Чем опасны вредоносные программы

Вредоносное ПО распространяется в магазинах приложений, рассылках, а также может быть предустановлено на устройствах перед продажей.

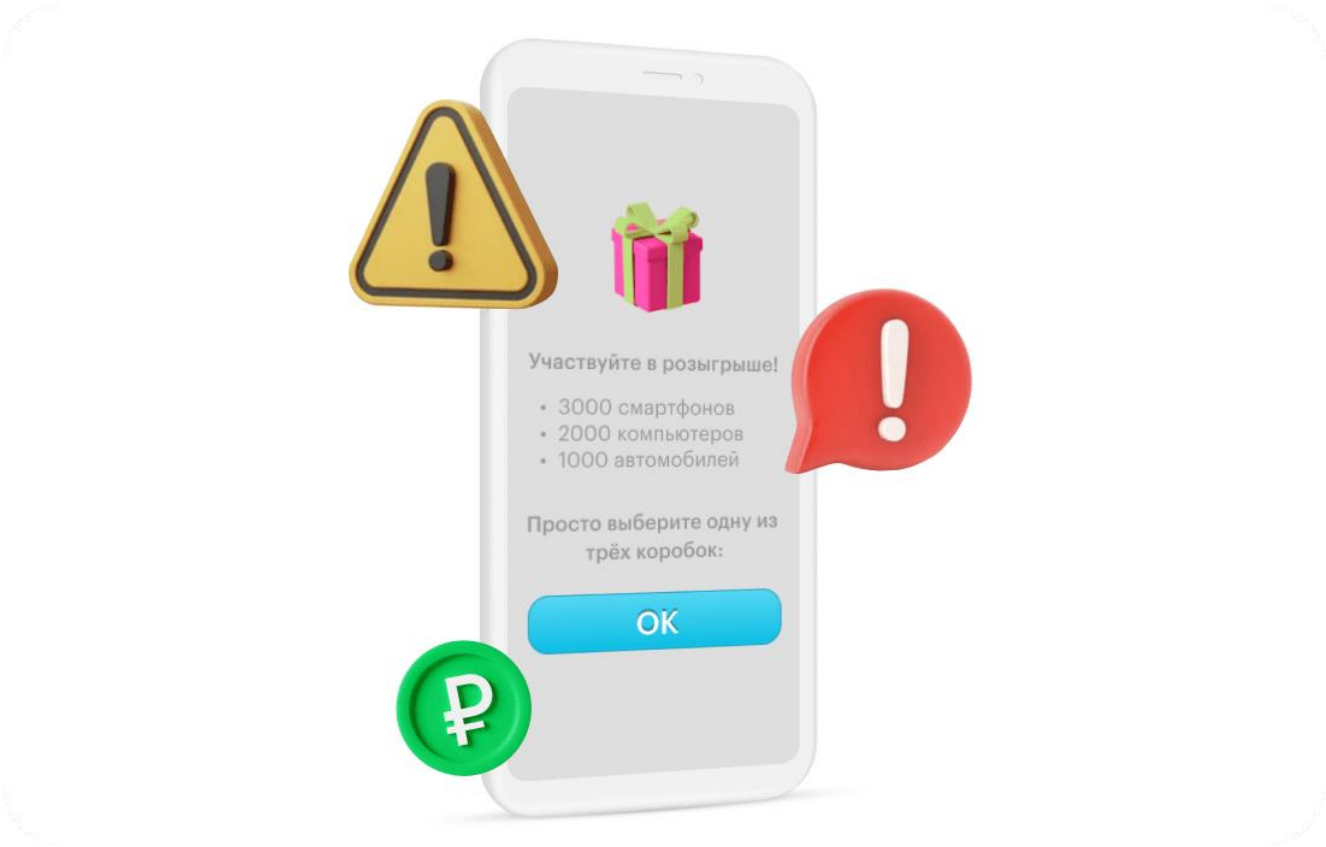
С помощью вредоносных программ мошенники могут получить доступ к данным банковских карт и другой конфиденциальной информации. На устройстве могут показывать рекламу без разрешения владельца и выводить деньги со счёта, используя мобильные трояны.

