ФГБОУ ВО «Смоленский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
Кафедра мобилизационной подготовки здравоохранения и медицины катастроф с курсом ДПО

Информационная безопасность личности в социальных сетях

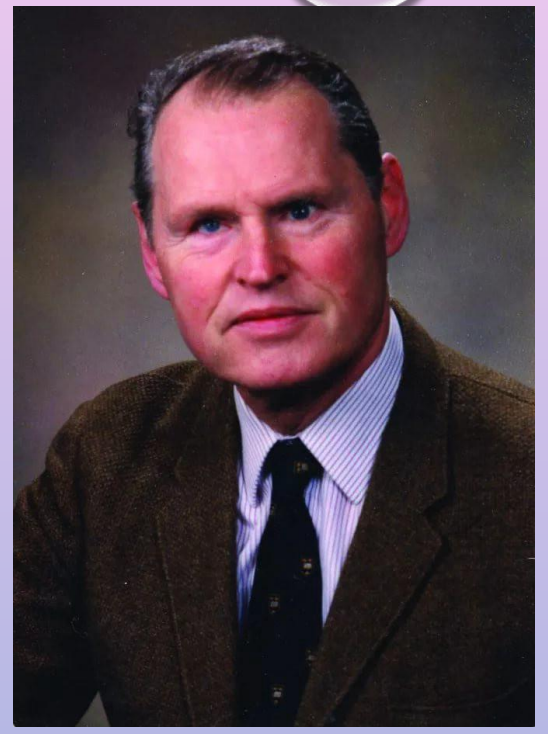
Выполнила: студентка 5 курса
514 группы
лечебного факультета
Маркова Оксана Викторовна.

Научный руководитель: Новикова Елена Васильевна.

Информационная безопасность личности в сети

Интернет-состояние и условие нахождение личности в информационном пространстве сети Интернет, использование различных сайтов и мессенджеров, при которых реализуется ее права и свободы.

Термин «социальная сеть» впервые введен **Джеймсом Барнсом в 1954 г.** в работе «Классы и собрания в норвежском островном приходе».



Социальная сеть — социальная структура, состоящая из группы узлов, которыми являются социальные объекты (люди или организации), и связей между ними (социальных взаимоотношений).

Существует множество примеров, когда информация в социальных сетях становится доступным третьим лицам…

В 2019 эксперты по информационной безопасности выяснили, что персональные данные известных пользователей Instagram попали в общий доступ. Пострадало почти 50 млн человек.

В каждой из утекших записей содержались личные данные блогеров Instagram, включая биографию, фотографии профиля, количество фолловеров, данные геолокации, электронную почту и номер мобильного телефона.

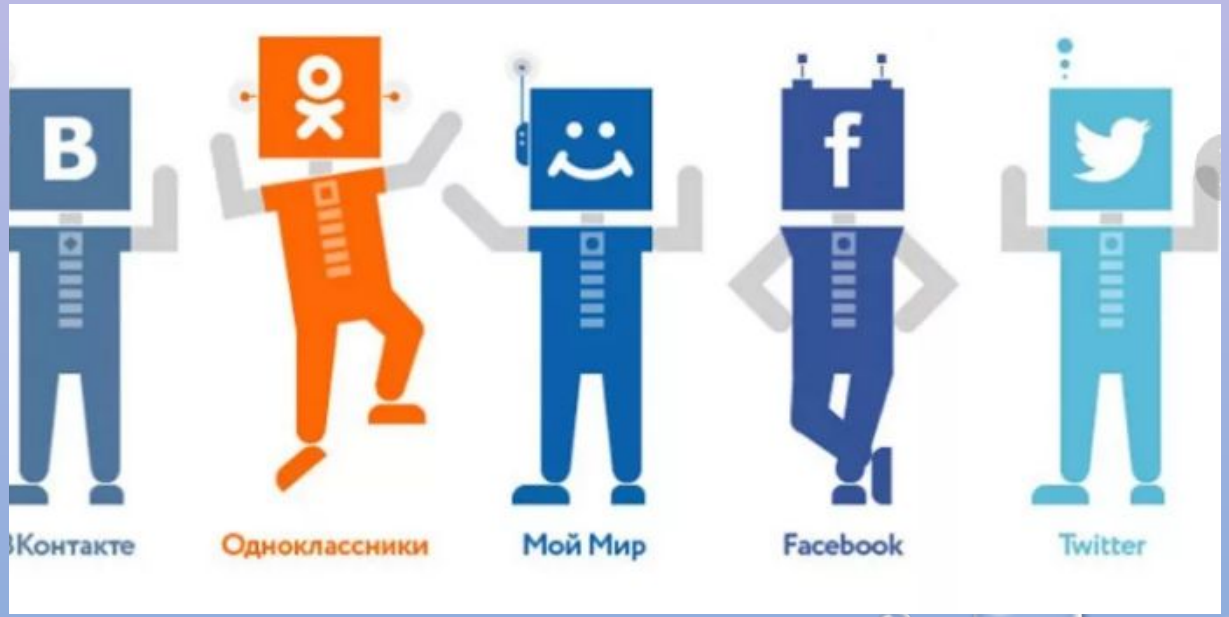
В статье В. Велюги проходит исследование трафика, отправляемого приложением «ВКонтакте» с мобильного устройства.

