



3. Рассылка фейковых СМС от банка и иных сообщений:

- смс-сообщения на телефон о блокировке карты;
- смс-сообщения с кодом для подтверждения покупки, которую человек не совершил, после чего поступает звонок от лжесотрудника банка с просьбой пройтиковать полученный код;
- смс-сообщения с кодом на восстановление пароля – могут поступать, если мошенники зашли на сайт банка, попытались авторизоваться в личном кабинете от вашего имени и инициировали процедуру сброса пароля. После этого поступает звонок мошенников, которому ни в коем случае нельзя готовить полученный код;
- смс-сообщения с текстом, что карта заблокирована. В конце сообщения указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит по номеру и попадает в рукинского мошенника, выплачивая его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки;

- смс-сообщения на мессенджеры «Вайбер» или «Вотсап» о том, что для гражданина истекает срок получения денежной компенсации и для ее получения необходимо перейти по указанной ссылке.

Что делать?

Не переходите по ссылке, заблокируйте или удалите сообщение, никогда и никому не сообщайте свои данные, а также любую банковскую информацию. При любом подозрении сами перезвоните на «горячую линию» банка, набрав номер телефона банка вручную.



4. Размещение в сети Интернет объявлений, не соответствующих действительности

- размещение не соответствующих действительности объявлений о продаже, при этом цена в объявлении, как правило, явно занижена. При контакте с «владельцем» он убеждает Вас в необходимости срочной продажи по различным причинам. Просит перевести задаток, ссылаясь на свое отсутствие в городе, отсутствие знакомых и родственников, которым он мог поручить участие в сделке, торопит с принятием решения. При этом общение продавца с покупателем происходит не по телефону, а через мессенджеры «Вайбер», «Вотсап», «Телеграм».

Ситуация

Молодая женщина в сети Интернет нашла объявление о сдаче квартир в аренду. Квартира ее устроила и девушка позвонила по указанному номеру. Во время разговора мужчина, который представился сотрудником агентства недвижимости, перед осмотром квартиры потребовал предоплату. Потерпевшая согласилась и перевела 3000 рублей на указанный мошенником счет, после чего, приедя по адресу сдаваемой квартиры, девушка узнала, что данная квартира не сдается. Мнимый сотрудник агентства перестал выходить на связь.

Что делать?

Будьте осторожными при аренде жилья. Убедитесь, что данная квартира действительно сдается, оформите сделку документально при личной встрече с риелтором и только после этого оплачивайте услугу.

Если вы все-таки стали жертвой мошенников, немедленно сообщите об этом в полицию, позвонив по телефону 02, либо по телефону дежурной части 8 (3452) 291-600.



ПАМЯТКА



Управление
МВД России
по Тюменской
области

Совет при Тюменской
областной Думе
по повышению
правовой культуры
и юридической
грамотности населения
Тюменской области

ПО ПРОТИВОДЕЙСТВИЮ
МОШЕННИЧЕСТВУ В СФЕРЕ
П-ТЕХНОЛОГИЙ

Тюмень
2021 год

СПОСОБЫ И СХЕМЫ МОШЕННИЧЕСТВА

1. Мошенники выдают себя за сотрудников банка

Мошенники звонят, представляются сотрудниками банка и интересуются у граждан, оформили ли они заявку на получение кредита. При получении отрицательного ответа злоумышленник сообщает, что мошенники пытаются воспользоваться личными данными клиента банка и, таким образом, незаконно оформить онлайн-кредит.

Злоумышленник убеждает гражданина самому воспользоваться данной заявкой и оформить кредит, после чего сразу же закрыть его. Не убедившись в достоверности информации, гражданин оформляет денежный заем лично через банк или онлайн-способом и под ликвиду мошенника переводит денежные средства на неизвестный счёт, думая, что закрывает полученный кредит.

На номер телефона поступает звонок от якобы сотрудника банка, который утверждает, что на паспортные данные гражданина оформлен несанкционированный кредит и для того чтобы сохранить денежные средства, нужно назвать данные своей карты, в том числе СУС-код, коды безопасности, затем снять наличность со своей карты и перевести на «безопасный» счет. Аналогичная схема «под контролем мошенников» действует и при проведении операций по обеспечению сохранности собственных денежных средств, находящихся на счетах граждан.

