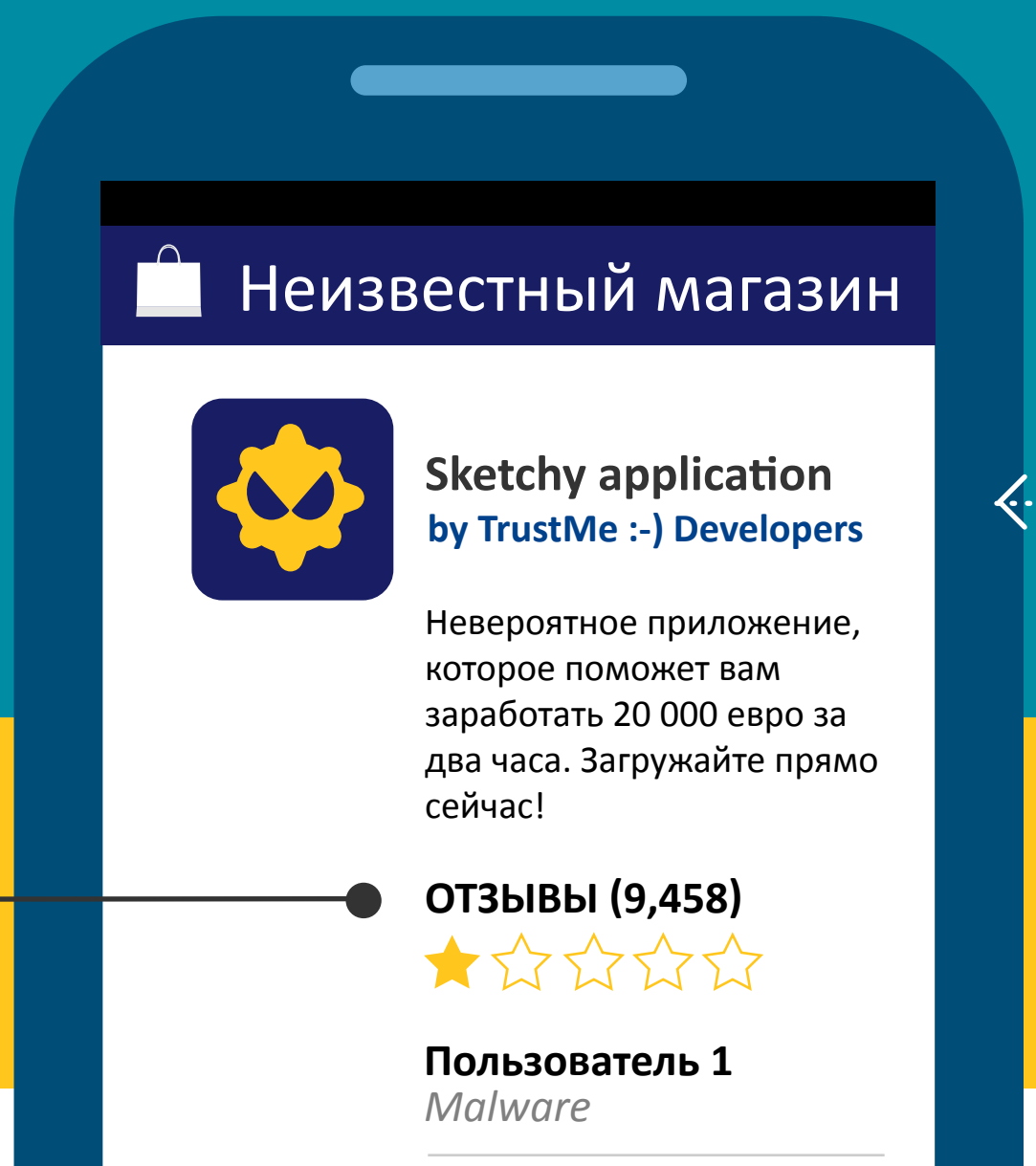
ПРИЛОЖЕНИЯ

ПРОСТО ИГРА?

Устанавливайте приложения только из официальных магазинов 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