Какой ущерб наносит фишинг

Фишинг от англ. fishing — «рыбалка».

Мошенники используют подставные ссылки, имитирующие соцсети, банковские сайты или интернет-магазины, и предлагают пользователям поучаствовать в несуществующих розыгрышах призов.

При переходе по такой ссылке мошенники могут получить доступ к вашим данным: e-mail, банковской карте и другой личной информации.

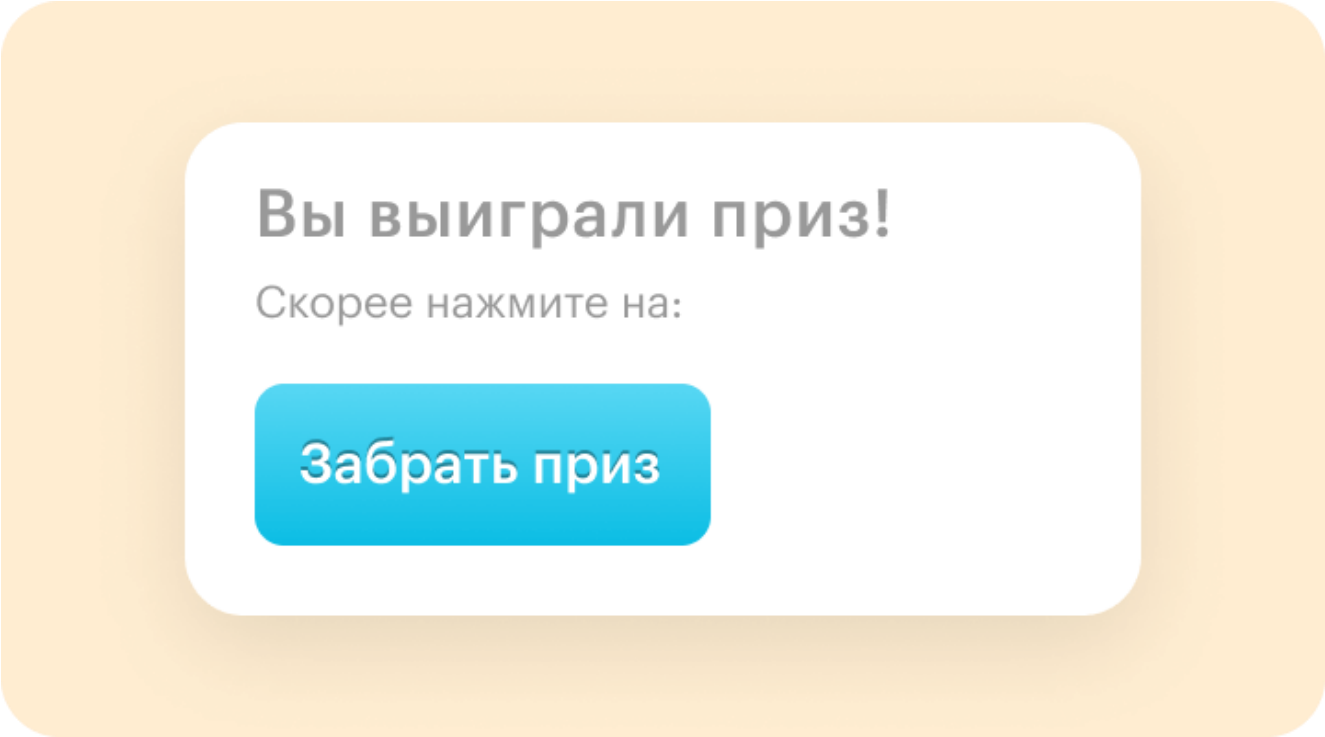


Ваш смартфон и данные в опасности, если

- С него скрытно отправляются SMS по списку контактов — к вам начинают обращаться знакомые, получившие сомнительные сообщения.
- В детализации услуг присутствуют SMS или вызовы, которые вы не отправляли и не совершали.
- Средства со счёта списываются быстрее, чем обычно.
- Списываются деньги с банковской карты, а вы ничего не покупали.

