

Аферисты постоянно находят новые способы украсть деньги или личные данные. Но какими бы хитрыми ни были схемы, есть признаки, по которым их легко разоблачить.



КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА!

1. НА ВАС ВЫХОДЯТ ПЕРВЫМИ

У мошенников много личин. Помните, что инициатору контакта всегда от вас что-то нужно.

2. ВАС ВЫВОДЯТ ИЗ РАВНОВЕСИЯ

Радуют или пугают, чтобы сбить вас с толку и притупить бдительность.

3. ВАС ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Преступников интересуют коды из СМС, пуш-уведомлений, данных банковской карты, персональные данные.

4. ВАС ТОРОПЯТ

Преступникам важно, чтобы вы действовали импульсивно.

5. ВАШИ ВОПРОСЫ ИГНОРИРУЮТ

Мошенник будет стараться следовать своему сценарию.

ВНИМАНИЕ! *Кладите трубку в разговоре с незнакомцем, если распознаете хотя бы два из этих признака. Помните, что цель любой схемы мошенников – получить от жертвы сведения, достаточные для доступа к ее деньгам.*
БУДЬТЕ ВНИМАТЕЛЬНЫ И ОСТОРОЖНЫ!

ТОП-5 САМЫХ АКТУАЛЬНЫХ СХЕМ ТЕЛЕФОННЫХ МОШЕННИКОВ

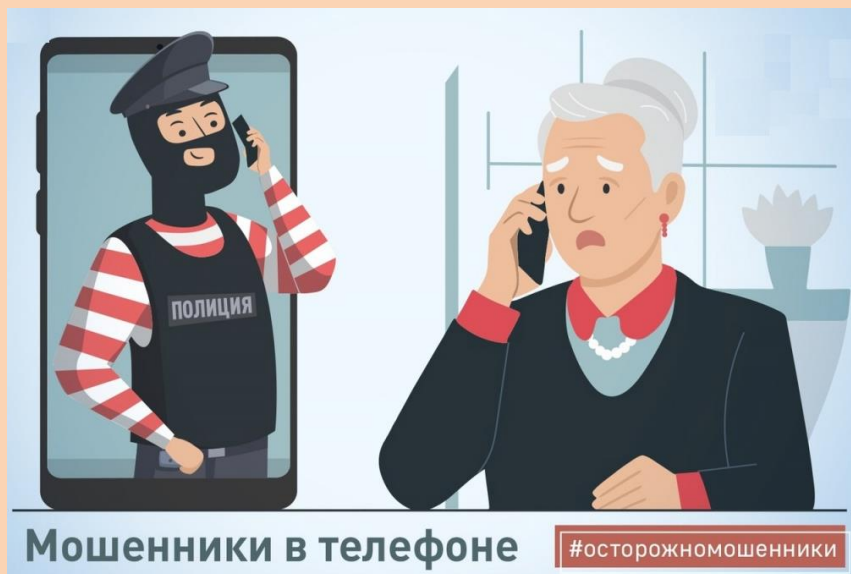


СХЕМА 1. Меняем медицинский полис!

Мошенник под видом сотрудника страховой компании сообщает, что у вас истек срок действия медицинского полиса. Документ нужно заменить. Для этого назовите код из смс, который придет на телефон.

Работники страховых компаний не просят устанавливать приложения или называть им коды из смс и данные. А медицинский полис действует бессрочно, и его не нужно менять.

СХЕМА 2. Вам цветы, примите доставку!

Мошенник под видом курьерской службы сообщает, что вам отправили букет, уточняет, куда и когда его привезти. После получения букета курьер просит назвать код из смс, чтобы подтвердить доставку заказа.

Курьерские службы не просят коды из смс для подтверждения доставки. Свяжитесь с отправителем подарка и уточните детали. Если это сделать не удастся – не принимайте презент.

СХЕМА 3. Получите письмо!

Мошенник под видом сотрудника «Почты России» сообщает, что вам пришла посылка/заказное письмо. Для его получения надо воспользоваться несуществующим чат-ботом и ввести код из смс.

