Лекарство от мошенников: инструкция по применению

Семь «НЕ», которые помогут вам сберечь свои деньги.

Жителей Пензенской области всё чаще атакуют обманщики. Они могут подкрасться к вам с любой стороны. Позвонить по телефону. Сделать заманчивое предложение в социальных сетях. Подойти на улице. Они действуют сотнями разных способов.

Чем опасны мошенники? Если вы поверите им, они лишат вас денег. И, возможно, другого ценного имущества.

Как сохранить свои деньги? Запомните простые правила защиты от злоумышленников. Расскажите о них своим родственникам, друзьям и знакомым, коллегам на работе. И вспоминайте эти правила каждый день. Чтобы обманщики не смогли застать вас врасплох даже ночью.

Вот эти правила.

№1. Не доверяйте незнакомцам!

Почему? Мошенник может представиться кем угодно – особенно если вступает с вами в контакт на расстоянии.

Чем это грозит? Если вы ему поверите, он станет вас пугать (например, скажет, что с вашей карты пытаются похитить деньги или на ваше имя кто-то посторонний взял кредит). Или постарается ввести в заблуждение (к примеру, убедит, что вам полагается социальная компенсация или приз).

Что делать? Если вам позвонил незнакомец, спросите у него фамилию, имя и отчество, место работы и должность, контактный телефон. Уточните, по какому вопросу он вас беспокоит. Скажите, чтобы он перезвонил вам через 10 минут. А сами в это время обратитесь к своим родственникам, знакомым или соседям. Расскажите им о том, кто и для чего вам звонил. Посоветуйтесь с ними, как действовать дальше.

№2. Не пускайте незнакомцев в дом!

Почему? Ваш дом – ваша крепость. Пока входная дверь закрыта, вы в безопасности.

Чем это грозит? Как только незнакомец (или незнакомка) с дурными намерениями оказался в вашем доме, он получает возможность отвлечь вас и впустить сообщников, которые незаметно для вас похитят деньги и имущество.

В другом случае он может ввести вас в заблуждение (например, сказать, что нужно менять «старые» деньги на «новые» или вам нужно проверить счётчики или газовое оборудование) и под этим предлогом украсть ваши сбережения.

Что делать? Если к вам домой пришли незнакомцы, представились сотрудниками социальной, коммунальной или любой другой службы, попросите их через дверь громко и отчётливо назвать свои фамилию, имя и отчество, место работы и должность, а также контактный телефон организации, которую они представляют.

Запишите эти данные. Затем позвоните по указанному телефону и уточните, действительно ли такой сотрудник работает в данном учреждении и в связи с выполнением служебных обязанностей должен находиться в вашем доме.

№3. Не перечисляйте деньги незнакомцам!

Почему? Преступнику не нужно ломиться в ваш дом или грабить вас на улице, если вы готовы сами отдать ему деньги.

Чем это грозит? Если вам обещают выдать кредит на условиях, в которых отказывают другие банки, говорят, что вам выпал приз в несколько сотен тысяч рублей или убеждают, что вам полагается компенсация за некачественные препараты – будьте начеку. Вам скажут, что через день вы сказочно разбогатеете – а для этого нужно перевести на чужой счёт небольшую сумму в качестве страховки, госпошлины или под любым другим предлогом. Если вы поверите, то разбогатеют только мошенники.

Что делать? Помните: если человек выиграет денежный приз в государственную лотерею, то налоги он платит ПОСЛЕ того, как получит выигрыш. Поэтому, если вам обещают выдать компенсацию или выигрыш по какой-нибудь акции, попросите сначала перечислить вам всю сумму. Объясните, что только после этого готовы вернуть все налоги, пошлины и оплатить услуги специалистов, которые якобы вам помогали.

Если вам говорят, что на счёт вашей банковской карты перечислили определённую сумму и просят вернуть её обратно, скажите, вам следует вначале обратиться в банк (лично в отделение или по телефону «горячей линии», указанному на обороте карты) и уточнить, действительно ли на ваш счёт поступила такая сумма. Если этого не произошло, значит, с вами говорят мошенники, и разговор с ними следует прекратить.

№4. Не сообщайте посторонним данные банковской карты и цифровые коды из смс!

Почему? Банковская карта – ключ к вашему банковскому счёту. Сообщить постороннему данные своей карты – всё равно, что дать ему ключ от своего дома.

Чем это грозит? Безопасно можно сообщить незнакомому человеку только НОМЕР карты – для перевода денег этого достаточно. Если посторонний человек узнает все данные вашей банковской карты – такие, как её срок действия, код безопасности с обратной стороны, ваши имя и фамилию, – ему останется всего один шаг до того, чтобы обчистить ваш счёт до копейки.

Последний рубеж защиты – цифровой код из смс-сообщения. Если вы сообщите этот код незнакомцу, можете сразу же попрощаться со всеми деньгами, которые храните на счёте в банке.

