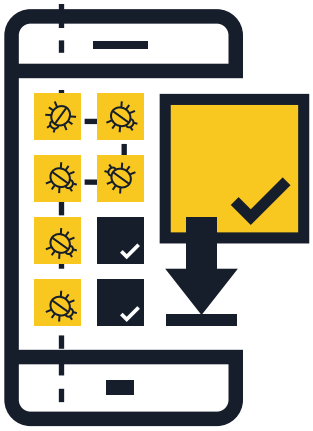
ВРЕДОНОСНОЕ ПО ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

КАК ЗАЩИТИТЬСЯ: СОВЕТЫ И РЕКОМЕНДАЦИИ

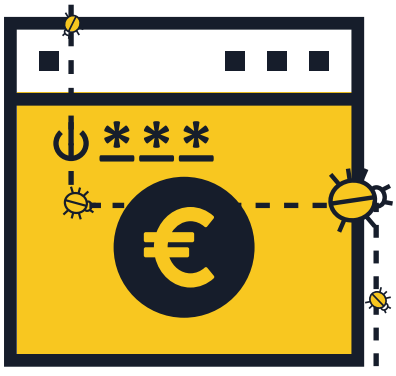


1 Устанавливайте приложения только из проверенных источников

- **Покупайте в известных магазинах приложений** — Перед загрузкой приложения узнайте больше о самом приложении и его издателе. Опасайтесь ссылок, поступающих по электронной почте и в текстовых сообщениях, - они могут подтолкнуть вас к установке приложений от третьих лиц либо из неизвестных источников.
- **Поинтересуйтесь отзывами пользователей и рейтингами**, если есть такая возможность.
- **Просмотрите разрешения приложения** — Проверьте, к каким данным имеет доступ это приложение и может ли оно передавать информацию наружу. Если условия установки вызывают подозрение или доставляют беспокойство, не загружайте это приложение.

2 Не нажимайте на ссылки или вложения в электронных письмах или текстовых сообщениях, которых вы не ожидали получить

- **Не доверяйте ссылкам в электронных письмах или текстовых сообщениях** (SMS и MMS), которых вы не ожидали получить, — сразу удаляйте их.
- **Тщательно проверяйте сокращённые интернет-адреса и QR-коды** — они могут привести вас на опасные веб-сайты либо непосредственно загрузить на ваше устройство вредоносное ПО. Чтобы подтвердить действительность веб-адреса, прежде чем нажать на него, воспользуйтесь инструментами, позволяющими выполнить предварительный просмотр сайта. Перед сканированием QR-кода запустите считыватель QR-кодов с предварительным просмотром веб-адреса в коде и используйте ПО для защиты мобильных устройств, предупреждающее о сомнительных ссылках.



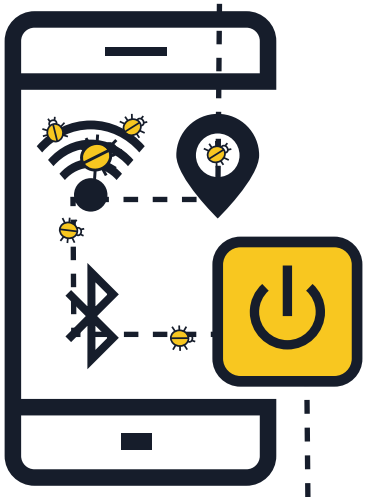
3 Совершив платёж, выходите из учётной записи на сайте

- **Никогда не храните в мобильном браузере или приложениях имена пользователей и пароли** — Если ваш телефон или планшет будет потерян или украден, в ваши учётные записи сможет войти любой. По завершении операции выйдите из учётной записи на сайте, а не просто закройте браузер.
- **Не пользуйтесь банковскими услугами и не совершайте покупок с использованием общедоступных сетей Wi-Fi** — Пользуйтесь онлайн-банкингом и совершайте операции только с использованием известных и надёжных сетей.
- **Тщательно проверяйте адреса сайтов** — Прежде чем войти в систему или послать конфиденциальную информацию, убедитесь в правильности веб-адреса. Загрузите официальное приложение вашего банка, чтобы быть всегда уверенными в том, что вы используете настоящий банковский сайт.

4 Регулярно обновляйте операционную систему и приложения

- **Загружайте обновления ПО для операционной системы вашего мобильного устройства, как только их вам предложат** — Самые свежие обновления гарантируют повышение не только безопасности вашего устройства, но и повышение его производительности.

5 Отключайте Wi-Fi, службы определения местонахождения и Bluetooth, когда они не используются



■ **Отключайте Wi-Fi, если он не используется**— Если соединение не защищено, киберпреступники могут получить доступ к вашей информации. Если есть возможность, вместо точек доступа используйте передачу данных через подключение 3G или 4G. Также вы можете выбрать режим виртуальной частной сети (VPN) для шифрования своих данных во время их передачи.

■ **Не разрешайте приложениям использовать без необходимости службы определения местонахождения** — Эта информация может стать известна другим и в дальнейшем использоваться для отправки рекламных сообщений в зависимости от вашего местонахождения.

■ **Отключайте Bluetooth, когда он вам не нужен** — Убедитесь, что он полностью отключён, а не просто пребывает в скрытом режиме. Часто базовые настройки позволяют другим пользователям подключаться к вашему устройству, не ставя вас об этом в известность. Злоумышленники могут скопировать ваши файлы, получить доступ к другим связанным устройствам и даже вашему телефону, чтобы совершать звонки и слать текстовые сообщения на немалые суммы.

6 Избегайте предоставления персональных данных

■ **Никогда не указывайте персональную информацию** в ответах на текстовые сообщения или электронные письма, присланные якобы вашим банком либо иной компанией. Вместо этого непосредственно свяжитесь с ними для подтверждения такого запроса.

■ **Регулярно просматривайте выписки по своему мобильному на предмет подозрительных начислений** — Если вы заметили расходы, которых не совершали, незамедлительно обратитесь к своему поставщику услуг.

7 Не делайте полного снятия ограничений (“джейлбрейк”) на своём устройстве

■ “Джейлбрейк” — это процесс снятия ограничений безопасности, определённых разработчиком операционной системы, с получением полного доступа к операционной системе и функциям. — **“Джейлбрейк” вашего устройства может существенно ослабить его безопасность,** обнаруживая бреши в безопасности, которые, возможно, ранее и не были очевидными.

8 Делайте резервные копии своих данных

■ **Многие смартфоны и планшеты способны к беспроводному резервному копированию данных** — Узнайте о вариантах резервного копирования в зависимости от операционной системы вашего устройства. Создав резервную копию для своего телефона или планшета, вы сможете легко восстановить свои персональные данные, если устройство потеряно, похищено либо повреждено.

9 Установите приложение мобильной безопасности

■ Все операционные системы уязвимы к заражению. Если есть возможность, **используйте решение для мобильной безопасности,** которое выявляет и блокирует вредоносное ПО, шпионские программы и вредоносные приложения, а также содержит другие функции конфиденциальности и защиты от хищения.