

Информация

о появлении новых и наиболее распространенных способах совершения дистанционных мошенничеств

В последнее время появились новые способы совершения дистанционных мошенничеств:

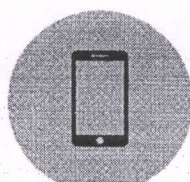
1. Мошенники под видом работников социальных служб звонят гражданам и сообщают о необходимости проверки подлинности имеющихся наличных денежных купюр. Для их проверки предлагается установить на мобильный телефон специальное приложение - «Банкноты Банка России», название которого совпадает с наименованием официально функционирующего приложения Центрального Банка Российской Федерации. Вместе с тем, злоумышленники дают ссылку на фальшивую программу, схожую по интерфейсу с официальным приложением. После установки такой программы мошенники получают удаленный доступ к телефону жертвы и, соответственно, к банковским приложениям, счетам, после чего похищают с них денежные средства.

2. Еще одним распространяющимся способом совершения киберпреступлений является так называемая «демонстрация экрана смартфона». На мобильные телефоны граждан поступают звонки от якобы сотрудника банка, с предложениями дополнительного заработка, оформления кредита. Далее мошенники настаивают продолжить разговор по видеосвязи, затем просят включить демонстрацию экрана смартфона, чтобы увидеть входящие уведомления на смартфоне. Это позволяет злоумышленникам изменить старый пароль входа в онлайн-банк и установить новый. В итоге злоумышленники получают доступ к мобильному банку жертвы и похищают денежные средства.

3. Мошенничество под предлогом оплаты товара по QR-коду (изображение, которое можно отсканировать современными средствами связи, чтобы получить доступ к интернет-сайту, приложению), через «Систему быстрых платежей» (сервис для совершения межбанковских переводов по номеру мобильного телефона).

Потенциальная жертва, заинтересовавшись каким-либо товаром, оставляет заявку на интернет-сайте, который на самом деле является фейковым (ложным, поддельным). Далее покупателю поступает звонок от якобы продавца магазина с подтверждением наличия товара, а также с предложением приобрести товар со скидкой при условии оплаты через «Систему быстрых платежей» по QR-коду. В случае согласия, злоумышленник отправляет ссылку на фишинговый (ложный, поддельный) сайт с формой оплаты по QR-коду. Как только покупатель совершает платеж с использованием QR-кода, деньги отправляются на счет злоумышленника.

Наиболее используемыми схемами дистанционных мошенничеств также остаются:



Посредством
подменной
телефонии



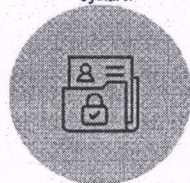
Под предлогом
инвестирования в ценные
бумаги



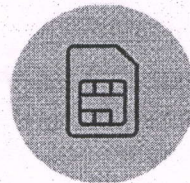
Под предлогом «Ваш
родственник попал в ДТП»



С использованием
торговых площадок



Незаконное получение
доступа к личным данным



Под предлогом продления
срока действия сим-карты