок, который резко обрывается. Если человек перезванивает, то слышит либо автоответчик, либо длинные гудки. За время ожидания снимаются деньги, которые поступают на счёт преступников.

### ***«Перерасчёт пенсии»***

Мошенники могут представляться сотрудниками Пенсионного фонда, в качестве предложения для предоставления сведений указывая «перерасчёт пенсии». Как вариант – звонят и строгим голосом сообщают, что в прошлом году пособие начислили в большем размере, поэтому необходимо провести проверку и исправить это, иначе грозит штраф. Упор здесь на эффекте неожиданности и страхе перед ответственностью. Конечно, сотрудники Пенсионного фонда не будут звонить и просить данные карты для «проверки», да и заниматься перерасчётами по телефону никто не станет. К тому же за излишне начисленные деньги не может наступить никакая ответственность.

### ***«Ваши анализы готовы»***

В основе другой схемы – тот факт, что пенсионеры часто ходят по поликлиникам и делают анализы. Мошенники обзванивают пожилых людей и сообщают, что их анализы готовы. Если человек недавно посещал больницу (в противном случае говорят, что ошиблись), то сообщают о плохих результатах и требуемом срочном лечении. Для выздоровления необходимы лекарства, которых в городе почти нет, но можно купить сейчас – нужны наличные, которые заберёт курьер при доставке препаратов. Под их видом привозят дешёвые витамины или БАДы. Предложить купить «чудо-препарат» или устройство для излечения болезней могут и лично, если пенсионер открывает дверь лицу, представившемуся сотрудником социальных органов. Преступник говорит, что действует огромная скидка, так как это поддержка властей, а приобрести можно только сейчас, так как это «последняя коробка». Конечно, соглашаться на такое нельзя.

### ***«Ремонт в кредит»***

Схема простая: к пенсионерам заходят мошенники, обещающие ремонт в рассрочку (замена окон и т.д.), а вместо этого подсовывают договор потребительского кредита на крупную сумму. В итоге ни окон, ни денег, так как после подписания преступники требуют отдать долг. Конечно, главная рекомендация – не пускать в дом незнакомцев, кем бы они не представлялись. Если сообщают о работе в государственных органах, позвоните на общий номер и уточните, работает ли там такой человек и входит ли в его обязанности обход жилых домов. Особенно это касается замены счётчиков – перед тем, как отдавать деньги или подписывать договор, убедитесь, что это плановые работы. Если договор уже подписан, идите в правоохранительные органы и суд, настаивайте на том, что вас ввели в заблуждение, поэтому документ должен быть признан недействительным.

### ***«Родственник в беде»***

Распространённая схема – просьба о помощи от внука или сына и т.д. Либо приходит СМС с информацией о том, что случилось что-то плохое, либо поступает звонок, разобрать в котором голос говорящего невозможно. Ситуации могут быть самыми разными. Например, случилась авария, родственник виноват и грозит уголовная ответственность, но этого можно избежать – вот номер счёта и конкретная сумма. Расчёт здесь на то, что пенсионер не сможет дозвониться близкому человеку, испугается и переведёт деньги. Конечно, делать так ни в коем случае нельзя – не предпринимайте никаких действий до того, как свяжетесь с родственниками.