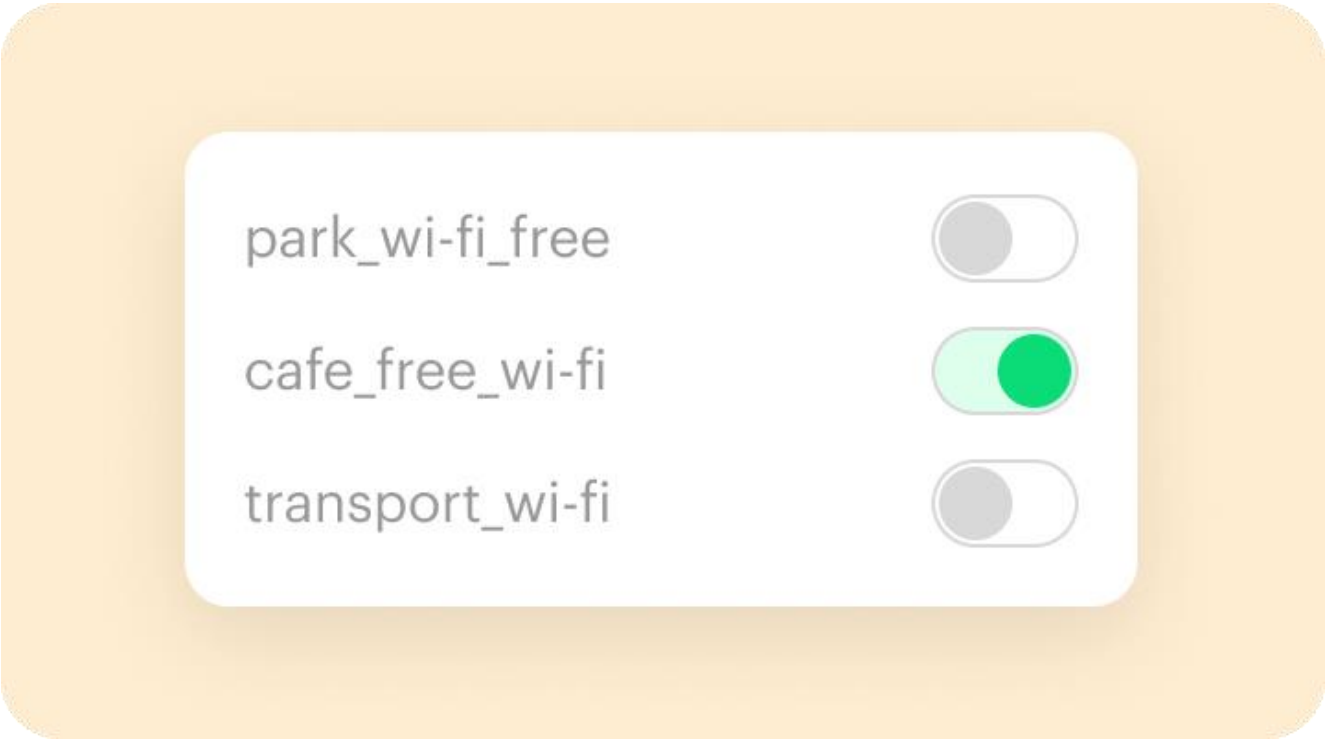
Рекомендации от провайдеров сотовой связи

