

Ребёнок сказал мошенникам код: что делать

Ребёнок отправил незнакомцу код из СМС, а потом рассказал об этом вам. Не спешите ругать его или забирать телефон. Сначала нужно выяснить, для чего предназначался код, и защитить аккаунты.



1 Выясните, какой код отправил ребёнок

Не каждый код из СМС дает доступ к деньгам, но некоторые позволяют войти в аккаунт, сменить пароль или подтвердить операцию.

Попросите ребенка показать сообщение с кодом и переписку с человеком, которому он его отправил. Обратите внимание на отправителя и текст СМС: там часто указано, для какого сервиса предназначен код и что он подтверждает.

Это может быть:

Код от игры или социальной сети

Мошенник использует его для входа в аккаунт ребенка.

Код от банка

Он может подтверждать вход или финансовую операцию. В этом случае действовать нужно **немедленно**.

Код от «Госуслуг»

Есть риск доступа к личным данным и услугам.

Не удаляйте переписку и СМС.

Сделайте скриншоты: они могут понадобиться при обращении в поддержку сервиса, банк или полицию.

2 Защитите аккаунт

Если код предназначался для входа в игру, социальную сеть или мессенджер, откройте приложение самостоятельно. Не переходите по ссылкам, которые прислал незнакомец.

Если доступ к аккаунту сохранился:

1. Смените пароль на новый, главное, не используйте такой же пароль, как и в других сервисах.
2. Проверьте список устройств и активных сеансов — его можно найти в настройках. Завершите все подключения, кроме активного.
3. Включите двухфакторную аутентификацию, если она доступна.
4. Проверьте, не изменились ли номер телефона, электронная почта и другие способы восстановления доступа.

Если войти уже не получается, воспользуйтесь официальной формой восстановления аккаунта или обратитесь в поддержку сервиса.

Важно: смена пароля не всегда автоматически отключает посторонние устройства. Поэтому обязательно проверьте активные сеансы.

3 Если код связан с банком — сразу звоните по горячей линии

Если ребенок отправил код от банковского приложения, подтверждения перевода или оплаты, немедленно свяжитесь с банком.

Номер телефона возьмите с официального сайта банка или с обратной стороны карты. **Не звоните по номерам из сообщений мошенников.**

Объясните сотруднику, какой код был передан и что произошло. Попросите проверить подозрительные операции и при необходимости заблокировать карту или доступ к онлайн-банку.

Если деньги уже списали, сообщите об этом банку и подайте заявление о несогласии с операцией. Банк рассмотрит обращение, но возврат денег не гарантирован.

Не пытайтесь самостоятельно «отменить перевод» по инструкции незнакомца. Мошенники часто используют такую схему, чтобы получить еще больше денег.

4 Если код был от «Госуслуг»

Попробуйте войти в учетную запись через официальный сайт или приложение.

Если доступ сохранился, смените пароль, проверьте активные сеансы, контактные данные и историю действий. Если заметили подозрительные изменения или потеряли доступ, обратитесь в официальную поддержку и восстановите аккаунт.

При признаках использования персональных данных посторонними стоит также обратиться в полицию.

5 Поговорите с ребёнком без обвинений

Представьте: ребенок хотел получить редкий предмет в игре. Незнакомец попросил код, пообещал подарок, а затем исчез.

Ребенок понимает, что его обманули, и боится рассказать вам.

В этот момент ему важно услышать не «Как ты мог на такое повестись?», а:

«Спасибо, что рассказал. Давай вместе разберемся, что произошло».

Не требуйте сразу объяснять, почему он поверил незнакомцу. Сначала решите проблему, а потом спокойно обсудите случившееся.

Мошенники умеют вызывать доверие, торопить и запугивать. На их уловки попадают и взрослые. Поэтому ошибка ребенка — не повод для насмешек или наказания.

Если ребенок уверен, что за признание его не будут ругать, ему проще обратиться за помощью вовремя.

6 Договоритесь, что делать в следующий раз

Когда ситуация разрешится, обсудите с ребенком несколько простых правил.

1. Коды из СМС и уведомлений нельзя передавать другим людям, даже если они представляются сотрудниками поддержки или друзьями.
2. Если незнакомец требует код, угрожает блокировкой аккаунта или обещает подарок за выполнение условий, лучше прекратить разговор и обратиться к взрослому.
3. И самое главное — договоритесь, что ребенок может рассказать вам о подозрительном сообщении, даже если уже успел ответить мошеннику.

Не обязательно устраивать долгую беседу о безопасности. Достаточно спокойно разобрать один конкретный случай и убедиться, что ребенок знает, к кому обращаться за помощью.

Мошенники рассчитывают в том числе на то, что ребёнок испугается и промолчит. Ваша задача — показать, что с проблемой ему не придётся справляться одному.