Что делать? Если незнакомец под любым предлогом запрашивает у вас информацию о данных вашей банковской карты (кроме номера), сразу же прекращайте разговор. Так действуют только мошенники!

№5. Не покупайте товар, не потрогав его!

Почему? В интернете много заманчивых предложений приобрести товары, которые в два-три-четыре раза дешевле, чем в магазине. Однако чем ниже цена, тем выше вероятность стать жертвой мошенников.

Чем это грозит? Вам обещают продать товар на выгодных условиях при условии, что вы перечислите 100-процентную предоплату. Или говорят, что товар пришлют наложенным платежом: это когда вы сначала платите за посылку, и только потом получаете возможность её открыть. В этом случае вам или не присылают ничего, или присылают совсем не то, что вы заказали.

Что делать? Избегать сделок с частичной либо полной предоплатой. Выбирайте такие условия, при которых товар сначала можно осмотреть, потрогать и проверить, и только затем платить за него. Это возможно, если пользоваться услугами курьерской доставки. В этом случае товар оплачивают после вскрытия посылки в присутствии курьера. Это убережет вас от ситуации, когда деньги за товар оплатили, но вещь так и не получили.

№6. Не верьте просьбам одолжить деньги!

Почему? Люди всё больше общаются в соцсетях. Иногда даже чаще, чем в реальной жизни. Поэтому к переписке в интернете многие относятся так, как будто разговаривают с человеком вживую.

Чем это грозит? Однажды в социальной сети вы получаете от знакомого пользователя сообщение о том, что у него брат в больнице и нуждается в операции / неприятности на работе / ещё тысяча причин, по которым автору сообщения срочно нужна значительная сумма, которую он просит у вас в долг. Если вы поверите и перечислите деньги на указанный в сообщении счёт банковской карты, обратно вы ничего не получите.

Что делать? Получив сообщение с просьбой одолжить деньги, свяжитесь с его автором любым способом, кроме социальной сети, и сообщите, что его аккаунт взломали. Такие просьбы через интернет пишут только мошенники!

№7. Не устанавливайте на свой телефон подозрительные приложения!

Почему? Большинство из нас управляет своим банковским счетом через телефон – через официальные банковские приложения или путем получения и отправки сообщений на короткий номер банка.

Чем это грозит? Если у вас мобильный телефон с операционной системой «Андроид», вы – в зоне повышенного риска. Во многих приложениях, разработанных для «Андроида», есть уязвимости. Мошенники пользуются этим, чтобы внедрить в приложения вирусы, которые затем позволят им управлять вашим телефоном и через него похищать деньги с вашего банковского счёта.

Другая опасность – когда обманщики по телефону представляются сотрудниками банков и предлагают установить приложения, с помощью которых якобы можно предотвратить или блокировать кражу денег с вашего счёта. На самом деле результат будет тот же самый – с вашего счёта похитят всё до последнего рубля.

Что делать? Установить на свой мобильный телефон антивирусные программы. Не скачивать приложения из ненадёжных источников. Никогда не устанавливать приложения по совету незнакомцев.

Запомните эти семь правил и следуйте им в любой ситуации. А если у вас возникнут сомнения, вы всегда можете обратиться за помощью и советом по телефонам полиции: 02 (со стационарного телефона) или 102 (с мобильного телефона).

Материал подготовлен пресс-службой УМВД России по Пензенской области

Распространенные виды мошенничества

Сайты-двойники

Мошенники создают сайт-двойник официального сайта, на котором совершаются онлайн-покупки. Потерпевший оплачивает услугу, переводя средства на счет преступника. Часто так происходит при заказе страхового полиса на сайте страховой компании. Не убедившись в подлинности источника, посетители заказывают страховку ОСАГО

Рассылка SMS

В этом случае на телефон приходит объемный файл с текстом якобы от вашего знакомого типа: «Вспомни, как у нас это было». Вы открываете файл, и ваш телефон заражается вредоносной программой. В итоге с привязанного к сим-карте банковского счета списываются деньги. Подобные смс/ ммс могут поступить и от того, чьи контакты действительно есть в вашей записной книжке

Рассылка на e-mail

Поступившие на электронную почту письма со ссылками на различные сайты также могут содержать вирусную программу. Перейдя по ссылке, вы запускаете вредоносное программное обеспечение, с помощью которого преступники получают доступ к вашим банковским счетам

Переписка в соцсетях

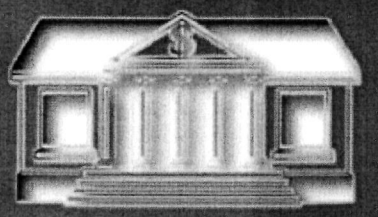
Злоумышленники взламывают страницу в социальной сети и от имени лица, на которое она зарегистрирована, рассылают сообщения его друзьям с просьбой занять деньги. Откликаясь на просьбу товарища, многие люди лишаются таким образом своих денег

Кража с потерянного телефона

Также списание денежных средств со счета гражданина может произойти в результате утери им сотового телефона, в котором не была отключена «привязка» телефонного номера к банковским счетам. Ведь любой нашедший телефон человек получает к ним доступ и имеет возможность перевести деньги

