

Осторожно сайты-дублиеры «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, ввести 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 общения 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 видясь 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?

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:

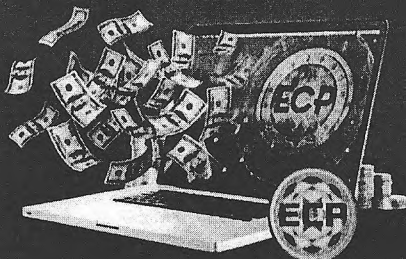
звонивший сообщает о том, что по Вашему банковскому счету пытаются оформить кредит и похитить денежные средства. Для предотвращения данных действий, мошенники просят перечислить хранящиеся на Вашем счете денежные средства на более безопасный счет, что бы Вы поверили им, они используя программное обеспечение 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