


# БУДЬТЕ БДИТЕЛЬНЫ — КИБЕРМОШЕННИЧЕСТВО!

**Кибермошенничество** — это обман с использованием цифровых технологий: интернета, мобильной связи, мессенджеров, социальных сетей.

**Цель злоумышленников** — получить доступ к персональным данным, банковским картам, аккаунтам, финансовым средствам или ввести в заблуждение ради выгоды.

 Особенно уязвимы сотрудники, имеющие доступ к внутренним системам, документам и почтовым каналам.



# ПРИЗНАКИ МОШЕННИЧЕСКОЙ АТАКИ

- Чаще всего мошенники представляются руководителями разного уровня, сотрудниками силовых структур или кредитно-финансовых организаций.
- Вас **торопят**, создают стресс или панику.
- Просят **перевести деньги**, оформить кредит, загрузить «программу безопасности».
- Упоминают **секретность**, не разрешают никому сообщать о разговоре.
- Используют номера, похожие на официальные (**подменный номер**).
- На письмах или сайтах — нелогичные **ошибки**, необычные домены (например, gosusligi.ru).
- **Вход** в Ваш аккаунт выполнен с нового устройства или региона.



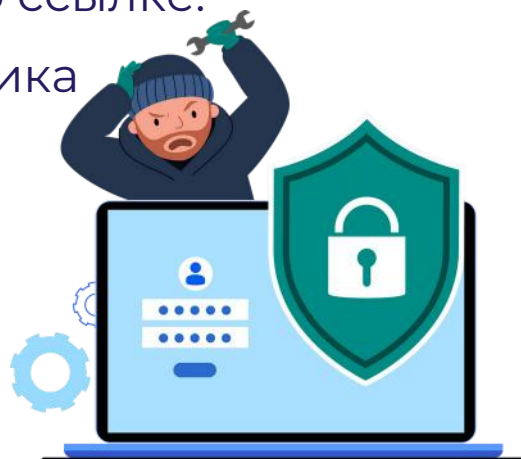
# КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА?

- Не спорьте — просто **положите трубку**.
- **Никому не сообщайте** коды из SMS, пароли от онлайн-банка, данные карты.
- Используйте **сложные пароли** и меняйте их регулярно.
- Не устанавливайте **сомнительные приложения**.
- Подключите **уведомления от банка** об операциях по картам.
- Не открывайте **ссылки от незнакомцев**.  
(переход по таким ссылкам может привести к краже вашей учетной записи)



## САМЫЕ РАСПРОСТРАНЕННЫЕ СООБЩЕНИЯ СО ССЫЛКАМИ ОТ МОШЕННИКОВ:

- Племянник (-ца) участвует в конкурсе, прошу поддержать, пройти по ссылке.
- От лица близкого родственника о том, что он(-а) попал (-а) в беду и нужна экстренная финансовая помощь.
- С просьбой о помощи тяжелобольному ребенку.

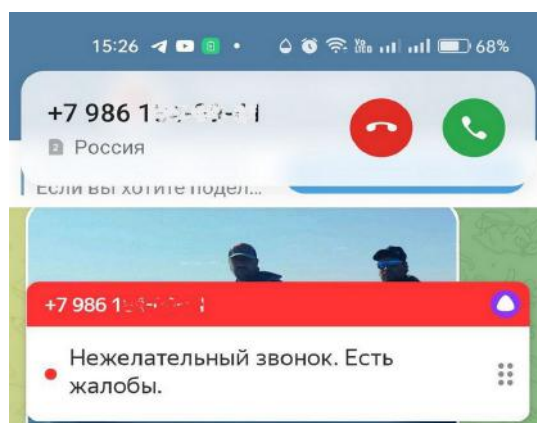


# КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА?

- Установите на своем устройстве **определитель номера (например, от Яндекса)**, который будет сообщать о подозрительных и нежелательных звонках.

