

## Телефонные мошенники

Сегодня номер мобильного телефона – это ключ ко всему: банковским приложениям, электронным госуслугам, данным о недвижимости, социальным сервисам и личной информации. Мошенники это понимают, поэтому все чаще используют сим-карты в своих схемах. Они представляются сотрудниками компаний-операторов сотовой связи, пугают блокировкой номера, требуют "продлить договор", манипулируя страхами и эмоциями людей.

### Как не стать жертвой злоумышленников

По словам правоохранителей, самое важное – сохранять критическое мышление и не реагировать эмоционально. Кроме того, чтобы защитить себя от мошенников, нужно соблюдать несколько ключевых правил.

**Регулярная проверка учетных записей.** Рекомендуется систематически просматривать состояние ваших аккаунтов на различных платформах и сервисах. Если замечаете подозрительную активность, немедленно обращайтесь в службу поддержки сервиса и обновляйте пароль.

**Мониторинг количества сим-карт на госуслугах.** Это можно сделать через личный кабинет. В профиле найти раздел "Сим-карты", в котором отображаются зарегистрированные на пользователя номера телефонов. Перейдя по приведенному номеру, можно будет увидеть данные договора, дату активации и оформления. Кроме того, есть возможность заблокировать ненужные номера и вообще расторгнуть договор с оператором связи.

**Использование двухфакторной аутентификации.** Помимо обычного ввода пароля, система запрашивает дополнительный код подтверждения, который приходит на ваш мобильный телефон или другое устройство.

**Разнообразие паролей.** Используйте разные пароли для каждого аккаунта. Это минимизирует риск одновременного доступа ко всем вашим данным в случае компрометации одного пароля.

**Диверсификация номеров телефонов и аккаунтов.** Эксперты рекомендуют иметь три номера телефона и три аккаунта. Один – чистый – для банка, госуслуг и т. п. Этот номер не стоит давать никому, кроме указанных структур. Второй – свободный – для друзей, коллег по работе и иного проверенного общения. Третий – "грязный" – для взаимодействия с магазинами, компаниями сферы услуг и прочими подобными организациями.

**Обновление программного обеспечения.** Постарайтесь держать операционную систему и приложения в актуальном состоянии. Часто вирусы и эксплойты эксплуатируются именно в старых версиях программного обеспечения, имеющих известные уязвимости.

**Проверка кредитной истории.** Вы можете дважды в год бесплатно получать отчет о своей кредитной истории через портал госуслуг. Проверяйте наличие незавершенных кредитов и заявок на займы, чтобы вовремя выявить возможные нарушения.

**Контроль налоговых счетов.** Через личный кабинет налогоплательщика на сайте ФНС России вы можете следить за состоянием ваших финансовых обязательств и отслеживать операции с налоговыми выплатами.

Кроме того, рекомендуется настроить уведомления о любых действиях с недвижимостью. А также проверять записи в ЕГРН хотя бы раз в год.

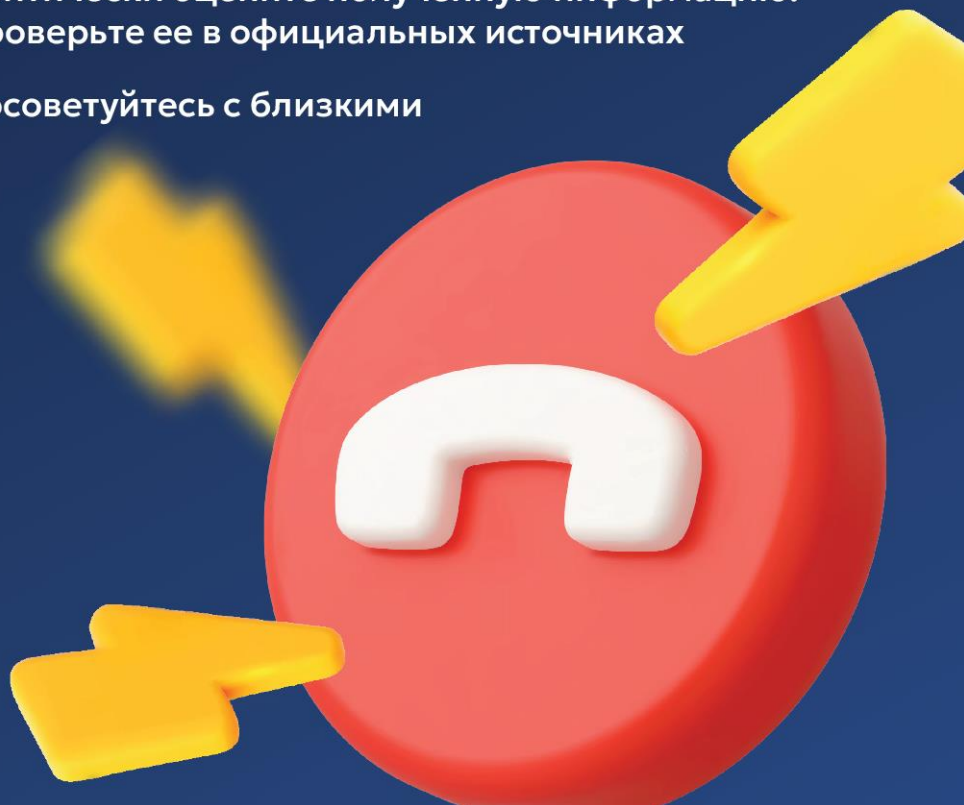
**Общение с пожилыми людьми.** Поговорите со своими близкими, особенно пожилыми родственниками и детьми. Научите их правилам цифровой гигиены. Распечатайте эту статью и дайте почитать своим родителям.