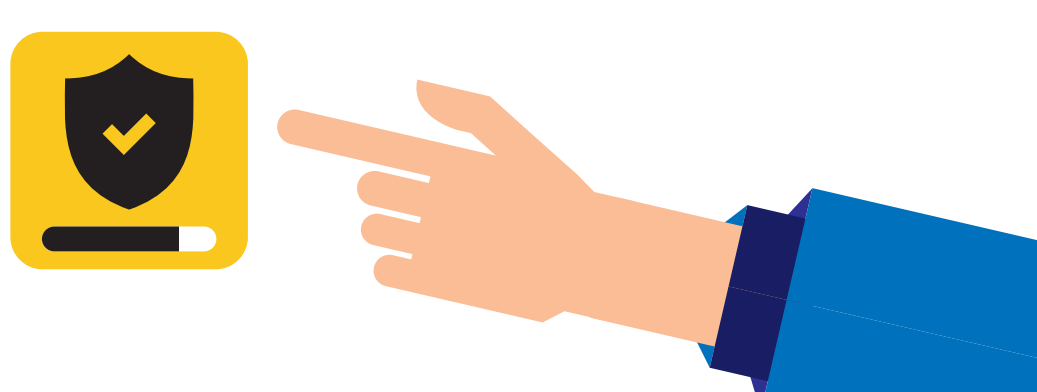


ПРОСМОТРИТЕ РАЗРЕШЕНИЯ ПРИЛОЖЕНИЯ

Проверьте, к каким данным имеет доступ это приложение и может ли оно передавать информацию наружу. Нужны ли приложению все эти разрешения? Если нет, — не загружайте его.

УСТАНОВИТЕ ПРИЛОЖЕНИЕ МОБИЛЬНОЙ БЕЗОПАСНОСТИ

Оно проверит все приложения, имеющиеся на вашем устройстве, а также каждое новое установленное приложение, и уведомит вас при обнаружении вредоносного ПО.



EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware

ВРЕДОНОСНОЕ ПО ДЛЯ МОБИЛЬНОГО БАНКИНГА

ВРЕДОНОСНОЕ ПО МОЖЕТ ДОРОГО ВАМ ОБОЙТИСЬ

Вредоносное ПО для мобильного банкинга предназначено для хищения финансовой информации, хранящейся в вашем мобильном устройстве.

КАК ОНО РАСПРОСТРАНЯЕТСЯ?

При посещении вредоносных веб-сайтов

При загрузке вредоносных приложений

Посредством фишинга

КАКИЕ РИСКИ?

Сбор информации, удостоверяющей вашу личность

Несанкционированное снятие денег

ЧТО С ЭТИМ ДЕЛАТЬ?

https://

Загрузите официальное мобильное приложение вашего банка и каждый раз проверяйте, действительно, ли вы находитесь на настоящем сайте банка.

Избегайте автоматического входа в учётную запись на банковском сайте или в приложении.

Никому не передавайте и не разглашайте номер вашей банковской карты и пароль.

Если есть возможность, установите приложение мобильной безопасности, которое будет уведомлять вас о любой подозрительной активности.

Если вы потеряли свой мобильный телефон или сменили номер, свяжитесь со своим банком для обновления информации.

Не передавайте информацию о вашем счёте текстовыми сообщениями или электронной почтой.

При подключении к мобильной версии сайта или приложению своего банка всегда пользуйтесь защищённой сетью Wi-Fi. Никогда не делайте этого посредством открытой сети Wi-Fi!

Периодически проверяйте свои финансовые выписки.

EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware

МОБИЛЬНОЕ ПО,
ТРЕБУЮЩЕЕ ВЫКУП

СКАЖИ “ПРОЩАЙ” СВОИМ ЛИЧНЫМ ФАЙЛАМ

Вымогательское ПО удерживает в заложниках ваше мобильное устройство и информацию, которая хранится на нем, требуя определённую денежную сумму. Этот тип вредоносного ПО блокирует экран вашего устройства либо доступ к файлам и функциям.

КАК ОНО РАСПРОСТРАНЯЕТСЯ?

При посещении скомпрометированных веб-сайтов.

При загрузке фальшивых версий настоящих приложений.

При открытии вредоносных ссылок или вложений, которые содержатся в фишинговых электронных письмах.

КАКИЕ РИСКИ?

Возможно, вам придётся сбросить своё устройство к заводским настройкам, потеряв все данные.

Злоумышленник может получить полный доступ к вашему устройству и поделиться вашими данными с третьими лицами.

ЧТО С ЭТИМ ДЕЛАТЬ?

Периодически делайте резервные копии своих данных и обновляйте все свои приложения и операционную систему.

Избегайте покупок в магазинах приложений, принадлежащих третьим лицам.

Если есть возможность, установите приложение мобильной безопасности, которое уведомит вас в случае компрометации вашего устройства.

Опасайтесь подозрительных электронных писем и веб-сайтов, а также слишком заманчивых предложений.

Никому не предоставляйте прав администратора вашего устройства.

Не платите выкуп. Заплатив, вы профинансируете преступность и подтолкнёте преступников к новым незаконным действиям.