Сотрудники «Почты России» никогда не звонят клиентам и не запрашивают код из смс. Вы можете самостоятельно подключить или отказаться от услуг сервиса на его официальном сайте или в приложении.

СХЕМА 4. Заканчивается договор сотовой связи

Мошенник под видом оператора сотовой связи сообщает, что у вас заканчивается контракт на мобильную связь. Его нужно продлить, иначе вы не сможете звонить, отправлять смс и пр. это можно сделать через «Госуслуги» просто продиктуйте код

СХЕМА 5. Зафиксирована подозрительная операция по вашей карте!

Мошенник под видом сотрудника банка сообщает, что по вашей карте зафиксирован подозрительный перевод или кто-то пытается оформить кредит на ваше имя. Для отмены этих финансовых операций вы должны назвать код из смс,

из смс.

Сотрудники оператора могут отключить связь, если вы не оплачиваете услуги или ваши персональные данные, указанные в договоре, необходимо актуализировать. Но это произойдет не сразу. Вы можете обновить данные не только через «Госуслуги», но в салоне связи.

который направит специалист.

Сотрудники банков, правоохранительных органов и государственных ведомств не звонят гражданам и не запрашивают у них персональные данные, коды из сообщений. Положите трубку и позвоните в организацию, по номеру с ее официального сайта.

БУДЬТЕ БДИТЕЛЬНЫ! Если вас просят назвать код из смс, не поддавайтесь на уговоры. Мошенники могут придумывать разные предлоги, чтобы выманить его. Этот код дает доступ к вашим персональным данным и банковским счетам.

И ЕЩЕ ТОП-5 ИНТЕРНЕТ-СХЕМ МОШЕННИКОВ



СХЕМА 1

Вам открытка!

Мошенники маскируют вредоносный код под открытку или картинку и рассылают ее по электронной почте. При нажатии на них пользователь скачивает на гаджет вирусную программу, которая похищает его персональные данные

Не доверяйте сообщениям от неизвестных людей. Если вы знаете отправителя, с настороженностью относитесь к нестандартным сообщениям, в том числе с

СХЕМА 2

Очень выгодное предложение!

Мошенники подделывают сайт маркетплейса и присылают пользователю на почту электронное письмо с промокодом на определенную сумму. Для его получения нужно перейти на сайт, там добавить товары в корзину, ввести реквизиты банковской карты, а подаренная сумма якобы зачтется.

Не переходите по ссылкам из электронных писем. Проверяйте акции,

вложением фото или картинки без предпросмотра. Уточните у него через другой способ связи, что во вложении.

СХЕМА 3

Инвестиционный проект с высоким доходом

Лжеброкеры рассылают письма на электронную почту с рекламой крупного инвестиционного проекта. При минимальных вложениях они обещают высокий доход в ближайшее время.

Не верьте обещаниям про легкое и быстрое обогащение! Прежде чем вложить деньги в такой проект, соберите информацию о нем, прочитайте отзывы, уточните контакты брокерской компании.

промокоды и другую информацию на официальном сайте интернет-магазинов.

СХЕМА 4

Предлагаем работу!

Мошенники публикуют объявления об удаленной работе. Условия привлекательные, зарплата высокая. Они предлагают человеку оформить банковскую карту на свое имя и передать курьеру, получить деньги на собственную карту, часть передать доверенному лицу или перевести кому-то, а вознаграждение оставить себе или стать администратором лотереи и рассылать победителям выигрыши.

Подобные предложения – замаскированная схема дропперства.

Не соглашайтесь на сомнительные предложения о легком заработке. Помните, что, участвуя в такой схеме, вы становитесь участником преступления и несете уголовную ответственность.

СХЕМА 5

Получите выплату!

Мошенники под видом специалиста портала «Госуслуги» или СФР рассылают письма на электронную почту и сообщают пользователю о назначении дополнительной выплаты. Для ее получения необходимо перейти по ссылке, ввести паспортные данные и указать реквизиты банковской карты, на которую переведут деньги.

Внимательно проверяйте адрес отправителя электронного письма. Помните, что информация о выплатах и льготах отображается в личном кабинете на «Госуслугах». Не переходите по ссылкам из подобных писем и не оставляйте свои данные на сомнительных ресурсах.

