ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

Осторожно сайты-дублеры «зеркальные сайты»

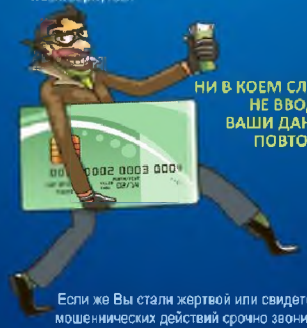
В Дагестане приобретают «популярность», так называемые, зеркальные сайты – когда злоумышленники в преступных целях используют сайт, адрес и внешнее оформление которого идентичны официальной торговой интернет-площадке.

Новая схема мошенничества состоит в том, что после размещения гражданином сообщения о продаже товара, злоумышленники связываются с продавцом через номер указанный в объявлении.

Пообщавшись и войдя в доверие, мошенники пересылают жертве ссылку на липовый сайт, где продавец должен зарегистрироваться, введя свои личные данные и данные банковской карты, на которую впоследствии якобы будет осуществлен перевод оплаты за товар.

Как только потерпевший вводит все указанные данные с его счета автоматически списываются денежные средства

Чтоб не стать жертвой «зеркального сайта» полицейские рекомендуют быть бдительными при онлайн продаже товаров и придерживаться простых правил: - первым «тревожным звоночком» при данной схеме мошенничества является то, что лже-покупатель требует общение через сторонние мессенджеры, хотя все современные торговые площадки дают возможность обсуждать сделку непосредственно на сайте;- адрес сайта, ссылку на который прислал злоумышленник, очень схож с официальным адресом торговой площадки, но всё же, при должном внимании можно заметить расхождения (дополнительные буквы, символы, цифры); - если вы всё же прошли по ссылке и ввели данные банковской карты, в следствии чего с вашего счета произошло списание денежных средств, не видитесь на уловку мошенников о том, что произошла техническая ошибка и деньги скоро к вам вернуться



НИ В КОЕМ СЛУЧАЕ НЕ ВВОДИТЕ ВАШИ ДАННЫЕ ПОВТОРНО!

Если же Вы стали жертвой или свидетелем мошеннических действий срочно звоните на телефон горячей линии МВД по РД

☎102/02

☎102/02

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ ПО РЕСПУБЛИКЕ ДАГЕСТАН ПРЕДУПРЕЖДАЕТ!

ВНИМАНИЕ!

ИНТЕРНЕТ МОШЕННИКИ

Как мошенники вводят в заблуждение посредством интернет магазинов и торговых интернет-площадок ?

Распространенный способ совершения хищении денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

ВНИМАНИЕ ЛОХОТРОН

Распространенный способ совершения хищении денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

-Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платёжных систем.

Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности.

Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные.

Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

СЛЕДУЕТ ПОМНИТЬ!

Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные.

Сотрудник банка может запросить у клиента только контрольное слово, ФИО.

При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом.

Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

-При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Вам начислены бонусы:
мошенники представляются сотрудниками ПАО «Сбербанк» сообщая потенциальной жертве приятную новость, но для зачисления бонусных баллов в денежном эквиваленте требуют сообщить им CVC-код банковской карты (трехзначный код с оборотной стороны) и пароли, поступившие в смс-сообщениях с сервисного номера.

Служба безопасности банка:
звонивший сообщает о том, что по Вашему банковскому счету пытаются оформить кредит и похитить денежные средства. Для предотвращения данных действий, мошенники просят перечислить хранящиеся на Вашем счете денежные средства на более безопасный счет, что бы Вы поверили им, они используя программное обеспечение направляют смс-сообщение на Ваш абонентский номер с номера «900». Таким же способом совершают звонки с абонентских номеров схожих с номерами банковских организаций.

Вам положена компенсация:
Интернет пространстве можно получить любую информацию, также о том на каких сайтах Вы заказывали тот или иной товар. Звонивший представляется сотрудником органов внутренних дел и сообщает, что по судебному решению Вам положена выплата за приобретенный лекарственный препарат (медицинский аппарат), но для получения выплаты требуют перечислить определенную сумму денежных средств в счет судебных издержек.

Быстрый заработок на биржевых платформах: предлагают установить биржевую платформу, посредством которой проводить торги и получать прибыль.

Вы периодически перечисляете разные суммы денежных средств, наблюдая за прибылью через приложение и предполагая, что они хранятся на Вашем «биржевом» счете, а на самом деле денежные средства уходят на счет мошенников и вывести их уже невозможно.

Если же Вы стали жертвой или свидетелем мошеннических действий срочно звоните на телефон горячей линии МВД по РД

☎102/02

☎102/02

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ ПО РЕСПУБЛИКЕ ДАГЕСТАН ПРЕДУПРЕЖДАЕТ!

ВНИМАНИЕ!