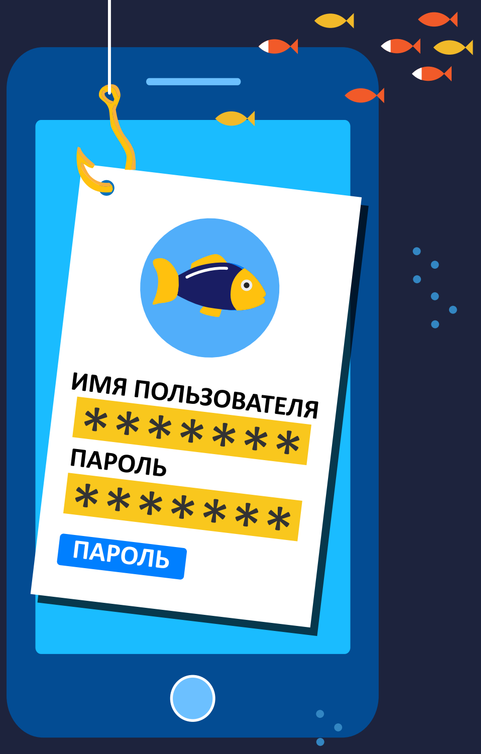
EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware

ВЕБ-УГРОЗЫ

ПРЕЖДЕ ЧЕМ ЧТО-ЛИБО НАЖАТЬ, ДВАЖДЫ ПОДУМАЙТЕ



Вы можете потерять свои деньги, персональную информацию, а также сохранённые данные, если устройство перестанет работать. Не попадитесь на крючок!

КАК ТАКОЕ ВОЗМОЖНО?

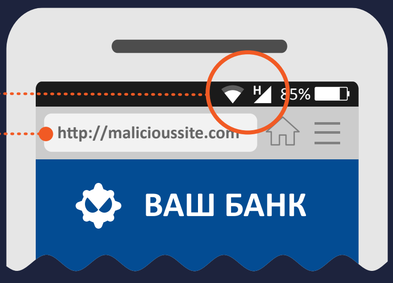
Фишинговые атаки: Распространяются через электронную почту, текстовые сообщения, социальные медиа и выманивают персональную информацию, выдавая себя за обращения легитимных компаний, которым пользователи доверяют.

Просмотр веб-сайтов: Ваше мобильное устройство может быть инфицировано просто при посещении опасного сайта.

Загрузка файлов: Вредоносные ссылки и вложения могут содержаться непосредственно в электронном письме.

ПОЧЕМУ ЭТО СТОЛЬ ДЕЙСТВЕННО?

Мобильные устройства **постоянно подключены** к сети Интернет.



Уменьшенный размер экрана устройства — это общий ограничивающий фактор. Браузеры для мобильных устройств показывают интернет-адреса в ограниченном пространстве экрана, в связи с этим сложно проверить домен.

Безоглядная вера пользователей в приватность мобильного устройства.

ЧТО С ЭТИМ ДЕЛАТЬ?

Относитесь с подозрением к SMS и звонкам от компаний, которые просят вас предоставить персональную информацию. Вы можете проверить, настоящие ли это сообщение или звонок, позвонив непосредственно по официальному номеру компании.

https://

Просматривая веб-страницы со своего мобильного устройства, убедитесь в том, что ваше соединение защищено по протоколу HTTPS. Вы всегда можете проверить так ли это, взглянув на начало интернет-адреса.

Никогда не нажимайте на ссылку или вложение в электронных письмах или SMS, получение которых вы не ожидали. Незамедлительно удаляйте такие сообщения.

^BE:%}
W@RY
*)Z#$=

Опасайтесь, попав на сайт с плохой грамматикой, орфографическими ошибками или низкой разрешающей способностью.

Если есть возможность, установите приложение мобильной безопасности, которое будет уведомлять вас о любой подозрительной активности.

EUROPOL EC3 European Cybercrime Centre

EMA

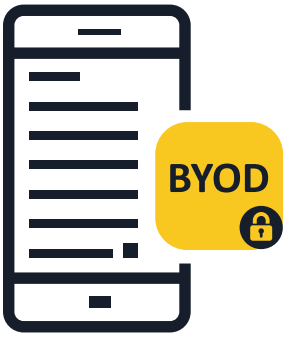
#MobileMalware

ВРЕДОНОСНОЕ ПО ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

СОВЕТЫ И РЕКОМЕНДАЦИИ ДЛЯ ПРЕДПРИЯТИЙ

1 Информируйте свой персонал о рисках мобильных устройств

- При эксплуатации мобильных устройств размывается грань между корпоративным и личным использованием. Предприятия могут серьёзно пострадать от атаки, изначально направленной на личное мобильное устройство. Мобильное устройство — это компьютер, и защищать его следует как компьютер.



2 Внедрение корпоративной политики для использования собственных устройств (BYOD)

- Работники, использующие свои мобильные устройства для доступа к информации и системам предприятия (даже если это лишь электронная почта, календарь или базы данных контактов), должны придерживаться политики компании. Тщательно выбирайте решения для управления и защиты мобильных устройств, а также мотивации вашего персонала быть осмотрительным.

