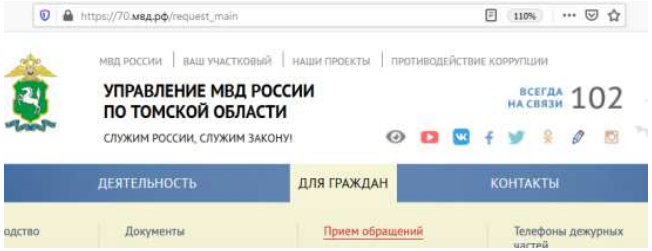

- При поступлении телефонного звонка из «банка» с сообщением о «подозрительной операции по банковскому счёту», «оформлении третьим лицом кредита на Ваше имя», «несанкционированном списании денежных средств» **помните – это мошенник!** Немедленно прекратите разговор и обратитесь в ближайшее отделение банка для уточнения информации, либо позвоните в организацию по официальному номеру, который указан на оборотной стороне банковской карты.
- Если потенциальный продавец или покупатель просит вас перейти по ссылке, якобы для оформления «безопасной сделки или доставки», или же под предлогом «зачисления денег на карту», «оплаты покупки» **помните – это мошенник!** Внимательно изучите информацию о «безопасной сделке» или «безопасной доставке» на официальном сайте торговой площадки, прежде чем совершить необдуманные операции!
- Не сообщайте никому, в том числе по телефону даже «роботу» или по «роботизированной линии» свои данные, данные банковских карт и коды из SMS-сообщений.
- Не устанавливайте на свои мобильные устройства приложения по просьбе незнакомых Вам лиц.
- При совершении покупок и продаж в сети Интернет внимательно изучите информацию о «продавце» или сайте в сети Интернет, не сообщайте и не указывайте дополнительные данные своих банковских карт, не проводите операции через банкомат по указанию незнакомых Вам лиц, воздержитесь от полной или частичной оплаты посредством перевода и совершайте сделки только «из рук в руки».
- При поступлении сообщения от близкого родственника, друга или просто знакомого с просьбой о помощи, в том числе занять денежные средства, необходимо самостоятельно перепроверить информацию, позвонив на номер телефона человека, и убедиться в необходимости осуществления финансовой операции.

## КУДА СООБЩАТЬ О ПРЕСТУПЛЕНИИ

Если вы стали жертвой мошенников или столкнулись с мошенническими действиями, незамедлительно обращайтесь в ближайшее отделение полиции или сообщайте в полицию по телефону «02», с сотового «102». Также для направления обращений, заявлений о правонарушениях или преступлениях возможно использовать сервис «Прием обращений» на официальном сайте УМВД России по Томской области - https://70.мвд.рф/request_main





Зачастую граждане, зная об основных видах и способах телефонного и Интернет мошенничества, попадаются на уловки злоумышленников, которые убеждают сообщить им конфиденциальную информацию, оперируя знаниями о личных данных.

## Главное помнить:

Мошенники могут обладать информацией о некоторых данных Вашего паспорта, месте жительства, детализации по банковскому счету, платежах по кредиту, о некоторых данных Вашей банковской карты, кодовом слове. Не поддавайтесь на провокации мошенников!

**Будьте бдительны! Не дайте себя обмануть!**
**Поделитесь информацией со своими близкими!**

УМВД России по Томской области

# ОСТОРОЖНО!!! ТЕЛЕФОННЫЕ И ИНТЕРНЕТ МОШЕННИКИ!


СОХРАННОСТЬ ВАШИХ ДЕНЕГ – ТОЛЬКО В ВАШЕЙ КОМПЕТЕНЦИИ

г. Томск
2020

Основные виды и способы преступлений, совершаемых с использованием IT-технологий:

**«Лжесотрудник банка»**

Наиболее распространённым способом обмана остается схема, при которой гражданину звонит неизвестный, представляется работником банка или службой безопасности банка, и предупреждает о якобы несанкционированной попытке или списании денежных средств, оформлении третьими лицами кредита на имя жертвы или совершения подозрительных операций по счетам. После чего, якобы для сохранности финансов, или же отмены подозрительных операций, мошенники просят сообщить им или «роботу» («роботизированной линии») реквизиты банковских карт, защитный код на оборотной стороне карты, состоящий из трех или четырех цифр, а также коды подтверждения операций из SMS-сообщений. Иногда мошенники убеждают граждан пройти до ближайшего банкомата и осуществить перевод денежных средств на «безопасный счёт» или «безопасную ячейку» банка. В некоторых случаях злоумышленники предлагают установить на телефон программу безопасности для мобильного банка, которая на самом деле является программой удаленного доступа, и, получая доступ к мобильному банку на мобильном устройстве жертвы, похищают денежные средства.

