

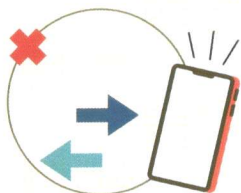


Осторожно мошенники:

Выигрыш в лотерее или приза



В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют это для своей деятельности и обмана людей. На Ваш мобильный телефон, как правило, в ночное время — приходит SMS-сообщения, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из вышеуказанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного денежную сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки и получения «кода регистрации».



ВАШИ ДЕЙСТВИЯ

Никогда и ни под каким предлогом не переходить по ссылкам, направляемым Вам незнакомыми лицами и не вводите данные своей банковской карты на сомнительных сайтах. Не переводить на незнакомые номера телефонов денежные средства.

В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ



Звоните по телефонам:

горячей линии МВД 8-800-222-74-47 (112),

УВД по ЮАО 8-499-320-55-17,

или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.



Лжеинвестиции:

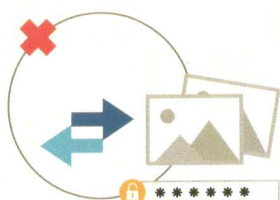
Поддельные котировки и кража через «комиссии»



Вам поступает звонок от «финансового консультанта», ссылается на партнерство с банком или крупной компанией и предлагает открыть инвестиционный счет — для старта достаточно небольшой суммы. А чтобы все оформить, нужно перейти по ссылке на сайт, который внешне напоминает известный брокерский сервис. После пополнения в личном кабинете отображаются вымышленные сделки и растущий баланс. Пока человек наблюдает за «прибылью», все выглядит убедительно.

Когда пользователь решает вывести деньги, то появляются дополнительные условия:

- Оплатить комиссию за вывод
- Внести депозит для «подтверждения статуса»
- Оплатить страховку или налоги заранее



ВАШИ ДЕЙСТВИЯ

Не переходите по ссылкам на неофициальные сайты, которые предлагают быстрый заработок, не сообщайте личные данные и не вносите предоплат. Будьте бдительны и осторожны, посещая подозрительные страницы в интернете!



В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ

Звоните по телефонам:

горячей линии МВД 8-800-222-74-47 (112),

УВД по ЮАО 8-499-320-55-17,

или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.



Маркетплейсы:

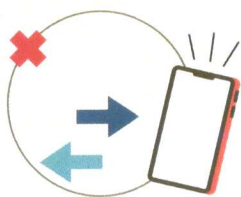
Фейковые блокировки и смена реквизитов продавца



Еще одна рабочая схема — атаки на продавцов маркетплейсов. Продавцу приходит письмо или сообщение: «Ваш аккаунт заблокирован за нарушение правил. Для продолжения работы подтвердите данные». Внутри — ссылка на «форму проверки», визуально копирующую интерфейс площадки. В действительности это поддельные сайты, как в предыдущей схеме. Если пользователь вводит логин и пароль, доступ к кабинету уходит злоумышленникам.

Дальше возможны несколько вариантов:

- Смена реквизитов для выплат — деньги от реальных заказов начинают уходить на счет мошенников
- Оформление кредитов или рассрочек на продавца под видом «финансирования закупки»
- Кроме того, аккаунт могут использовать для обмана покупателей. Например, разместить выгодное предложение и получать оплату за заказы, не отправляя товар



ВАШИ ДЕЙСТВИЯ

Игнорируйте подозрительные сообщения, поступающие с неизвестных номеров и не переходите по ссылкам.



В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ

Звоните по телефонам:

горячей линии МВД 8-800-222-74-47 (112),

УВД по ЮАО 8-499-320-55-17,

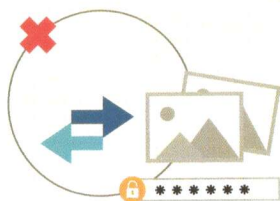
или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.



Мошенничество под предлогом инвестирования в различные криптобиржи, криптовалюты, акции



Граждане находят в сети Интернет различные «зарубежные» финансовые организации, которые предлагают под их управлением инвестировать деньги в валюту, крипто-валюту, акции, металлы, биржевые товары и т.п., обещая при этом доходы, существенно превышающие действительные биржевые курсы. Злоумышленники просят установить приложение, скачанное с их сайта, на котором отображаются биржевые котировки, создать личный кабинет и специальный счет для участия в торгах. Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с телефона.



ВАШИ ДЕЙСТВИЯ

Не открывайте неизвестные файлы, проигнорируйте сообщение, не заходите на сомнительные и непроверенные файлы.