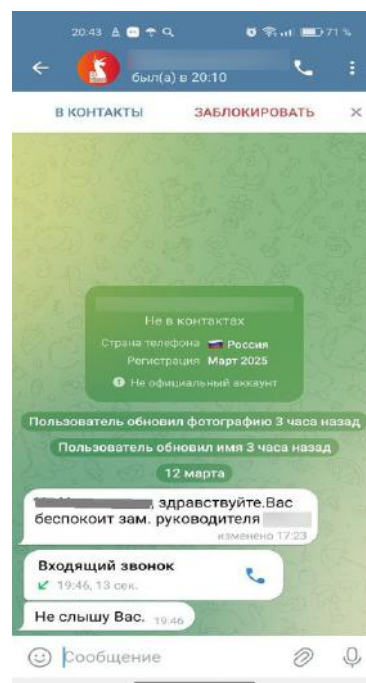


(Для корректной работы должен быть установлен только один определитель номера.)



- Обратите внимание на **дату создания аккаунта**, с которого приходят подозрительные сообщения.

(Если дата создания такого аккаунта совпадает с датой отправленных вам сообщений, то вероятнее всего этот аккаунт принадлежит мошенникам.)



# КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА?

## ЗАЩИТА ОТ МОШЕННИКОВ — САМОЗАПРЕТ НА КРЕДИТЫ

Один из распространённых видов мошенничества — заставить человека обманом или психологическим давлением оформить на себя кредит.

С 1 марта 2025 года на Госуслугах можно установить или снять **самозапрет** на выдачу кредитов. После снятия самозапрета взять кредит можно будет только через один рабочий день или больше. Это время отвели на период «охлаждения». Он так же нужен для препятствования мошенникам.

### ЗАПРЕТ ДЕЙСТВУЕТ:

Потребительский кредит  
Кредитные карты  
Микрозайм  
Овердрафт

### ЗАПРЕТ НЕ ДЕЙСТВУЕТ:

Образовательный кредит  
Договор поручительства  
Автокредит  
Ипотека



# ЧТО ДЕЛАТЬ ПРИ ВЗЛОМЕ АККАУНТА?

Если Вы подозреваете, что Ваш аккаунт в соцсети или мессенджере взломан:

**1. Попробуйте войти с другого устройства** и немедленно смените пароль.



**2. Нет доступа?**

Обратитесь в службу тех.поддержки для восстановления доступа:

ВКонтакте — [vk.com/support](https://vk.com/support)

Одноклассники — [ok.ru/help](https://ok.ru/help)

Телеграм — [abuse@telegram.org](mailto:abuse@telegram.org)

«Госуслуги» — 8 800 1007010 / [support@gosuslugi.ru](mailto:support@gosuslugi.ru)

**3. Уведомите знакомых и коллег о взломе Вашего аккаунта.**

**4. Защитные меры.**

- Проверьте настройки безопасности на отсутствие постороннего номера и почты.
- После восстановления доступа включите двухфакторную аутентификацию.
- Проверьте вкладку «Активные сессии»/«Где вы в сети» — выйдите с незнакомых устройств.

# ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ПЕРЕВЕЛИ ДЕНЬГИ МОШЕННИКАМ?

- Немедленно **позвоните в банк и заблокируйте** карту/операцию (телефон указан на карте).
- **Сообщите в экстренные службы** — по телефону 112, 102 (полиция) или лично.
- **Сохраните все доказательства:** скриншоты, чеки, переписку, имена, номера.
- **Подайте заявление** в ближайший отдел МВД ([68.mvd.pf/contact/units](https://68.mvd.pf/contact/units)).
- **Напишите жалобу в Роскомнадзор**, если мошенники используют сайты или домены ([68.rkn.gov.ru](https://68.rkn.gov.ru)).
- Заполните на Госуслугах форму **«Информация о подозрительном звонке»** ([www.gosuslugi.ru/600465/](https://www.gosuslugi.ru/600465/)) и в сервисе **«Фильтр звонков»** ([callfilter.app](https://callfilter.app)).