Как защитить устройства от вредоносных программ и фишинга



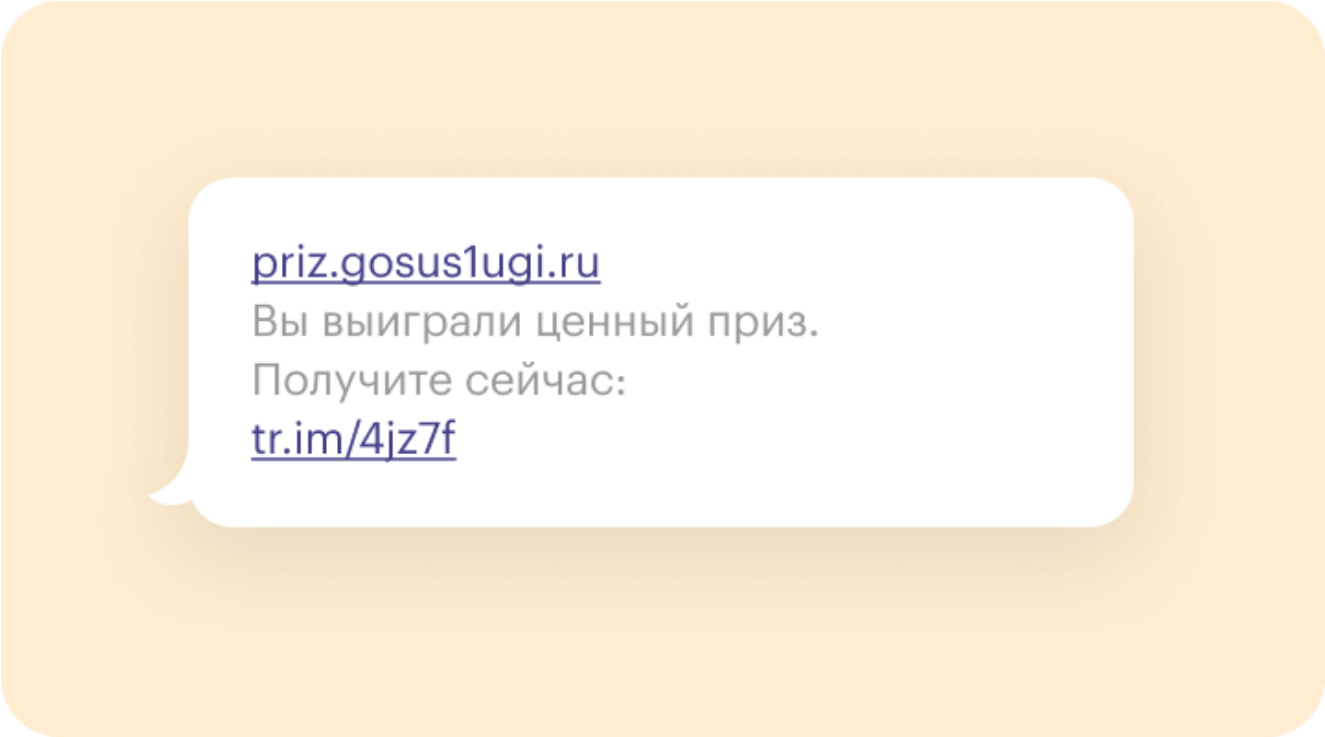
Не переходите по подозрительным ссылкам

Не открывайте ссылки из e-mail, SMS или сообщений в соцсетях, если не уверены в адресате. Если ссылку прислал друг, узнайте, отправлял ли он её



