# Управление МВД России по г. Таганрогу предупреждает граждан о новом виде мошенничества!

В текущем году на территории Ростовской области участились случаи совершения хищений денежных средств с помощью программ удаленного доступа, таких как RustDesk, Zoom и другие. При совершении преступления злоумышленники, представляясь сотрудниками службы безопасности банка, звонят клиенту и сообщают, что необходимо произвести замену номера, прикрепленного к лицевому счету, для того чтобы предотвратить мошеннические действия. Далее они предлагают жертве установить на телефон вышеупомянутые приложения, которые позволяют дистанционно управлять мобильным телефоном и открывать приложения онлайн банков. Гражданину в смс-сообщении направляется код, злоумышленник просит его продиктовать и с этого момента гаджет жертвы находится под контролем обманщиков.

Мошенники не стоят на месте и активно следят за новыми технологиями – сейчаспреступники не спрашивают ваши персональные данные и даже данные банковских карт. Их цель – этообычные пользователи смартфонов, планшетов и компьютеров, в которых каждый из нас хранит всю важную для себя информацию.

Под видом защиты ваших денежных средств, они просят установить некое приложение или программу удаленного доступа, с помощью которого все сделают сами.

Вам поступает звонок якобы от представителя банка. «Сотрудник» сообщает, что в данный момент кто-то хочет войти в ваш мобильный банк и совершить транзакцию, а затем, убеждают вас войти в официальный магазин приложений PlayМаркет либо ApStore, чтобы скачать и установить программу «для удалённой помощи» - «RustDeskRemoteDesktop», чтобы «здесь и сейчас» СПАСТИ ВАС от несанкционированного снятия денег. Люди наивно устанавливают программноеобеспечение и теряют свои деньги.

После скачивания и установки подобных программ мошенники получают полный доступ ко всем данным своей жертвы (счетам, записной книжке и даже паролям от аккаунтов).

Все виды мошенничеств строятся прежде всего на доверии граждан. Совсем недавно мошенники еще не могли получить удаленный доступ к гаджету жертвы. Теперь же обманутых тысячи.

Как не стать жертвой мошенников?

Не устанавливайте по просьбе неизвестных программное обеспечение, в частности программы: «AnyDesk», «RustDesk», «RealVnk», «TeamViewer», «Zoom» идругие приложения, программы и «антивирусы» с похожими названиями.

Установка таких приложений и программ по просьбе звонящего, предоставит мошенникам полный доступ к телефонной книге, мобильным банкам и другим личным данным, которые хранятся в памяти ваших гаджетов.

Помните!

Подобный звонок должен настораживать. Банки не звонят своим клиентам с просьбой что-либо установить, никогда не настаивают на том, чтобы клиент продиктовал номер банковской карты. Если поступил такой звонок, перезвоните по официальному номеру (его можно узнать на официальном сайте банка или на оборотной стороне вашей банковской карты) и убедитесь в том, что Вам действительно звонит сотрудник банка. Если вы все же стали жертвой мошенников, незамедлительно обратитесь в полицию.

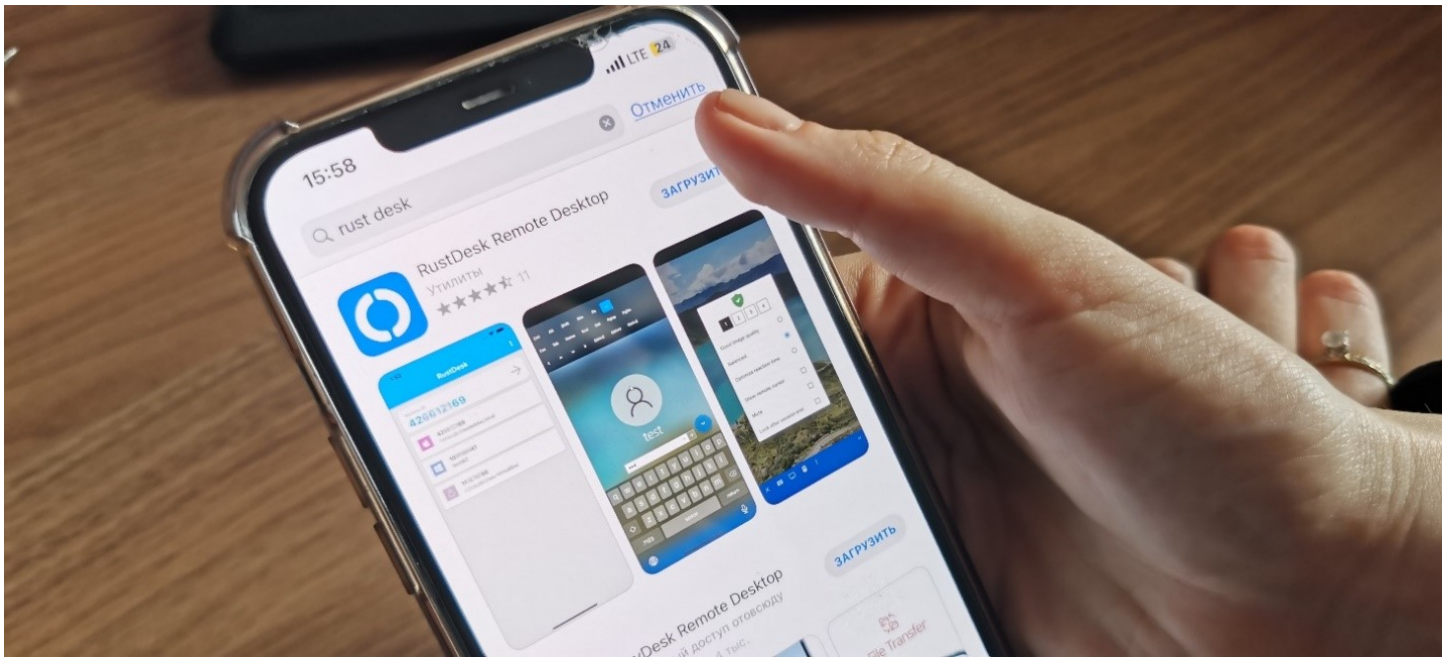
**Будьте бдительны!**

**Проведите разъяснительную беседу о том, как не стать жертвами мошенников со своими родственниками, особенно пожилого возраста.**

**Обо всех подозрительных лицах и звонках незамедлительно сообщайте по тел.: 02, 102, 112, 8(8634) 63-22-20**

**Адрес Управления МВД России по г. Таганрогу: ул. Александровская, 45, г. Таганрог, Ростовская область, 347900**

**Адрес электронной почты: taganrogovd61@mvd.ru.**




AnyDesk

TeamViewer

zoom

RUSTDESK
Your remote desktop

REALVNC