ПАМЯТКА ПО ТЕЛЕФОННОМУ МОШЕННИЧЕСТВУ



Как распознать мошенника по телефону

- **Звонят «от имени банка», «службы безопасности», «Госуслуг» или госорганов** и сразу требуют срочно что-то сделать: перевести деньги, назвать код из СМС, установить приложение, «заморозить счёт». Настоящие сотрудники банков и госорганов не просят коды и не заставляют действовать немедленно.
- **Создают ощущение срочности и паники**: «счёт заблокируют через 5 минут», «деньги прямо сейчас списывают», «если не подтвердите личность — доступ потеряете». Это типичный приём давления.
- **Просят данные, которые никому нельзя сообщать**: коды из СМС и пуш-уведомлений, CVC/CVV-код, пин-коды, пароли от онлайн-банка, данные карты.
- **Предлагают «вывести деньги на безопасный счёт»** или «пройти верификацию по ссылке». Безопасных счетов для спасения денег не существует.
- **Звонят через мессенджеры** (WhatsApp, Telegram и т. п.) якобы от банка или полиции. Банки не используют мессенджеры для официальных уведомлений.
- **Используют подмену номера**: на экране может высветиться номер банка или ведомства, но это не гарантия подлинности.

Что делать, если поступил подозрительный звонок

1. **Не сообщайте никакие данные** — ни коды, ни пароли, ни реквизиты карты, ни паспортные сведения.
2. **Не переходите по ссылкам**, не устанавливайте приложения по просьбе звонящего.
3. **Прервите разговор** и сами перезвоните в организацию по официальному номеру (с сайта банка, с оборотной стороны карты, из справочника).

4. **Если речь о банке** — свяжитесь напрямую с банком и уточните, действительно ли есть проблема.
5. **Если речь о полиции, госоргане, Госуслугах** — уточните информацию через официальные каналы (сайт, горячая линия), а не через того, кто позвонил.
6. **Сообщите о звонке**: в банк (часто есть отдельная линия для подозрительных операций) и при необходимости — в полицию.
7. **Сохраните детали**: номер телефона, время звонка, суть разговора — это пригодится для заявления.

Практические меры защиты

- **Включите блокировку спама** в настройках телефона или через сервис оператора связи.
- **Не публикуйте в открытом доступе** номер телефона и личные данные.
- **Настройте лимиты и уведомления** в мобильном банке: оповещения о списаниях, лимиты на переводы, запрет онлайн-операций при необходимости.
- **Используйте сложные пароли** и двухфакторную аутентификацию везде, где возможно.
- **Регулярно обновляйте приложения и операционную систему** — это снижает риски взлома.

Частые сценарии и как на них реагировать

- **«С вашего счёта пытаются списать деньги, срочно подтвердите личность»** — положите трубку и сами свяжитесь с банком.
- **«Вам одобрен кредит, назовите код для отказа»** — не называйте код, не подтверждайте ничего. Лучше проверьте статус кредита в официальном приложении.
- **«Это полиция, нужно помочь в расследовании, переведите средства на спецсчёт»** — это мошенничество. Полиция не просит переводить деньги.
- **«Родственник попал в беду, срочно нужны деньги»** — прервите разговор и свяжитесь с родственником по известному вам номеру.

Куда обращаться, если стали жертвой или заметили мошенничество

- **Банк** — для блокировки операций и проверки счёта.
- **Полиция** — подать заявление (можно онлайн через сайт МВД или лично).
- **Роскомнадзор** — если речь о незаконном использовании персональных данных или массовых обзвонах.