Ситуация

На сотовый телефон поступает звонок от неизвестных, которые представляются сотрудниками банка. Женщины, которые пояснили, что на имя гражданина без его ведома одобрены кредиты и если он не вмешается, то эти денежные средства будут перечислены на счета мошенников.

Для усыпления бдительности граждан мошенники в звонках потерпевшим и уверяют их в достоверности происходящего, убеждении в том, что будут возбуждены и расследованы уголовные дела, для чего потерпевшему необходимо оказывать содействие полиции и банку.

Далее злоумышленники сообщают, что для исключения перевода кредитных денежных средств на счета мошенников гражданину необходимо проехать в отделение банка, оформить реальный кредит и забрать деньги. При этом, используя психологические уловки и фактор внезапности, мошенники внушают, что гражданин «никому и ни при каких обстоятельствах не должен рассказывать о происшедшем, даже самым близким родственникам», так как все строго конфиденциально и разглашение этой информации может повлечь невозможность пресечения преступления, дальнейшее аннулирование кредита и возврата банку денежных средств.

Находясь в стрессовой ситуации, выполняя инструкции преступников, потерпевший через банкомат переводит деньги на указанные счета, после чего теряет свои денежные средства.

Что делать?

В любой ситуации не теряйте самообладания и не принимайте в первые же минуты быстрых и необдуманных решений.

В случае, если вам позвонили и представились сотрудником банка, удостоверьтесь в личности сотрудника банка – для этого уточните у него представительство банка, в котором он работает, его местонахождение и иные данные, которые могут быть Вами проверены – этот способ работает – мошенники тут же прекращают разговор.

Либо сами прекратите разговор и сами перезвоните на «горячую линию» банка, набрав номер телефона банка вручную.

2. Мошенничество при совершении онлайн-покупок в сети Интернет

Ситуация 1

Мужчина нашел в сети Интернет частное объявление о продаже коробки передач для снегохода. Созвонившись с продавцом и обсудив условия покупки и доставки товара, мужчина перечислил на счет лжеиздавца денежные средства. После совершения перевода денежных средств продавец перестал выходить на связь.

Ситуация 2

Две женщины заказали товар на сайтах в сети Интернет. В качестве способа оплаты женщины выбрали наложенный платеж. Одна гражданина оплатила кипор стоимостью четыреста тысяч рублей, но получила посылку

с детской шапкой. Другая хотела приобрести шапль за пять тысяч рублей, но, вскрыв пакет, обнаружила в нем шарф. Стоимость полученных женшинами вещей оказалась значительно ниже установленных ими сумм.

Ситуация 3

Гражданин решил заказать пластиковые окна в одной из фирм города. Набрал в поисковой строке браузера интересующую информацию и, получив результат, перешел по ссылке. На сайте оформил заказ и осуществил оплату товара путем онлайн-оплаты. В назначенный день доставки товар гражданину поставлен не был. Когда он связался с представителями фирмы, последние пояснили, что никакого заказа от его имени не принимали и денежные средства на счет их фирмы не перечислялись.

Что делать?

Будьте бдительными при совершении покупок в сети Интернет. Помните об основных мерах безопасности при купле-продаже товаров по объявлению:

- не перечисляйте предоплату при покупке товаров в незнакомых интернет-магазинах, на сайтах, где размещаются частные объявления, таких как «Авито», «Юла» и т.д., расплачивайтесь только при личной встрече после осмотра товара. Помните, что при выборе непроверенного магазина даже оплата товара наложенным платежом не всегда является гарантией того, что содержимое посылки будет соответствовать ожиданию заказчика;
- в любой сомнительной ситуации (низкая цена, срочная сделка, отказ от личной встречи, необходимость предоплаты, дистанционная продажа из другого региона) откажитесь от сделки;
- прежде чем оформить заказ, выясните как можно больше информации о магазине, ознакомьтесь с отзывами других покупателей.

