ДИСТАНЦИОННЫЕ МОШЕННИКИ: КАК НЕ СТАТЬ ИХ ЖЕРТВОЙ

Телефонные и интернет-аферисты становятся всё хитрее. Они маскируются под сотрудников банков, госслужб и даже врачей. Как распознать обман и защитить себя? Рассказываем простым языком.

🚨 Самые частые уловки мошенников

Звонок или сообщение могут выглядеть очень правдоподобно. Вас могут:

- Пугать: «Ваш счёт взломали!», «На вас оформили кредит!», «Ваш родственник в беде!».

- Соблазнять: «Вы выиграли приз!», «Вам положена выплата!», «Давайте увеличим ваши сбережения!».

- Предлагать помощь: «Улучшим скорость интернета», «Запишем на бесплатное обследование», «Пройдите опрос».

- Притворяться официальными лицами: из банка, полиции, прокуратуры, «Госуслуг», налоговой.

Их цель — заставить вас действовать быстро, не думая!

⚡ Что они просят (НИКОГДА ЭТОГО НЕ ДЕЛАЙТЕ!)

-Назвать коды из СМС— это всегда пароли к вашим деньгам!

- Установить программу - на телефон/компьютер (AnyDesk, TeamViewer и др.) — это даст им полный доступ к вашему устройству.

- Перевести деньги - на «безопасный счёт» или для «проверки».

- Сообщить данные карты: номер, срок, CVC-код, пароли из банковских приложений.

- Срочно позвонить по указанному номеру - (это номер мошенников).

🛡️ Правила цифровой безопасности: памятка для каждого

1. **Это главное: НИКОМУ И НИКОГДА не сообщайте коды из СМС, пароли и данные карт**. Настоящие сотрудники банка и госорганов **НЕ ЗНАЮТ** и **НЕ СПРАШИВАЮТ** эти коды.

2. **Не спешите**. Любая история, требующая сиюминутных действий, — подозрительна. Положите трубку и **самостоятельно** перезвоните в банк или организацию по **официальному номеру** с сайта.

3. **Не перезванивайте** на номера, присланные в подозрительных СМС. Не звоните по просьбе звонящего «аферист».

4. **Проверяйте звонки.** Включайте в настройках телефона **«Определение номера»** или **«Спам-защиту»**. Если видите отметку «Банк» или «Служба доставки» — это легитимный вызов. Без отметки — будьте настороже.

5. **Защитите аккаунты:**

- Используйте **сложные пароли** (разные для разных сервисов!).

- Включайте **двухфакторную аутентификацию** везде, где это возможно.

6. **Не устанавливайте** неизвестные программы и не открывайте файлы по просьбе незнакомцев.

🏛 Государство вам в помощь: простые способы усилить защиту

Эти инструменты созданы специально для защиты граждан:

- **«Самозапрет» на новые кредиты на «Госуслугах**» — банки не смогут выдать вам кредит онлайн без вашего прямого согласия. Очень мощная защита.

- **«Самозапрет» на новые SIM-карты на «Госуслугах»** — мошенник не сможет оформить симку на ваше имя. Снять запрет можно только лично в МФЦ.

- Доверенное лицо в банке — вы можете назначить родственника, которому банк будет звонить для подтверждения подозрительных крупных переводов.

- **Правило для SIM-карты** — карта должна использоваться только её владельцем. Передавать можно только самым близким родственникам (без переоформления договора).

✅ Что делать, если всё-таки попался?

1. **Немедленно позвоните в банк** по номеру с карты или официального сайта и заблокируйте карту.

2. **Напишите заявление в полицию** через ближайшее отделение или сайт МВД.

3. **Пожаловаться на мошеннический номер** можно оператору связи (МТС, Билайн, МегаФон, Теле2) и в Роскомнадзор.

Главное — помните: ваши финансы и данные под угрозой только тогда, когда вы сами передаёте коды и доступы. Остановитесь, перезвоните в организацию сами и посоветуйтесь с родными.