



## **Следственное управление СК России по Республике Дагестан призывает граждан быть внимательными и не дать обмануть себя Интернет-мошенникам**



Стремительное развитие компьютерных технологий и сети Интернет упрощает гражданам процесс получения информации, оказания услуг, оформления документов, совершения покупок.

Вместе с тем, резко возросло количество киберпреступлений, связанных с хищением средств, информации или доступов к ней.

Наиболее распространенными видами мошенничества является осуществление телефонных звонков от якобы сотрудников банка с просьбой перевести деньги на защитный счет, чтобы их сохранить, сообщение о том, что ваша банковская карта заблокирована - предлагается



Официальный сайт  
Следственное управление  
Следственного комитета Российской Федерации  
по Республике Дагестан

---

бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

Другим способом является создание сайтов-клонов популярных интернет магазинов, целью которых является получение сведений о логинах и паролях пользователей, номерах их банковских карт. Такие сайты предлагают товары по заниженным ценам, контрафактные и некачественные, а во многих случаях деньги покупателей просто присваиваются, а товар не доставляется. Отличительной чертой таких сайтов является отсутствие телефонов, по которым можно связаться с продавцами, а также юридического адреса.

Мошенники также используют такой способ обмана, как сообщение о выигрыше в лотерею - злоумышленник представляется менеджером известной компании и сообщает, что клиент стал победителем розыгрыша. Для получения вознаграждения необходимо срочно выслать реквизиты своей банковской карты.

Чтобы не стать жертвой мошенников необходимо соблюдать правила «цифровой или компьютерной гигиены»:

- не доверяйте личные данные незнакомым лицам, откажитесь от сделки, если имеются сомнения в надежности покупателя (продавца);
- не следует звонить по номеру, с которого отправлен SMS – есть вероятность, что в этом случае с Вашего телефона будет автоматически снята сумма денежных средств;
- не используйте подозрительные Интернет-сайты;
- подключите Интернет-банк и СМС-оповещение;
- не сообщайте данные своей банковской карты другим лицам, в том числе банковским служащим, работникам интернет-магазинов (никто не вправе требовать ваш ПИН-код);
- при возможности откройте отдельную карту, на которой храните определенную сумму денежных средств для осуществления безналичных платежей.
- используйте специальные программы, устанавливаемые на смартфоны, которые определяют организацию, из которой исходит звонок, и предупреждают владельца телефона о нежелательности ответа.

Особое внимание необходимо обратить на цифровые покупки несовершеннолетних, которые осуществляют их, играя в компьютерные игры, приобретая различную игровую валюту,



Официальный сайт  
Следственное управление  
Следственного комитета Российской Федерации  
по Республике Дагестан

---

виртуальных персонажей компьютерных игр и т.д.

Если деньги были перечислены мошеннику через электронную платежную систему или банк, необходимо незамедлительно обратиться в службу поддержки клиентов этих организаций. Кроме того, подать жалобу на компьютерное мошенничество можно на сайте Роскомнадзора (государственный орган по надзору в сфере информационных технологий).

За мошенничество с использованием электронных средств платежа предусмотрена уголовная ответственность по статье 159.3 Уголовного кодекса Российской Федерации, санкция которой предусматривает наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы до десяти лет.

Также предусмотрена уголовная ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (статья 159.6 Уголовного кодекса Российской Федерации), за совершение которого предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы до десяти лет.

27 Мая 2021

Адрес страницы: <https://dagestan.sledcom.ru/news/item/1574372>