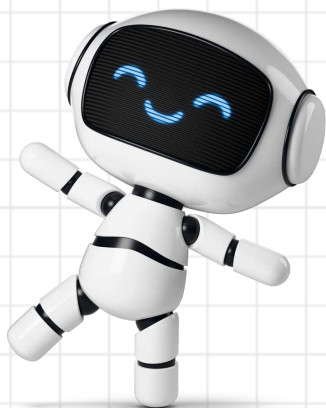


9 НЕ ДОВЕРЯЙТЕ НЕЗНАКОМЫМ ПРИЛОЖЕНИЯМ

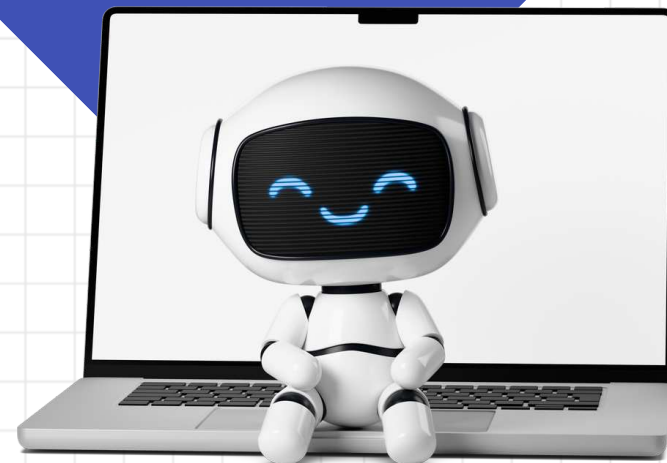
Иногда пользователи устанавливают сторонние программы, которые незаметно воруют данные. Загружайте приложения только из официальных магазинов (RuStore, Play Market) и читайте отзывы других пользователей.

10 НАУЧИТЕСЬ РАСПОЗНАВАТЬ ОБМАН

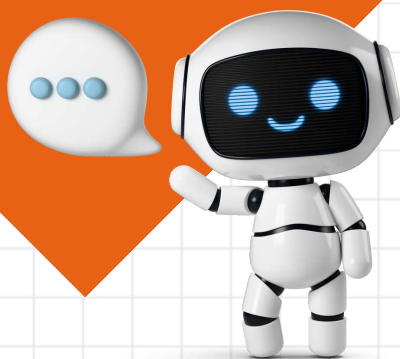
Некоторые технологии умеют подделывать голоса и лица людей (deepfakes). Если получили сообщение или звонок от друга или знакомого, но оно кажется странным, постарайтесь проверить информацию другими способами, прежде чем реагировать.



350010
Краснодарский край
г. Краснодар
ул. Офицерская, 50
+7 (861) 253-51-61
pmc@mtsr.krasnodar.ru
<https://kmc23.ru>



КАК ЗАЩИТИТЬ ЛИЧНЫЕ ДАННЫЕ: 10 простых шагов



1 ДЕЛАЙТЕ ПАРОЛИ СЛОЖНЫМИ И ВЕЗДЕ РАЗНЫМИ

Пароль должен быть длинным и содержать разные знаки: буквы большие и маленькие, цифры и символы. Лучше всего запоминать пароли через специальное приложение (менеджер паролей), которое создаст сложный пароль и сохранит его безопасно.

2 ПРОВЕРЯЙТЕ САЙТЫ И ПИСЬМА ВНИМАТЕЛЬНО

Если получаете странные сообщения с просьбой срочно обновить информацию или подтвердить оплату, перепроверьте название сайта. Мошенники любят маскироваться под известные бренды (банки, магазины, соцсети).

3 АКТИВИРУЙТЕ ДВОЙНУЮ ЗАЩИТУ

Двухступенчатое подтверждение помогает усилить безопасность вашего аккаунта дополнительным уровнем защиты. Обычно это одноразовый код, присылаемый на смартфон или e-mail. Благодаря этому, даже если злоумышленник узнает ваш пароль, он не сможет попасть в профиль без подтверждения с вашего устройства.

4 ОСТАВЛЯЙТЕ МЕНЬШЕ СЛЕДОВ В ИНТЕРНЕТЕ

Фотографии с геоданными, чеки, билеты на самолет или поезд — это все ценная информация для преступников. Подумайте дважды, прежде чем делиться такими вещами публично.

5 БЕРЕГИТЕ ВАЖНУЮ ИНФОРМАЦИЮ

Всегда делайте резервные копии своих важных файлов и храните их там, куда никто посторонний не доберется. Современные облачные хранилища защищают данные специальными технологиями шифрования.

6 ОЧИЩАЙТЕ СВОИ СТАРЫЕ УСТРОЙСТВА

Перед продажей старого телефона, планшета или компьютера обязательно сотрите с них всю личную информацию. Выполните полную очистку памяти или воспользуйтесь специальной программой для стирания данных.

7 БУДЬТЕ ОСТОРОЖНЫ В ОБЩЕСТВЕННЫХ WI-FI ЗОНАХ

Общественный Wi-Fi (в кафе, транспорте) небезопасен, потому что преступники могут увидеть и украсть ваши данные.

8 ЗАЩИТИТЕ МОБИЛЬНОЕ УСТРОЙСТВО

Используйте средства блокировки экрана смартфона или планшета (PIN-код, рисунок, отпечаток пальца). Также установите программы защиты от вирусов и вредоносных приложений, такие как Dr.Web, Kaspersky Mobile Security или Avast Antivirus. Обновляйте прошивку мобильного устройства регулярно, так как каждое обновление повышает уровень защиты.