

«Вас уже изучили в интернете»: как мошенники используют открытые данные и почему нельзя называть код из СМС

Откуда мошенники знают про вас?

Мошенники **не гадают**. Чаще всего они просто заходят в **открытые источники**:

- ваши страницы в соцсетях (ВКонтакте, Одноклассники, Telegram);
- сайты с отзывами и объявлениями (Авито, Юла);

Из этих источников можно узнать:

- **дату рождения**;
- **адрес и место работы**;
- **контактный телефон** (если он есть в объявлениях или соцсетях);
- **состав семьи**, хобби, привычки.

Эти сведения мошенники используют, чтобы **вызвать доверие**: они звонят и называют ваши имя, фамилию, адрес, место работы — и вы уже меньше сомневаетесь, что на другом конце «свой».

Схема «Поздравляем, вы выиграли!» или «Вам подарок, доставка цветов»

Как это выглядит:

- Вам звонят.
- Сообщают: «Вы выиграли приз (телефон, бытовая техника, путевка)», «Вам заказали доставку цветов», «Вам отправили подарок от магазина».
- Чтобы подтвердить получение или оформить доставку, просят **назвать код из СМС**, который придет на ваш телефон.

Что происходит на самом деле:

- Код из СМС — это **ключ от вашего аккаунта** (на «Госуслугах», в онлайн-банке, на маркетплейсе).
- Продиктовав код, вы сами даёте мошенникам доступ к вашему личному кабинету.

Пример из жизни:

Вам звонят: «Здравствуйте, это служба доставки. Вам заказали букет цветов. Для подтверждения адреса назовите, пожалуйста, код из СМС». Вы называете — и через минуту с вашей карты списывают деньги, а на «Госуслугах» меняют пароль.

Что делать:

- **Никогда, никому и ни при каких обстоятельствах не называйте код из СМС.**
- **Настоящая доставка не требует кода. Она требует только адреса и имени.**
- **Если вам сообщают о выигрыше — положите трубку. Бесплатных призов не бывает.**

Через несколько минут (или часов) после того, как вы назвали код, вам снова звонят.

- Теперь звонящие представляются **сотрудниками полиции, ФСБ, Следственного комитета, прокуратуры, Центрального банка или службы безопасности банка и иных организаций.**
- Они говорят примерно следующее:
«Вам только что звонили мошенники. Мы это зафиксировали и пресекли их действия. Но ваши счета уже под угрозой. Чтобы спасти деньги, срочно переведите их на безопасный счёт».
Или: *«Из-за действий мошенников ваши деньги необходимо задекларировать. Назовите данные карты и код из нового СМС или необходимо передать денежные средства доверенному лицу организации (курьеру)».*

Почему это работает на психологическом уровне:

- Первый звонок («цветы / выигрыш») уже состоялся — значит, мошенники действительно проявили активность.
- Второй звонок («полиция / ФСБ») логично вписывается в картину: раз звонили мошенники, то и правоохранительные органы должны подключиться.
- У жертвы создаётся иллюзия, что её уже взяли под защиту.

Что происходит на самом деле:

- Никакой «полиции» и «ФСБ» на линии нет. Это те же мошенники, которые продолжают вести многоходовую комбинацию.
- «Безопасного счёта» не существует. Это счёт злоумышленников.
- «Декларирование денег» по телефону — выдумка. Ни один государственный орган не проводит таких процедур через звонок или мессенджер.

Пример из практики:

После того как пенсионерка С. назвала код из СМС якобы для подтверждения доставки, ей через 10 минут позвонил «сотрудник полиции». Он сообщил, что её счёт пытаются обнулить, и убедил перевести 450 000 рублей на «резервный счёт для проверки». Деньги не вернулись.

Что делать:

- **Положите трубку.** Настоящий сотрудник полиции, ФСБ, Следственного комитета или банка **никогда не попросит вас переводить деньги** на какой-либо счёт.
- **Никаких «безопасных счетов» не существует.** Это 100% признак мошенников.
- **Не поддавайтесь на «срочность» и «секретность».** Если вам говорят «срочно», «операция засекречена», «никому не говорите» — значит, вас изолируют от помощи близких.
- **Перезвоните сами** в банк или в полицию. Не по телефону, который вам продиктовали, а по официальному.

★ Главная памятка для семьи (повесьте на холодильник)

Что говорят мошенники	Что это значит на самом деле
«Назовите код из СМС для подтверждения»	Украдут доступ к вашему аккаунту и деньгам
«Переведите деньги на безопасный счёт»	Счёт мошенников, деньги не вернут
«Вас взламывают, срочно действуйте»	Давят на страх, чтобы вы не думали
«Никому не говорите, это секретная операция»	Изолируют от помощи
«Вам выиграш, подарок, цветы»	Обман, чтобы вы назвали код

Простые правила, которые спасут ваши деньги

1. **Код из СМС — это ваша подпись и печать. Никому его не называйте. Даже если звонящий знает ваше имя, адрес и место работы.**
2. **Никаких «безопасных счетов» не существует.** Если просят перевести деньги — это мошенники.
3. **Положите трубку и перезвоните сами** по официальному номеру (на карте, в договоре, на сайте).
4. **Предупредите пожилых родственников.** Мошенники специально звонят им — они больше доверяют.
5. **Помните:** дата рождения, адрес, место работы — это не тайна. Мошенники собирают эту информацию в основном из соцсетей. Не удивляйтесь, если звонящий знает про вас всё.

Если вы уже назвали код или перевели деньги — немедленно звоните в банк и в полицию.