3 Сделайте политику безопасности в отношении мобильных устройств частью вашей общей системы безопасности

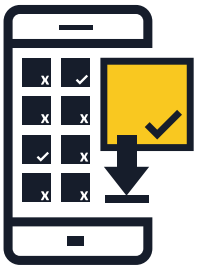
- Если устройство не соответствует политике безопасности, оно не может получить разрешение на подключение к корпоративной сети и доступ к корпоративным данным. Компаниям следует внедрять собственные решения для управления мобильными устройствами (Mobile Device Management, MDM) или управления корпоративными мобильными решениями (Enterprise Mobility Management, EMM).
- В дополнение к этому, крайне важно установить решение для защиты от мобильных угроз. Это обеспечит повышенную видимость и понимание уровня угроз для приложений, сети и операционной системы.

4 Опасайтесь использовать для доступа к корпоративным данным общедоступные сети Wi-Fi

- В целом, общедоступные сети Wi-Fi - небезопасны. Если работник осуществляет доступ к корпоративным данным с помощью бесплатного подключения Wi-Fi в аэропорту или кафе, эти данные могут быть доступными и для злоумышленников. В связи с этим компаниям рекомендуется разрабатывать политику “рационального использования”.

5 Регулярно обновляйте операционные системы и приложения

- Рекомендуйте своим работникам загружать обновления программного обеспечения для операционной системы их мобильных устройств, как только им это будет предложено. Изучайте политику операторов мобильной связи и производителей мобильных телефонов в отношении обновлений, - особенно это актуально для платформы Android. Самые свежие обновления гарантируют повышение не только безопасности вашего устройства, но и повышение его производительности.



6 Устанавливайте приложения только из проверенных источников

- На мобильных устройствах, которые подключаются к корпоративной сети, компании должны разрешать установку приложений только из официальных источников. Также возможен вариант создания корпоративного магазина приложений, в котором конечные пользователи смогут загрузить и установить приложения, согласованные компанией. Обратитесь к своему поставщику решений безопасности за рекомендациями в отношении настроек или разработайте собственное решение.

7 Предотвращение полного снятия ограничений (“джейлбрейка”)

- “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. В корпоративной среде не следует разрешать использование устройств с разблокированной учётной записью суперпользователя.

8 Рассмотрите варианты использования облачных хранилищ данных

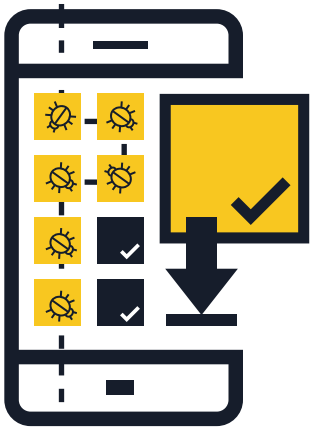
- Часто пользователи мобильных устройств хотят получать доступ к важным документам не только через свои рабочие компьютеры, а и, находясь за пределами офиса, - через личные телефоны или планшеты. Компаниям следует оценить возможность создания безопасного облачного хранилища и служб синхронизации файлов для безопасного удовлетворения подобных нужд.

9 Содействуйте тому, чтобы ваши сотрудники устанавливали приложения мобильной безопасности

- Все операционные системы уязвимы к заражению. Если есть возможность, обеспечьте, чтобы они использовали 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.

ВРЕДОНОСНОЕ ПО ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

КАК ЗАЩИТИТЬСЯ: СОВЕТЫ И РЕКОМЕНДАЦИИ

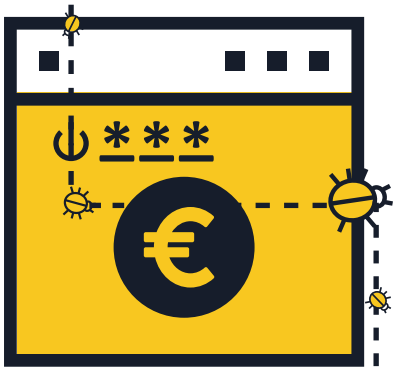


1 Устанавливайте приложения только из проверенных источников

- **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.



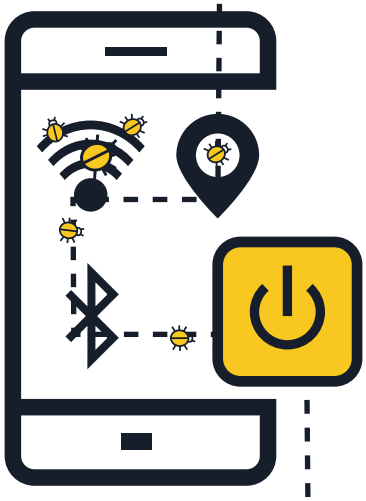
3 Совершив платёж, выходите из учётной записи на сайте

- **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.