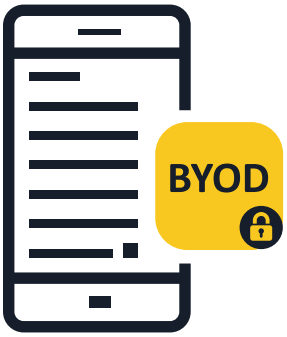
ВРЕДОНОСНОЕ ПО ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

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

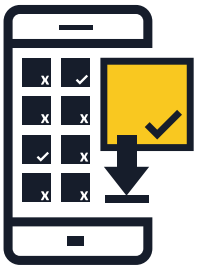
- Если устройство не соответствует политике безопасности, оно не может получить разрешение на подключение к корпоративной сети и доступ к корпоративным данным. Компаниям следует внедрять собственные решения для управления мобильными устройствами (Mobile Device Management, MDM) или управления корпоративными 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.