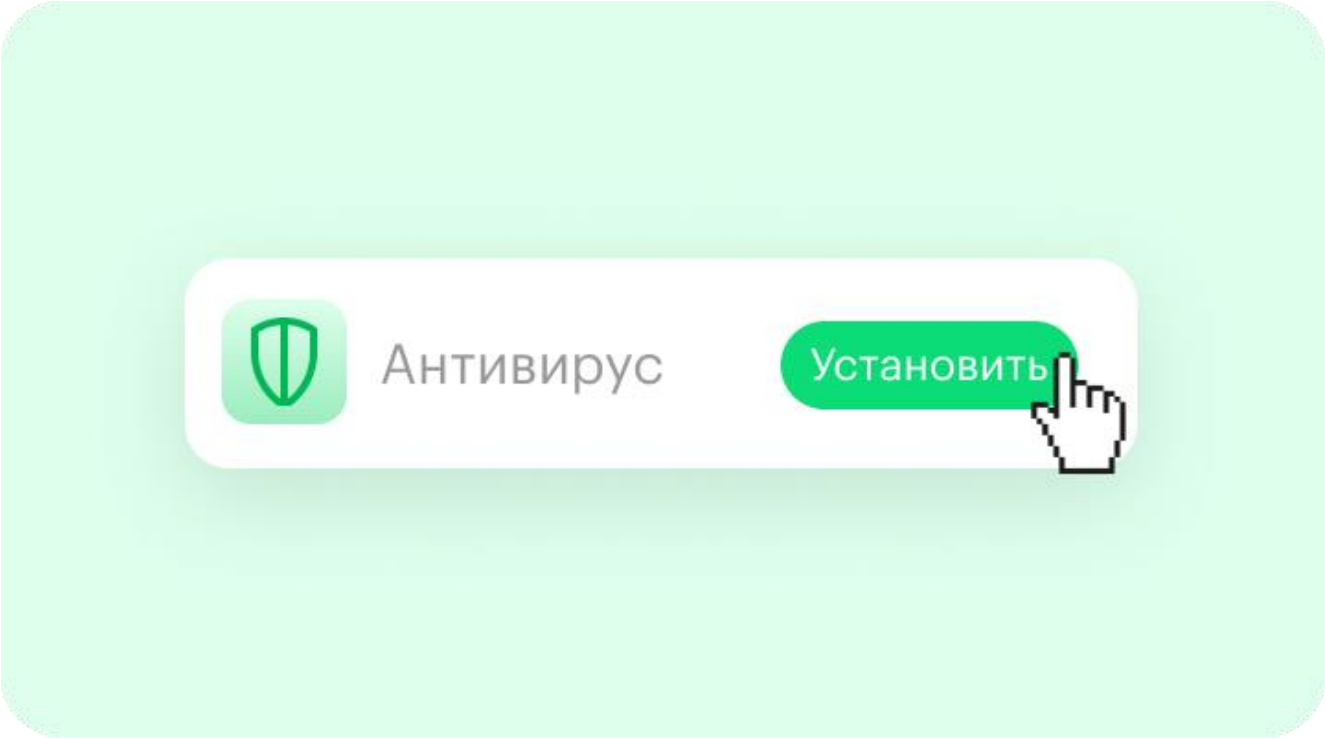
Будьте осторожны в общественном Wi-Fi

Проверяйте имя соединения и уточняйте IP-адрес у работника места с общедоступной сетью



