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 – для того чтобы удостовериться в личности сотрудника банка, 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 вы прекратите разговор и перезвоните на «горячую линию» банка.

Мошенничество при совершении онлайн-покупок в сети Интернет

Жертвой может стать как человек, желающий приобрести товар, так и человек, желающий продать. В первом случае потерпевший находит объявление об интересующем его товаре и связывается с автором. Человеку сообщают, что предложение о продаже в силе и просят внести предоплату. Когда заявитель соглашается и переводит деньги, оппонент перестает выходить на связь.

В ситуации, когда потерпевший публикует объявление о продаже, с ним связывается мошенник и просит реквизиты для внесения предоплаты. Затем злоумышленник под различными предлогами узнает данные банковской карты, после чего списывает со счета потерпевшего все имеющиеся средства.

Размещение не соответствующих действительности объявлений в сети Интернет

Ситуация

В сети Интернет размещается объявление о сдаче квартиры в аренду. Когда вы позвоните по указанному в объявлении номеру телефона с целью договориться о просмотре, как правило, неизвестные, представляясь сотрудниками агентства недвижимости, просят перед осмотром квартиры произвести предоплату. Потерпевший, соглашаясь с условиями, переводит на указанный мошенником счет денежные средства. После этого, придя по адресу сдаваемой квартиры, потерпевшие узнают, что данная квартира не сдается. Мнимый сотрудник агентства перестает выходить на связь.

Что делать?

Будьте осторожными при аренде жилья. Убедитесь, что данное жилье действительно сдается, оформите сделку документально при личной встрече с риэлтором и только после этого оплачивайте услугу.

Особый признак размещенного не соответствующего действительности объявления о продаже (аренде) жилья – это существенно заниженная цена.

При контакте с «владельцем» недвижимости он убеждает вас в необходимости срочной продажи недвижимости по различным причинам. Просит перевести задаток за квартиру, 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-мошенника и покупателя происходит не по телефону, а через мессенджеры «Viber», «WhatsApp» и «Telegramm».

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.

УМВД России по Тюменской области

625000, г. Тюмень, ул. Водопроводная, 38,

тел. 8 (3452) 793-023 или 102,
тел. 8 (3452) 793-023 или 102
(для абонентов мобильной связи).

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

УМВД России по Тюменской области

ПАМЯТКА

ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

г. Тюмень, 2024

ИСПОЛЬЗУЮТСЯ СЛЕДУЮЩИЕ СПОСОБЫ И СХЕМЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

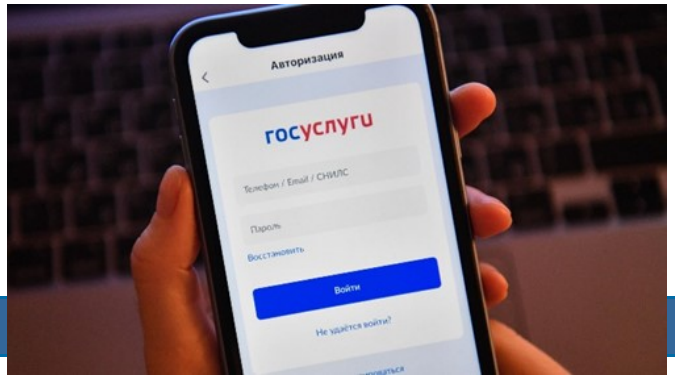
Мошенники на госуслугах

Мошенники звонят под видом сотрудников госуслуг и сообщают, что ваш аккаунт кто-то пытался взломать. В качестве меры предосторожности они просят назвать код из SMS, чтобы «помочь защитить аккаунт». На самом деле мошенники в этот момент отправляют заявку на восстановление пароля и после того как вы назовете код, они получат доступ к вашему личному кабинету.

Что может сделать мошенник, получив доступ к вашему кабинету?

1. Получить доступ к вашему мобильному банку.
2. Получить данные о банковских картах.
3. Зарегистрировать на ваше имя фиктивную фирму.
4. Продать ваши данные в даркнете. Стоимость персональной информации постоянно растет.
5. Взять кредит в микрофинансовой организации.

- Если вас уже взломали, звоните в полицию и блокируйте свои карты.
- Если вам будут звонить мошенники, сразу кладите трубку и меняйте пароль и поставьте двойную аутентификацию.



Мошенники в мессенджерах

От имени знакомых с использованием аккаунтов в «WhatsApp» и «Telegramm» рассылается всем имеющимся контактам текст с просьбой проголосовать за ребенка, при этом прикрепляется ссылка, по которой необходимо пройти для голосования. Злоумышленники получают доступ к аккаунтам «WhatsApp», «Telegramm», используя вредоносную ссылку, и после прохождения гражданами по данной ссылке получают доступ к их учетной записи в мессенджере.

В этой связи полиция **предупреждает и призывает** граждан не переходить по сомнительным ссылкам, которые тиражируются, как правило, в виде розыгрыша призов, голосования за детей, опросника по любым темам, и не вводить свои личные данные.

Если вы подозреваете, что все-таки случайно прошли по подозрительной ссылке, можете проверить наличие параллельного доступа «к вашему» аккаунту, **зайдя в приложение «Настройки» и перейдя во вкладку «Привязанные устройства».** Если в данной вкладке отобразится неизвестное устройство, которое вы не привязывали, немедленно осуществите выход из данной сессии.

Ситуация: «Ваш родственник попал в ДТП»

Мошенники звонят под видом адвокатов или сотрудников правоохранительных органов. Потерпевшему рассказывают, что кто-то из его близких спровоцировал ДТП с пострадавшими и для урегулирования проблемы необходимо передать крупную денежную сумму. Когда человек соглашается, к нему направляют курьера за наличными денежными средствами. До его приезда мошенники требуют оставаться с ними на связи и запрещают звонить кому-либо из родственников.

Ситуация: «Звонок от сотрудника банка»

На сотовый телефон поступает звонок от неизвестного, который представляется сотрудником кредитной организации. Лже-сотрудник поясняет, что средствами собеседника пытаются завладеть неизвестные. Далее мошенники либо под различными предлогами узнают данные банковской карты жертвы и переводят все имеющиеся денежные средства, либо убеждают взять кредит и перевести деньги по указанным преступниками реквизитам или на безопасный счет. Нередко мошенники сначала похищают накопления с банковского счета, а затем убеждают взять кредит либо продать имущество.

Для усыпления бдительности граждан мошенники «разыгрывают» данную схему с участием лже-сотрудников полиции. Роль таких лже-полицейских заключается в звонках потерпевшим и уверении их в достоверности происходящего, убеждении в том, что будут возбуждены и расследованы уголовные дела, для чего потерпевшему необходимо оказывать содействие полиции и банку.

Используя психологические уловки и фактор внезапности, мошенники внушают, что вы никому и ни при каких обстоятельствах не должны рассказать о произошедшем, 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 денежные средства на счет, озвученный мошенником, после чего теряет свои денежные средства.