



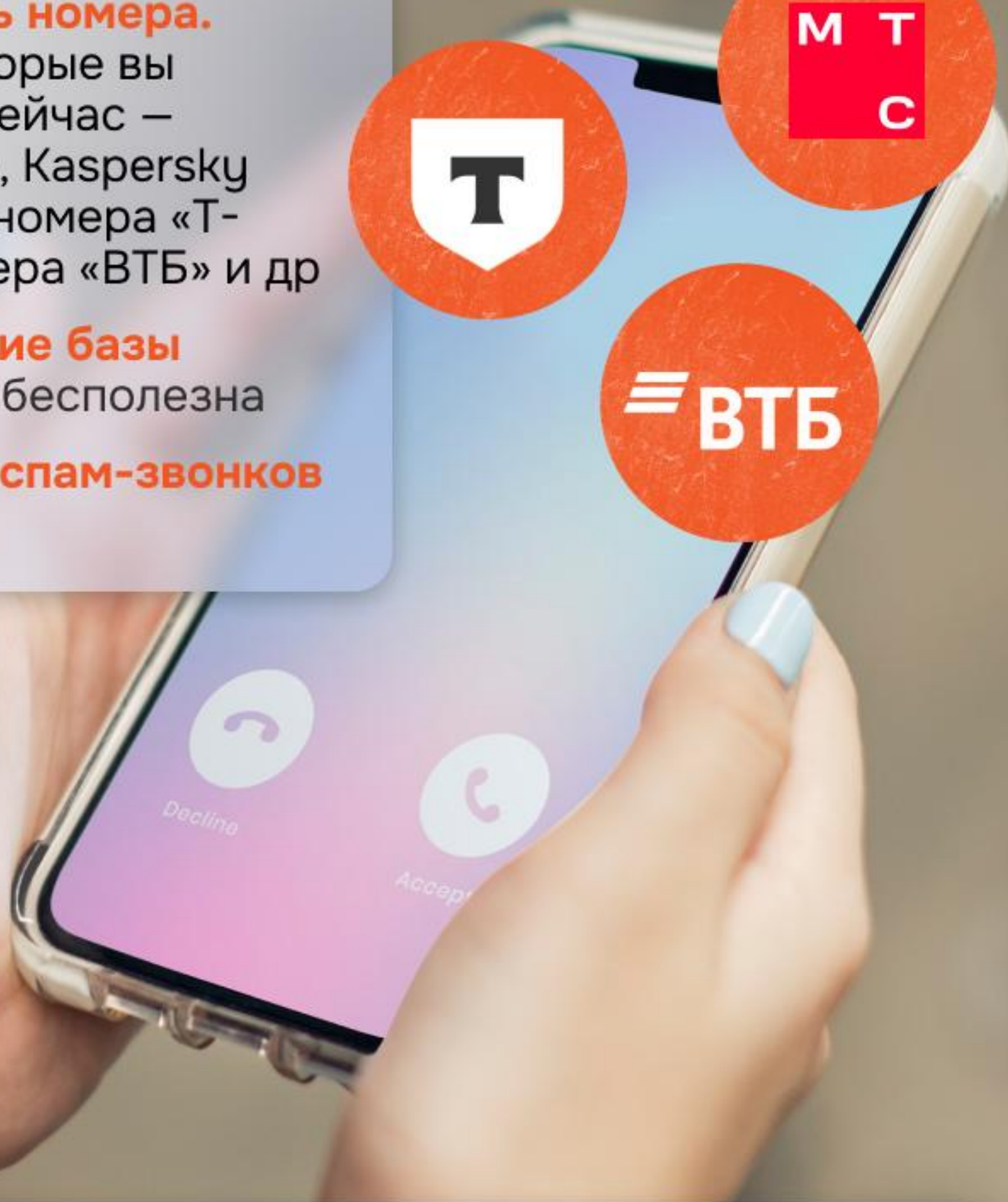
Защитите себя сами:

**5 простых правил, которые обезопасят
вас и ваши данные от мошенников**

Опасный звонок? Узнайте сразу



- Установите **определитель номера**.
Бесплатные сервисы, которые вы можете установить уже сейчас – определитель от Яндекса, Kaspersky Who Calls, определитель номера «Т-банк», определитель номера «ВТБ» и др
- Настройте **автообновление базы номеров** – иначе защита бесполезна
- Подключите **блокировку спам-звонков** в настройках смартфона



Важно: определитель помогает сразу понять, стоит ли брать трубку, и не попасться на уловку злоумышленников.

Антивирус ≠ лишняя программа. Скорее установите его



- Установите **антивирус** для защиты от вирусов, троянских программ и фишинговых ссылок
- Бесплатные версии есть у **Kaspersky, Dr.Web, PRO32**
- Он нужен и владельцам **Android и IOS**: Android чаще заражают вирусами, а iPhone — мишень для фишинга и мошеннических ссылок



Важно: без антивируса достаточно одного клика по фейковой ссылке — мошенники получают доступ к вашим данным и деньгам. А с ним вы и ваши данные в безопасности!

Придумайте надежный пароль. Сложный = безопасный



- Используйте **уникальные пароли** для каждого сервиса
- Длина пароля – **минимум 12 символов** (буквы, цифры и символы)
- Не используйте **личные данные:** имена, даты рождения, телефон
- Регулярно меняйте **пароли**



Важно: если взломают один слабый пароль – злоумышленники получат доступ ко всем вашим аккаунтам.

