

Россиянам рассказали, чем опасна просьба включить демонстрацию экрана

Телефонное мошенничество становится всё изощрённее: преступники выдают себя за сотрудников банков, МФЦ или даже работодателей. Одной из популярных схем стало использование демонстрации экрана на смартфоне. Под предлогом проверки безопасности или настройки программы злоумышленники просят жертву включить эту функцию, после чего перехватывают СМС-коды и получают доступ к банковским счетам или аккаунтам на «[Госуслугах](#)». По данным [ВТБ](#), 30–40% кибератак связано с программами удалённого доступа, а МВД отмечает, что такие схемы составляют до 20% всех случаев мошенничества.

Для атаки мошенники притворяются сотрудниками служб техподдержки или представителями компаний, используя аккаунты, похожие на официальные. Как поясняет Владимир Абрамов из PRO32 Connect, демонстрация экрана может быть полезной, но в руках злоумышленников превращается в инструмент кражи данных. Преступники охотятся за кодами аутентификации, личной перепиской и банковской информацией. В качестве [примера](#) можно привести случай из Абакана, где пенсионер потерял более 750 тысяч рублей, доверившись мошеннику, который представился покупателем дачного участка.

Эксперты настоятельно советуют никогда не соглашаться на демонстрацию экрана, если собеседник вызывает подозрения. Если ситуация требует этого, предварительно отключите уведомления, закройте приложения с конфиденциальной информацией или отправляйте скриншоты вместо трансляции экрана. В случае сомнений лучше прервать разговор и перезвонить в организацию самостоятельно. Компании, в свою очередь, рекомендуют обучать сотрудников основам [кибербезопасности](#) и использовать специализированное ПО для демонстрации экрана.