КУДА ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ

ПОЛЕЗНЫЕ ТЕЛЕФОНЫ

Банк России
банковские услуги, кредиты, противодействие мошенничеству **8-800-300-30-00**

Роспотребнадзор по Саратовской области
защита прав потребителей финансовых услуг **8-800-100-18-58**

Социальный фонд России
социальные выплаты, пенсии и пособия **8-800-100-00-01**

Судебные приставы (ФССП)
задолженность и исполнительное производство **8-800-250-39-32**

Бесплатная юридическая помощь
включая вопросы банкротства граждан **+7 (8452) 65-34-36**

СКАНИРУЙ И УЗНАВАЙ БОЛЬШЕ

Мессенджер MAX

ВКонтакте

ГАУ ДПО «СОИРО»

Мои финансы РФ

Финансовая культура

Наведи камеру смартфона на QR-код

ТВОЯ ФИНАНСОВАЯ БЕЗОПАСНОСТЬ – В ТВОИХ РУКАХ!

Региональный центр финансовой грамотности ГАУ ДПО «СОИРО»

Если вы стали жертвой мошенников — действуйте быстро!



Если мошенники получили доступ к вашим личным данным, банковской карте или Госуслугам, нужно действовать быстро. Спасти ситуацию поможет скорость вашей реакции.

Что делать в таких случаях, рассказываем в специальной рубрике **Объясняем.рф** и Киберполиции России.

1 Если украли данные банковской карты



- Смените пароль и код доступа от банковского сервиса.
- Заморозьте банковские карты и счета.
- Свяжитесь с банком по номеру, указанному на банковской карте или официальном сайте, сообщите о произошедшем.
- Предупредите близких, чтобы они не переводили деньги на ваши карты.

ЧТО ДЕЛАТЬ

2 Если взломали личный кабинет на Госуслугах



- Смените пароль и код доступа к банковскому сервису.
- Позвоните на горячую линию Госуслуг: 8 (800) 100-70-10 и сообщите об утечке данных.
- Если получилось войти в личный кабинет, проверьте заявки, разрешения, в том числе в сторонних сервисах.
- Обратитесь в полицию.

ЧТО ДЕЛАТЬ

3 Если получили доступ к телефону



- Свяжитесь с мобильным оператором и сообщите о случившемся. Сотрудник клиентского сервиса подскажет, как действовать.
- Все аккаунты сервисов и приложений привяжите к другому номеру телефона.
- Следите за приходящими СМС о блокировке или перевыпуске сим-карты.
- Предупредите родных и знакомых, что с вашего номера могут звонить и писать злоумышленники.

ЧТО ДЕЛАТЬ

4 Если взломали ваши соцсети или мессенджеры



- Предупредите знакомых о взломе по другим каналам связи.
- Восстановите доступ к аккаунту.
- Смените пароль, включите двухфакторную идентификацию.
- Сделайте аккаунты в соцсетях закрытыми — так у мошенников меньше шансов вас шантажировать.
- В списке привязанных к аккаунту устройств отключите все незнакомые девайсы.
- Обратитесь в службу поддержки, если не удаётся войти в аккаунт.
- Попросите родственников и друзей жаловаться на ваш аккаунт в поддержку, чтобы его заблокировали.

ЧТО ДЕЛАТЬ

ВАЖНО!

Если злоумышленники получили неправомерный доступ к вашим данным, изменили, блокировали их или воспользовались информацией, чтобы похитить у вас деньги **обращайтесь в полицию.**

112 **Звонок бесплатный**

Всегда используйте сложные уникальные пароли, двухфакторную аутентификацию и не переходите по сомнительным ссылкам.

Не сообщайте коды из СМС

Не сообщайте CVV-коды карт

Узнайте больше на сайте Банка России

cbr.ru

Ваша безопасность — в ваших руках!