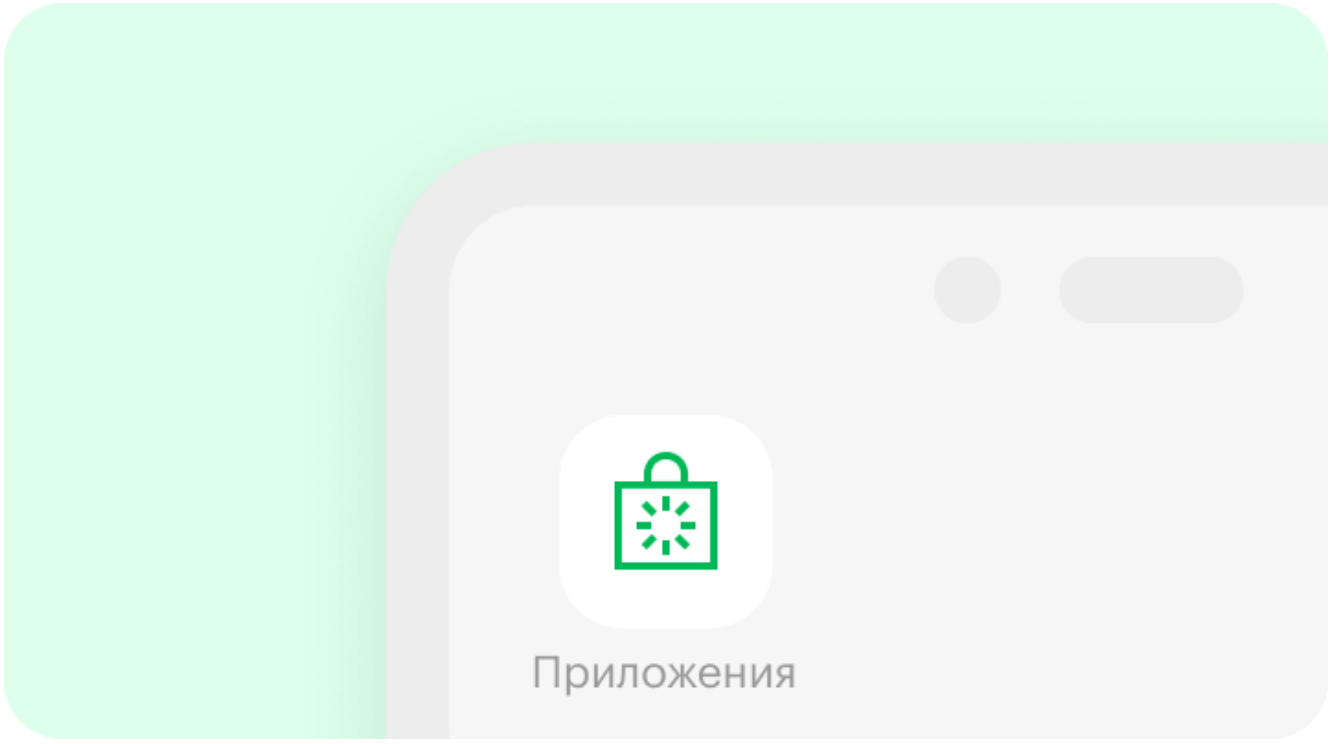
Проверяйте адрес сайта

Заходите только на официальные сайты, не верьте в обещания лёгких выигрышей и не переходите по сомнительным ссылкам



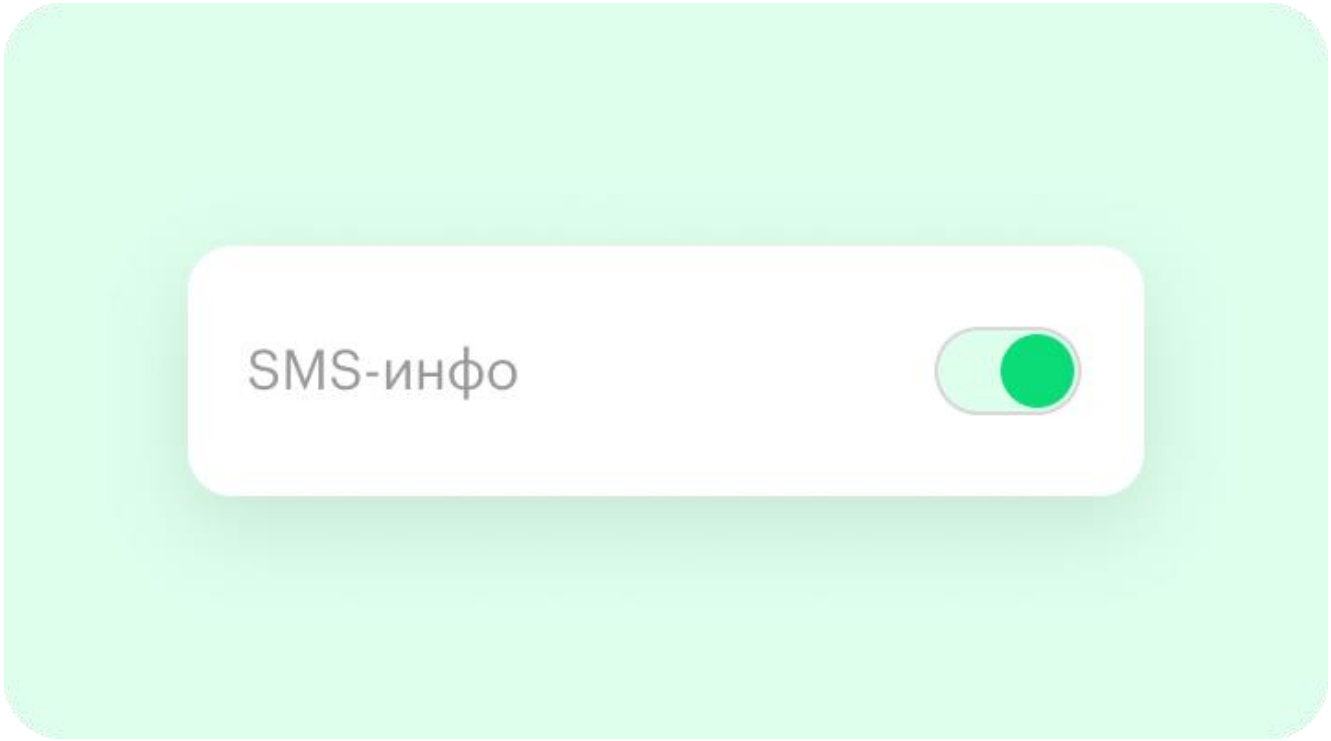
Используйте антивирус и обновляйте операционную систему