**«Ложный покупатель»**

Другой схемой обмана остается хищение денежных средств при осуществлении продажи товаров через популярные торговые площадки сети Интернет.

Зачастую, граждане, которые решили продать свои личные вещи, или же различные предметы, сталкиваются с таким видом мошенничества, при котором потенциальный покупатель (он же мошенник) поясняет, что он из другого города, или даже области, и просит отправить ему товар службой доставки, оформив «безопасную доставку» или же «безопасную сделку», и для этого предлагает перейти по ссылке, которую отправляет в мессенджере или по электронной почте. Перейдя по ссылке, потерпевшие попадают на «фейковую» страницу, которая визуально схожа с официальным сайтом торговой площадки, или платёжной системы. На поддельной странице предлагается ввести полные реквизиты банковской карты, чтобы якобы получить деньги за товар, оплатить покупку или доставку. Если человек введет полные данные карты, включая трехзначный код с обратной стороны, то мошенник сможет украсть деньги с его счета.

Также «ложный покупатель» может попросить сообщить ему номер карты, а также трёхзначный код, расположенный на оборотной стороне банковской карты и код подтверждения операции из SMS-сообщения, якобы необходимые ему для зачисления на Вашу карту денежных средств, а в действительности произойдет списание Ваших финансов.

**«Ложный продавец»**

Иногда потерпевшие «на доверии» или «на честном слове» переводят деньги в счет оплаты товара или услуги, объявление о продаже которого они нашли в Интернете, в результате чего не получают оплаченный товар, а продавец перестает выходить на связь. Или же продавец отправляет посылку, в которой содержится товар, не соответствующий заявленному.

**«Займи-помоги»**

Не менее распространённым способом обмана является мошенничество в социальных сетях, при котором, злоумышленник, получив доступ к странице пользователя, от его имени, под различными предлогами, просит у Вас занять денежные средства, и рассылает данное сообщение всему списку «друзей». Граждане, которым приходит данная просьба от «друга», не перепроверяют информацию и осуществляют переводы на указанные им номера и счета, в результате чего становятся жертвами мошенников.

**«Фальшивое знакомство»**

В связи с участившимися случаями стоит отметить мошенничество, при котором молодые люди знакомятся в социальных сетях и различных сайтах знакомств с якобы девушками, которые в процессе переписки, предлагают совместный поход в кино/театр, или же посидеть в уютной домашней обстановке, наслаждаясь суши или пиццей. Далее, злоумышленники присылают ссылку на «фейковый» сайт (театр, кино, служба доставки суши и пиццы) и завлеченные знакомством граждане совершают покупки билетов на несуществующие сеансы кино и спектакли, или же оплачивают доставку мнимой еды, указывая реквизиты своих банковских карт на мошеннических страницах, после чего лишаются всех денежных средств, которые находятся на их счетах.

**«Родственник в беде»**

Данный вид телефонного мошенничества по-прежнему имеет место быть и заключается в том, что Вам поступает звонок с неизвестного номера и незнакомец представляется сотрудником правоохранительных органов. Далее злоумышленник сообщает, что Ваш близкий человек задержан и в настоящее время принимается решение о привлечении его к уголовной или же административной ответственности. Могут указываться разные причины (ДТП, незаконное хранение оружия, совершенное убийство, обнаружение наркотиков, нанесение телесных повреждений другому лицу и т.п.). Затем мошенник передает трубку якобы близкому человеку, который взволнованным, нечетким голосом или шёпотом сообщает, что попал в беду. Телефон при этом якобы передается сотруднику правоохранительных служб, который предлагает свою помощь в этой ситуации за денежное вознаграждение. Если жертва соглашается, то звонящие сообщают место, куда необходимо привезти деньги или передать «курьеру». Иногда деньги просят перевести на номер телефона или по номеру карты.

**«Ложный выигрыш или выплата»**

Зачастую, пользователи Интернета получают сообщения, уведомления или рекламу, о том, что именно они стали победителем в розыгрыше, и им положен выигрыш. Или же гражданам полагается большая выплата и поддержка. Далее, для получения денежных средств, предлагается перейти по ссылки и указать свои данные и реквизиты карты, якобы для расчета положенной суммы. Указывая данные банковских карты, граждане прощаются со своими деньгами, так и не получив обещанные денежные средства.