

Как **демонстрация экрана**
может привести
к потере денег?

Злоумышленники используют изощренную схему обмана, при которой под видом руководства вашей организации, сотрудника банка или оператора, требуют включить демонстрацию экрана для регистрации на различных ресурсах.

Особую опасность представляет возможность считывания кодов подтверждения прямо с экрана устройства жертвы, что позволяет мошенникам полностью завладеть аккаунтом.

Механизм мошенничества прост и эффективен

- 01 Создание поддельного аккаунта, имитирующего официальный
- 02 Звонок жертве под видом руководства
- 03 Требование зарегистрироваться на определенном ресурсе
- 04 Просьба включить демонстрацию экрана
- 05 Кража персональных данных в режиме реального времени
- 06 Получение доступа к аккаунту на портале "Госуслуги"

Рекомендации

- 1** Никогда не включайте демонстрацию экрана при общении с незнакомыми лицами
- 2** Проверяйте личность собеседника через официальные каналы связи
- 3** Не реагируйте на просьбы о регистрации на любых ресурсах по требованию неизвестных лиц
- 4** При подозрении на мошенничество немедленно прекращайте общение
- 5** Отключите отображение содержания уведомлений (вы узнаете то что в них написано, только когда откроете сообщение)



Артем Шейкин

*Сенатор РФ, Первый заместитель
председателя Комитета Совета Федерации
по конституционному законодательству
и государственному строительству*

“ —

Чтобы максимально обезопасить себя, заведите отдельный номер телефона и электронную почту только для работы с онлайн-банком и подтверждения финансовых операций.

Почему это важно?

- ✓ Этот номер и почта будут использоваться только для финансовых целей, минимизируя риск попадания в руки мошенников.
- ✓ Не используйте их для регистрации в социальных сетях, интернет-магазинах и других онлайн-сервисах.
- ✓ Не публикуйте их в открытом доступе.