Установите антивирус, чтобы защитить устройство от вредоносных программ, регулярно обновляйте его и саму операционную систему устройства



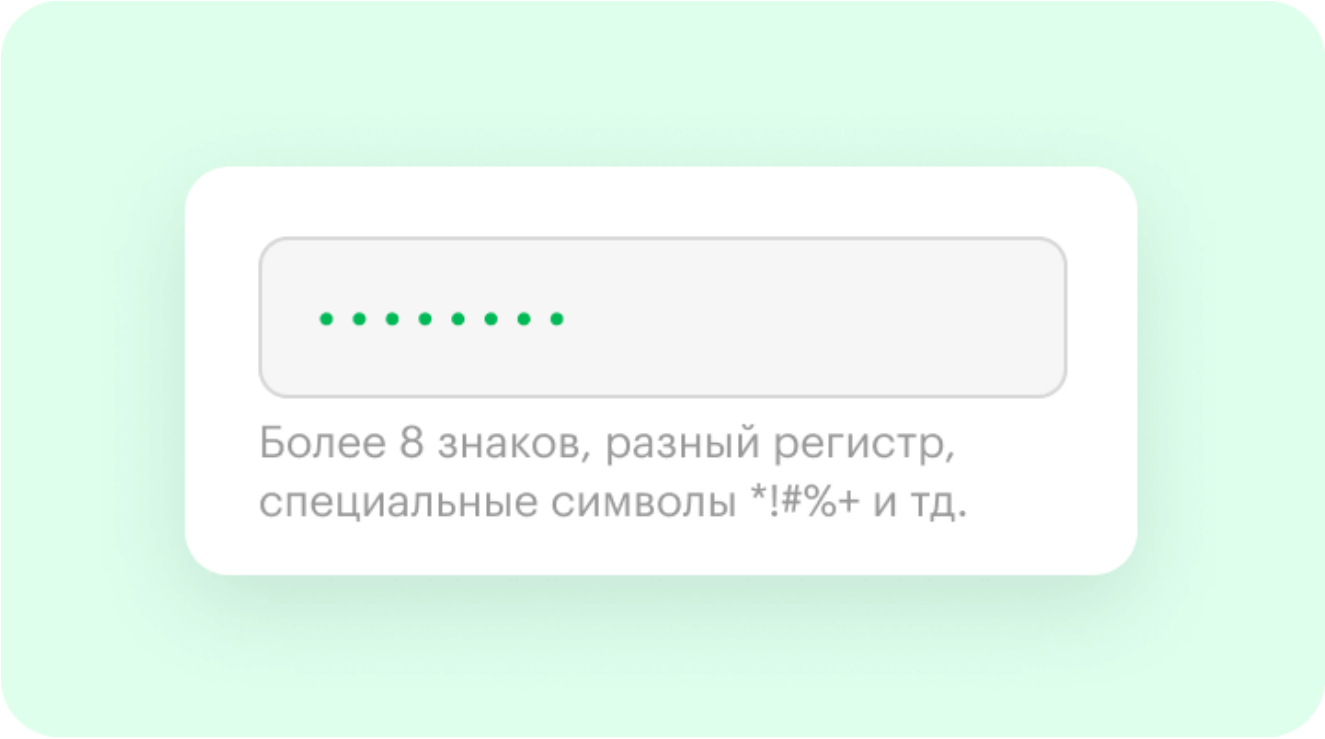
Устанавливайте приложения из официальных магазинов

