



В День защиты персональных данных в специальной рубрике [Объясняем.рф](#) и [Киберполиции России](#)

рассказываем, что нельзя сообщать незнакомым людям, даже если они представляются сотрудниками банка, полиции или техподдержки Госуслуг.

1. Банковские данные

Номер карты, срок её действия, CVC-код (три цифры на обороте), логины и пароли от интернет-банка. Этой информации достаточно, чтобы украсть ваши деньги.

2. Коды из СМС

Одноразовые пароли открывают доступ к Госуслугам, почте и подтверждают платежи. Именно их чаще всего и выманивают мошенники. Никогда никому не диктуйте коды из СМС.

3. Документы

Серия и номер паспорта, ИНН, СНИЛС, фото документов. Зная эти данные, злоумышленники могут оформить заём или зарегистрировать новый номер телефона на человека. Читайте в наших постах, как оформить самозапрет на [кредиты](#) и [сим-карты](#).

4. Личная информация

Не сообщайте по телефону и не указывайте на открытых страницах в соцсетях данные: ваш адрес, номера близких, маршрут поездки, если куда-то едете, ваше точное местоположение на данный момент.

5. Комбинации данных

Иногда мошенникам хватает всего трёх деталей: имени, даты рождения и номера телефона, чтобы подобрать пароль к аккаунту, взломать почту или оформить заём.

Если вашими данными завладели мошенники — действуйте по алгоритму, который мы описали в [инструкции](#).

[Вестник Киберполиции России](#)

[#объясняемрф@obyasnyemrf](#)

[#безопасность@obyasnyemrf](#)

Читать нас в МАХ: vk.cc/cOzNMG