ТЕЛЕФОННЫЕ МОШЕННИКИ

Вам звонят из банка ?!
Как телефонные мошенники воруют деньги со счетов граждан

Осторожно сайты-дублеры «зеркальные сайты»

Мошенники создают сайты-клоны торговых площадок с отличной репутацией (копируют интерфейс оригинального сайта), с небольшим отличием в доменном имени сайта, Вы отдаете деньги мошенникам, думая, что покупаете товар.

Производите покупки и продажи товаров строго в пространстве официального сайта торговой интернет-площадки. Не в коем случае не переходите по сторонним ссылкам!

ЭТО МОШЕННИКИ!

«Вам положена компенсация»

Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы, либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

ЭТО МОШЕННИКИ!

Звонок либо сообщение

о несчастном случае Просьба перевести какую-либо сумму от Вашего знакомого, аккаунт которого был взломан это мошенники!

Прервите разговор (переписку) и позвоните ему лично

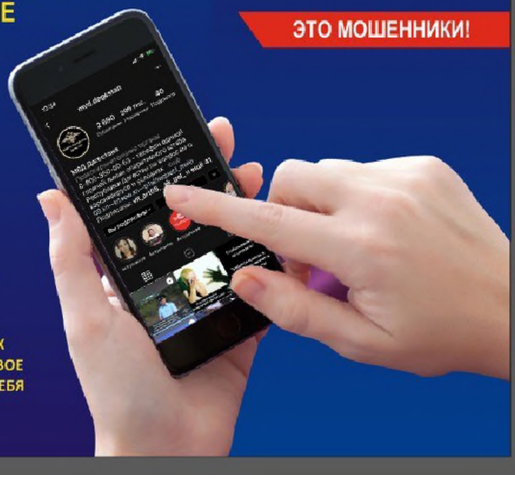
ЭТО МОШЕННИКИ!

МВД ПО РЕСПУБЛИКЕ ДАГЕСТАН ПРЕДУПРЕЖДАЕТ ОСТОРОЖНО! ДИСТАНЦИОННЫЕ МОШЕННИКИ!

102/02

mvd.dagestan

ПРЕДУПРЕДИТЕ РОДНЫХ И ДРУЗЕЙ О МОШЕННИКАХ И ИХ СХЕМАХ! БЕРЕГИТЕ СВОЕ ИМУЩЕСТВО! НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!



«Онлайн покупки»

Якобы продавец просит за товар предоплату, либо полную оплату покупки, после чего связь с мошенником прекращается

Не производите предоплату непроверенным (незнакомым) лицам! Мошенники создают собственные интернет-магазины как правило товарами по цене существенно ниже среднерыночной, либо с большими скидками.

ЭТО МОШЕННИКИ!

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категории товаров по ценам значительно НИЖЕ, чем среднерыночная цена.

ЗЛОУМЫШЛЕННИКИ:

Создают сайт интернет-магазина и запускают рекламный трафик с целью появления в топе поисковых систем.

Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина.

Требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен.

После перевода денежных средств покупателем перестают выходить на связь, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

Неоправданно низкая цена на товар.

Электронная почта или мессенджеры в качестве способов коммуникации.

Оплата без расчетного, банковского счета, отсутствие наименования организации в любой из форм собственности.

Обязательная предоплата, зачастую более половины стоимости товара.

Отсутствие физического адреса расположения магазина или его несоответствие данным интерактивных карт.

ЗАПОМНИТЕ!

Необходимо выбирать магазин, предлагающий забрать товар самовывозом. При необходимости закажите доставку товара;

Самый безопасный способ оплаты - после получения заказа;

Критично относитесь к ситуации, когда менеджер интернет-сайта проявляет излишнюю настойчивость или просит немедленно оплатить заказ под различными предлогами (акционный товар, последний экземпляр, ожидается подорожание продуктовой линейки

На сегодняшний день почти у каждого из нас есть свой личный аккаунт в социальных сетях. В связи с отсутствием достаточной его зашиты, учащаются случаи взлома аккаунтов социальных сетей жителей Республики Дагестан.

ЗЛОУМЫШЛЕННИКИ:

Создают аккаунт, являющийся точной копией оригинального (аккаунт-клон).

Выставляют статус от имени хозяина оригинального аккаунта, с просьбой финансовой помощи, а так же рассылают сообщения подобного характера всему списку друзей.

ЗАПОМНИТЕ!

- Прежде чем помочь какой-либо товарищу из списка ваших друзей.
- Позвоните ему на мобильный телефон.
- В случае отсутствия мобильного телефона, произведите обзвон Ваших общих знакомых, с целью выяснения проблемы происшедшей с ним
- Произведите поиск ранних диалогов с данным лицом.
- Не проверив достоверность данной просьбы, не осуществляйте перевод денежных средств на карточный счет.