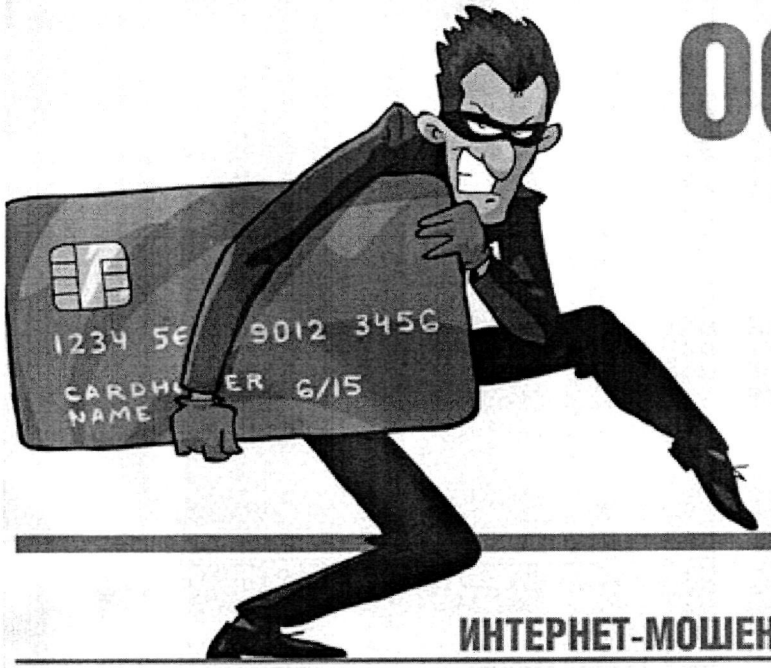
Как предостеречь себя?

- В целях получения необходимых услуг пользуйтесь только официальными сайтами. Для оплаты используйте дополнительную карту (не основную), на которую будет заблаговременно переведена нужная для оплаты приобретаемого товара или услуги сумма.
- При смене сим-карты отключайте так называемые «привязки» номеров телефонов к банковским счетам. При утере телефона с подключенной услугой «Мобильный банк» - сразу же заблокируйте сим-карту либо отмените действие данной услуги.
- Не доверяйте поступившим на телефон или электронную почту смс, в которых требуется переход по различным ссылкам. Лучше перепроверьте информацию.
- Не перечисляйте деньги друзьям, которые просят об этом в соцсети – возможно, их страница взломана мошенниками. Сначала убедитесь, что товарищи действительно нуждаются в вашей помощи.



ВАЖНО

Сотрудники банка никогда не запрашивают пароли и коды СМС-подтверждений по телефону – никогда никому их не сообщайте! Внимательно относитесь к СМС и e-mail-сообщениям от имени банка, в которых содержится информация о блокировке вашей карты, никогда не перезванивайте по номерам, указанным в этих сообщениях, всю дополнительную информацию узнавайте у официальных представителей банка по телефонам, указанным на карте.



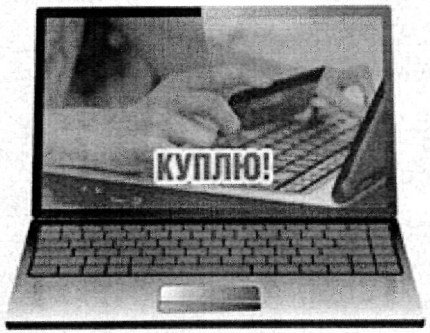
ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



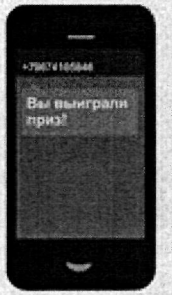
ТЕЛЕФОННЫЕ МОШЕННИКИ

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

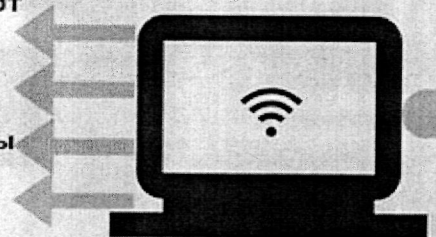


ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Хищения денег под видом продажи товара ненадлежащего качества, не соответствующего заявленному, с использованием интернет-площадок

При осуществлении входа на сайт уже известных Вам банков или организаций внимательно изучите открывшуюся страницу- она может оказаться двойником

Мошенники создают интернет-сайты "двойники" по продаже товаров, которые идентичны оригинальным



Не производите предоплату товара.

Продажа несуществующей в реальности продукции в лже-интернет магазинах

Деньги можно отдать только в том случае,если заказанный товар проверен и полностью устраивает

Хищение денег с банковских счетов физических лиц при использовании неправомерного доступа к банковским картам потерпевших

Ни под каким предлогом и ни при каких обстоятельствах не сообщайте незнакомым людям цифры, написанные на вашей банковской карте