**Запрет сделок с недвижимостью.** Для дополнительной защиты недвижимости вы можете обратиться в МФЦ или через портал госуслуг, чтобы наложить запрет на любые сделки с вашей собственностью без личного участия.

## ЗВОНЯТ С НЕЗНАКОМОГО НОМЕРА И ПРОСЯТ СООБЩИТЬ ДАННЫЕ ИЛИ ПЕРЕВЕСТИ СРЕДСТВА?

### ВАШИ ДЕЙСТВИЯ:

- Немедленно кладите трубку
- Позвоните по официальному телефонному номеру организации, сотрудником которой представился звонящий (собеседник)
- Критически оцените полученную информацию. Проверьте ее в официальных источниках
- Посоветуйтесь с близкими





Банк России



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ

## **ЗВОНЯТ С НЕЗНАКОМОГО НОМЕРА И ПРОСЯТ СООБЩИТЬ ДАННЫЕ ИЛИ ПЕРЕВЕСТИ СРЕДСТВА?**

### **ВАШИ ДЕЙСТВИЯ:**

- Немедленно кладите трубку
- Позвоните по официальному телефонному номеру организации, сотрудником которой представился звонящий (собеседник)
- Критически оцените полученную информацию. Проверьте ее в официальных источниках
- Посоветуйтесь с близкими





Банк России

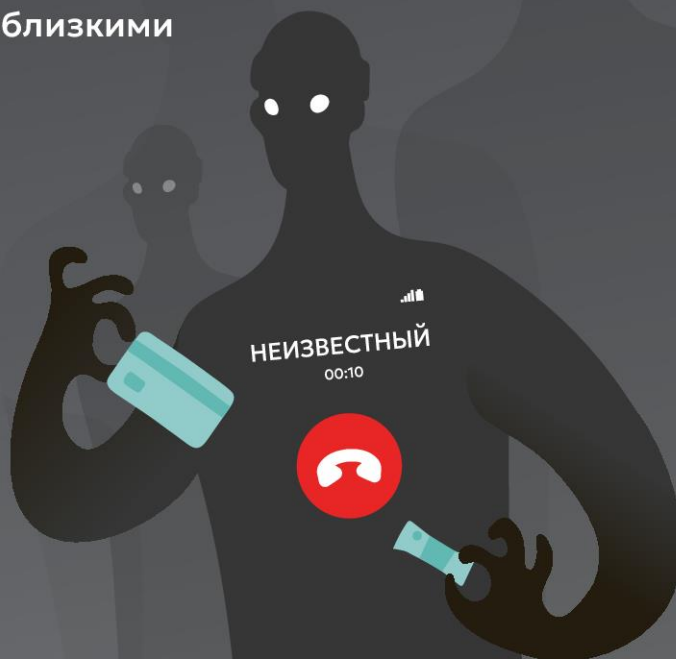


ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ

## ЗВОНЯТ С НЕЗНАКОМОГО НОМЕРА И ПРОСЯТ СООБЩИТЬ ДАННЫЕ ИЛИ ПЕРЕВЕСТИ СРЕДСТВА?

### ВАШИ ДЕЙСТВИЯ:

- Немедленно кладите трубку
- Позвоните по официальному телефонному номеру организации, сотрудником которой представился звонящий (собеседник)
- Критически оцените полученную информацию. Проверьте ее в официальных источниках
- Посоветуйтесь с близкими





Банк России



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ

## ЗВОНЯТ С НЕЗНАКОМОГО НОМЕРА И ПРОСЯТ СООБЩИТЬ ДАННЫЕ ИЛИ ПЕРЕВЕСТИ СРЕДСТВА?

### ВАШИ ДЕЙСТВИЯ:

- Немедленно кладите трубку
- Позвоните по официальному телефонному номеру организации, сотрудником которой представился звонящий (собеседник)
- Критически оцените полученную информацию. Проверьте ее в официальных источниках
- Посоветуйтесь с близкими

