

# Как защитить смартфон от мошенников



Финансовая  
культура



RuStore

# Скачивайте приложения из официальных источников

Вирусы можно подхватить через приложения, скачанные с подозрительных сайтов или форумов. Например, они могут содержаться в клонах мобильных банков и государственных сервисов. Чтобы обезопасить себя, устанавливайте и обновляйте программы только с сайтов разработчиков или официальных магазинов приложений, таких как RuStore.

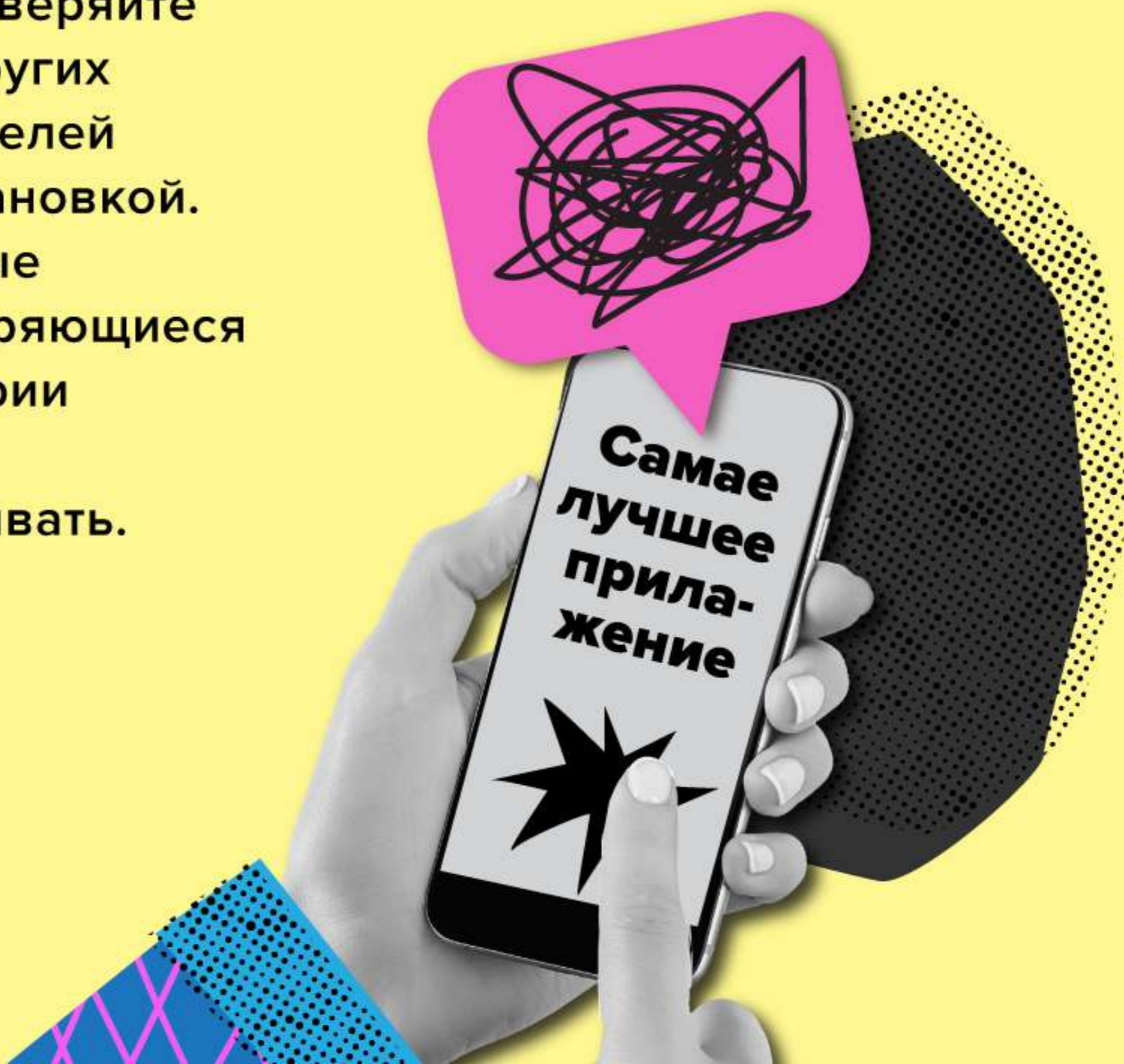
**СКАЧАТЬ**



# Обращайте внимание на описания

Внимательно читайте карточку приложения, которое собираетесь скачать. Если в названии присутствуют лишние буквы или их не хватает, а в описании – куча ошибок, есть вероятность, что это подделка.

Также проверяйте отзывы других пользователей перед установкой. Негативные или повторяющиеся комментарии должны настораживать.



# Следите за разрешениями

Иногда приложения запрашивают лишние данные. Например, калькулятор просит поделиться местоположением, а приложение с рецептами — доступом к списку контактов.

Обращайте внимание на эти разрешения. Если считаете, что сервису не нужен доступ к камере, телефону или другим настройкам, лучше им не делиться.



# Используйте актуальную версию антивируса

Регулярно проверяйте смартфон на наличие вирусов. Это особенно важно при подозрительной активности устройства — например, когда начинают самостоятельно открываться приложения.

В RuStore можно проверить смартфон с помощью встроенного сканера от «Лаборатории Касперского». Он покажет все подозрительные приложения на вашем смартфоне и предложит их удалить.



# Обновляйте операционную систему и приложения

В обновленных приложениях разработчики часто рассказывают о том, какие ошибки и уязвимости прежней версии они устранили. Мошенники пользуются этой информацией и в первую очередь пытаются атаковать пользователей, которые еще не успели обновить операционную систему или приложения. Чтобы не рисковать, своевременно устанавливайте новые версии.

