Твой мобильный телефон – опасный друг или верный помощник?

Только от тебя зависит, насколько надежным ты сделаешь свой любимый гаджет. Современные мобильные устройства очень сложны, и это дает злоумышленникам множество возможностей для проведения атак. Для взлома вашего смартфона может быть использовано буквально все — от Wi-Fi и Bluetooth до динамика и микрофона.

Мобильных телефонов в мире в 5 раз больше, чем компьютеров

Номофобия — боязнь остаться без мобильного телефона

Россияне проводят 4 часа в день в мобильных телефонах

В среднем около 110 раз в день человек разблокирует свой смартфон

В среднем у пользователя смартфона установлено 36 приложений

Основные правила для защиты мобильных устройств

1 Антивирусное ПО

Используй лицензионное антивирусное ПО для мобильных устройств.
Бесплатные средства защиты не всегда обеспечивают высокий уровень безопасности

2 Блокировка устройства

Обязательно используй для защиты пароль (графический, Touch ID, Face ID). Не используй в качестве пароля памятные даты и другую личную информацию. Используя графический или цифровой пароль, помни, что пальцы оставляют следы на экране. Эти следы можно увидеть, просто внимательно посмотрев на экран. Чаще протирай экран

3 Неиспользуемые сервисы

Отключай Wi-Fi и Bluetooth, если в данный момент они не нужны. Если Bluetooth все же включен, старайся не принимать никаких запросов на соединение и тем более файлов от неизвестных пользователей

4 Установка обновлений

Регулярно и своевременно обновляй программное обеспечение, в том числе операционную систему и все используемые приложения. В обновлении разработчик улучшает не только функционал, но и характеристики защиты

Твой мобильный телефон – опасный друг или верный помощник?

Основные правила для защиты мобильных устройств

5 **Сообщения от неизвестных источников**

Удаляй любой запрос с просьбой предоставить финансовую информацию или пароли. Не переходи по ссылкам, которые появляются во всплывающих окнах и в рекламных объявлениях

6 **QR-коды**

QR-коды не всегда отправляют пользователей на официальные, защищенные сайты. QR-код может содержать ссылку на мобильный вирус или загрузку нежелательных приложений. При переходе по распознанной ссылке убедитесь, что она привела именно на ожидаемый сайт

7 **Чистка приложений**

Удалите приложения, которыми больше не пользуетесь, или которые скачали когда-то «попробовать» и «на всякий случай». Меньше неожиданностей, больше свободного места

8 **Wi-Fi**

Используй защищенные точки доступа Wi-Fi, требующие ввода пароля. В открытых зонах Wi-Fi передаваемые данные (логины, пароли и т.д.) могут быть перехвачены

9 **Физическая защита устройства**

Держи устройство в поле зрения и не передавай другим людям

10 **Установка и разрешения приложений**

Контролируй разрешения приложений. Если приложение-фонарик требует доступ к сети, адресной книге и GPS-координатам, найдите фонарик поскромнее.
Не позволяй ему таскать ваши данные для решения чьих-то маркетинговых задач.
Для установленных приложений разрешения тоже можно контролировать (и отключать)