Плохой: Sakko12

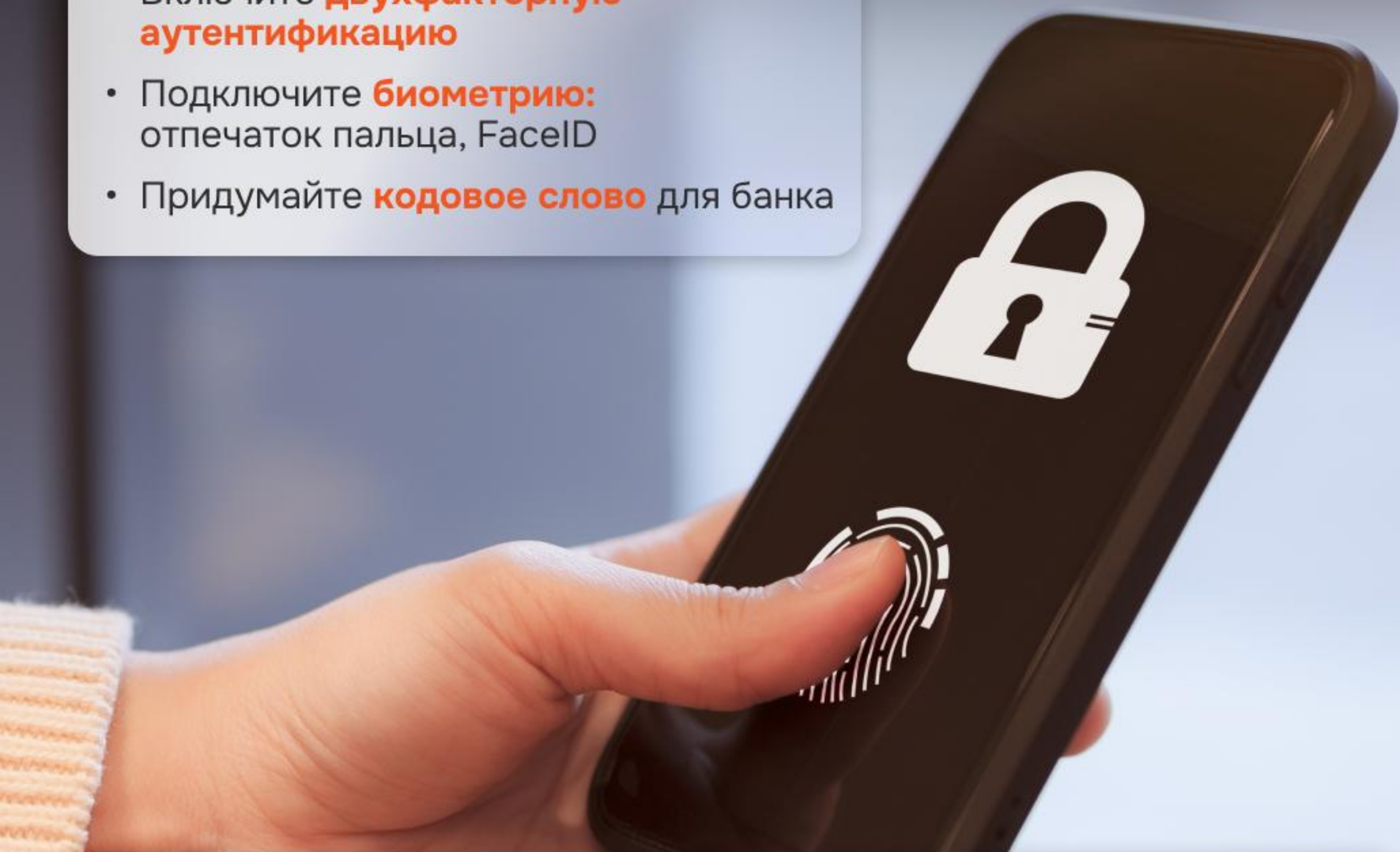
Хороший: A0r+Uc^T0|in^76



Установите двойную защиту — она ваш щит



- Включите **двухфакторную аутентификацию**
- Подключите **биометрию**: отпечаток пальца, FaceID
- Придумайте **кодовое слово** для банка



Важно: двойная защита должна быть на всех важных сервисах: социальные сети, Госуслуги, почта, мессенджеры и другие. Даже если ваш пароль украдут, вторая проверка не даст мошеннику войти в аккаунт.

Ваши данные = ваша безопасность. Будьте осторожны!



- Проверяйте **настройки приватности**: сделайте профиль закрытым, отключите лишний доступ к микрофону, камере, геопозиции
- Не передавайте **персональные данные** сомнительным сайтам/сервисам
- Отключите **автоматическое скачивание файлов** в мессенджерах
- Не переходите по **подозрительным ссылкам и QR-кодам**
- Своевременно обновляйте **программное обеспечение и операционную систему**
- Регулярно проверяйте свою **кредитную историю** через Госуслуги или Центральный каталог кредитных историй (ЦККИ)

Важно защищать свои данные, потому что это защищает ваши деньги и личную жизнь от мошенников.