В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ



Звоните по телефонам:

горячей линии МВД 8-800-222-74-47 (112),

УВД по ЮАО 8-499-320-55-17,

или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.

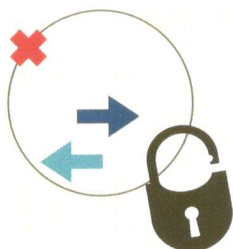


Осторожно мошенники:

Поддельные службы доставки



В этом сценарии мошенники притворяются специалистами известных служб доставки: СДЭК, Яндекс Доставка, Сбермаркет, Delivery Club. Они пишут людям в мессенджерах с поддельных аккаунтов этих сервисов, которые похожи на реальные: мошенники используют такие же логотипы, описания и названия, стилистику общения. Люди получают сообщения примерно такого содержания: «Ваш заказ готов к доставке, подтвердите адрес» или «Для выдачи посылки оплатите хранение/доплату за вес». Более изощренный вариант схемы — к человеку приезжает реальный курьер с коробкой и QR-кодом для оплаты или подтверждения заказа. Получатель сканирует код, попадает на такой же фальшивый сайт и вводит реквизиты карты, включая секретные данные.



ВАШИ ДЕЙСТВИЯ

Игнорируйте сообщения, которые поступают в мессенджерах от представителей служб доставки. Откройте официальное приложение и свяжитесь с поддержкой, чтобы уточнить информацию по заказу.

В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ



Звоните по телефонам:
горячей линии МВД 8-800-222-74-47 (112),
УВД по ЮАО 8-499-320-55-17,
или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.

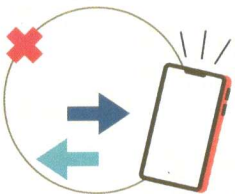


Осторожно мошенники:

Предложение получить доступ к смс-переписке и звонкам абонента



Учитывая склонность некоторых граждан «пошпионить» за близкими и знакомыми, злоумышленниками используется следующая схема мошенничества в сети Интернет: пользователю предлагается изучить содержание смс-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 рублей на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента. После того, как пользователь отправляет смс, с его счета списывается сумма гораздо больше той, что была указана мошенниками, а интересующая информация впоследствии так и не поступает.



ВАШИ ДЕЙСТВИЯ

Не переводите на незнакомые номера телефонов денежные средства и не вносите предоплат.



В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ

Звоните по телефонам:
горячей линии МВД 8-800-222-74-47 (112),
УВД по ЮАО 8-499-320-55-17,
или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.



Осторожно мошенники:

Сбрось мне свою геолокацию

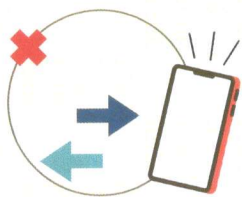


Сценарий начинается безобидно: переписка в боте знакомств. Дальше собеседник предлагает перейти в мессенджер и «запланировать встречу». После непродолжительной переписки звучит просьба: *«Скинь геолокацию какого-нибудь известного места в твоём районе — так проще понять, где нам назначить встречу»*. Как только геометка отправлена, мошенник переходит к следующему этапу плана. На телефон приходит видеофайл.

В ролике человек сообщает, что по указанным координатам могут проводиться незаконные действия. Видео снято так, чтобы создать ощущение реальности происходящего.

Затем поступает звонок якобы от сотрудника спецслужб. Он сообщает, что передача координат важного городского объекта может трактоваться как помощь в организации теракта, и начинает угрожать уголовной ответственностью за отправку геопозиции. Дальше, чтобы «избежать проблем», человеку предлагают «доказать свою лояльность» и «помочь» правоохранительным органам:

- Показать на камеру квартиру
- Открыть банковские приложения — свои и родителей — и перевести либо снять со счета деньги
- Найти дома наличные и украшения, подготовить их для «изъятия» — и передать курьеру (им оказывается один из мошенников, который играет роль «сотрудника полиции в штатском»).



ВАШИ ДЕЙСТВИЯ

Не переписывайтесь с людьми на сомнительных и неизвестных сайтах. Если получили смс с незнакомого номера, не открывайте сообщение. При открытии сомнительных видеороликов или фотографий, сохраняйте спокойствие и обратитесь в правоохранительные органы для выяснения ситуации.

В СЛУЧАЕ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ



Звоните по телефонам:

горячей линии МВД 8-800-222-74-47 (112),

УВД по ЮАО 8-499-320-55-17,

или по телефону ОМВД по месту жительства. Оставьте заявление на сайте МВД или в Отдел полиции по месту жительства. Когда дежурный в Отделе полиции примет заявление, он выдаст Вам талон-уведомление.