Скачивайте программы и приложения только из официальных и проверенных магазинов и будьте осторожны при выдаче доступов — особенно на обработку вызовов и SMS



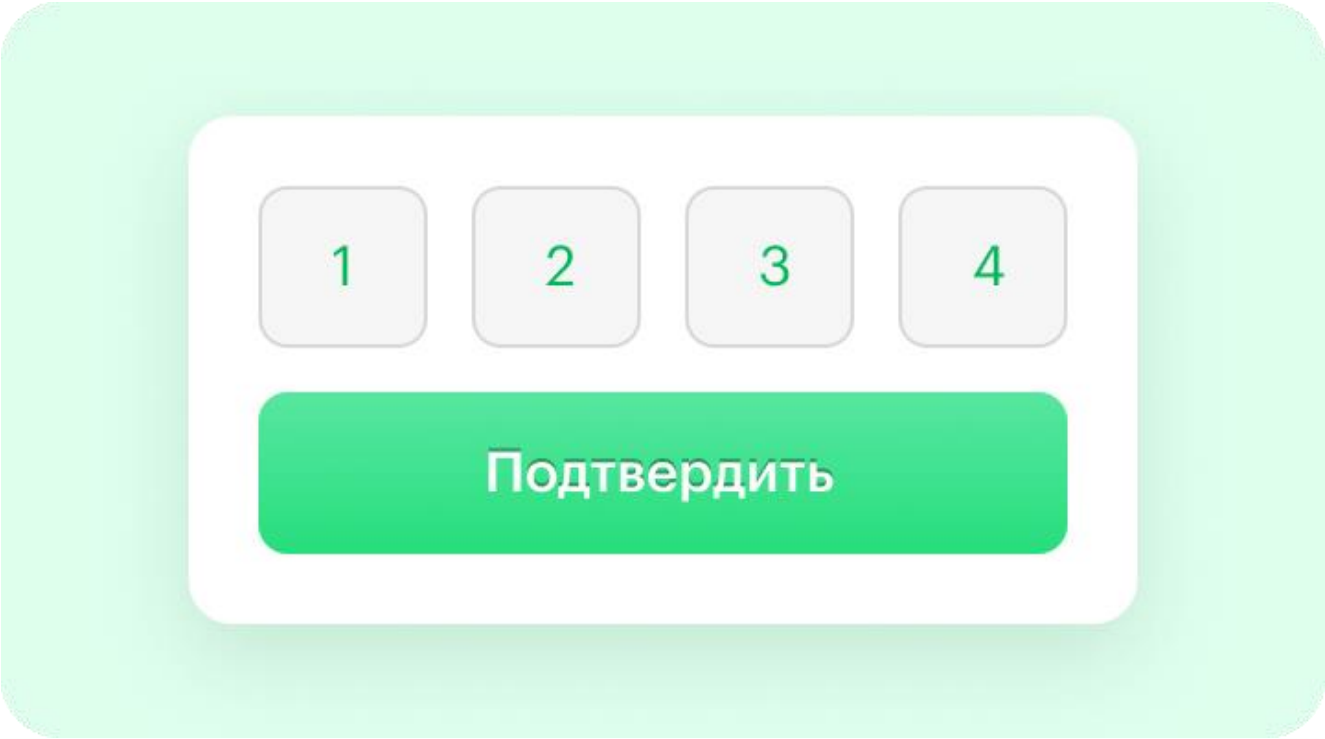
Контролируйте операции по вашей банковской карте

В приложении вашего банка подключите отправку SMS и уведомлений о списаниях



Используйте сложные пароли

Надёжный пароль состоит из прописных и строчных букв, цифр и специальных символов



Используйте двухступенчатый вход

Включите две ступени защиты ваших аккаунтов: пароль и код подтверждения, который приходит в SMS

Проверяйте содержание сайта

Обращайте внимание на ошибки в тексте, устаревший дизайн и адрес сайта — если в начале адресной строки отсутствует https, вероятно, эта страница небезопасна