В результате чего обнаруживается, что данная социальная сеть, помимо своих метрик и телеметрий, отправляет такие данные о пользователе и его устройстве, как:

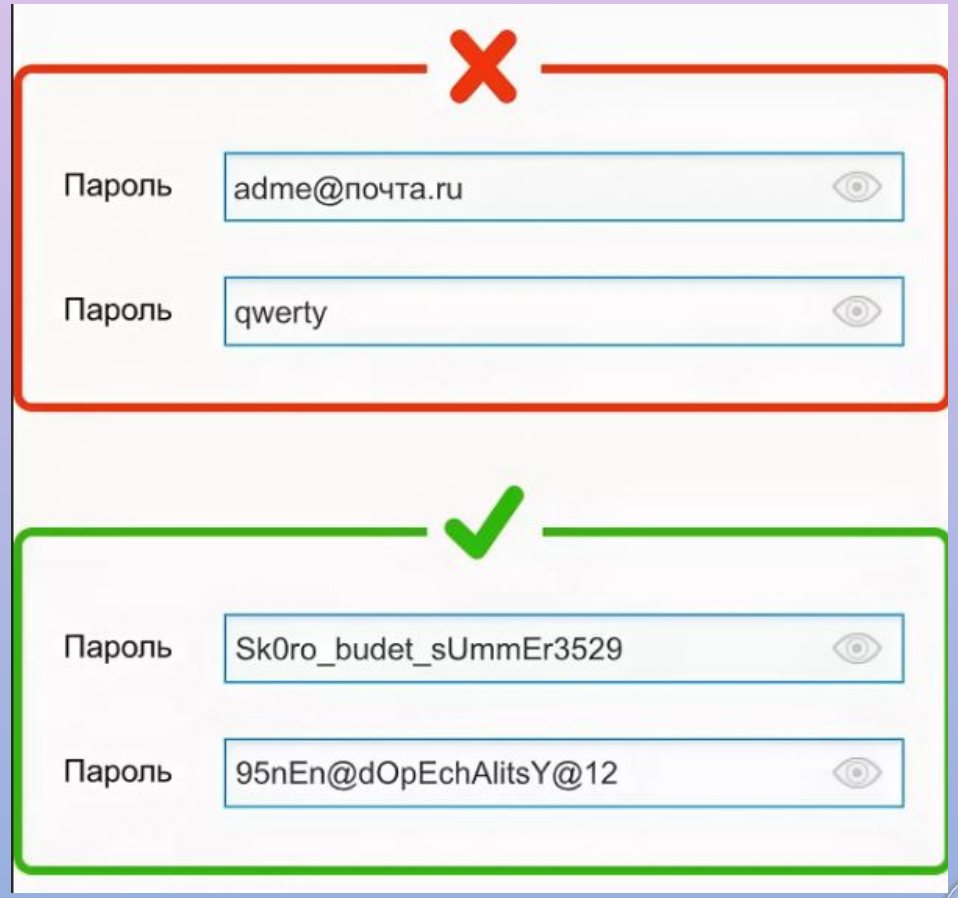
- текущее местоположение мобильного устройства;
- характеристики ближайших точек доступа в сеть Интернет;
- все действия, осуществляемые на смартфоне;
- считывается вся информация о самом устройстве, в том числе и данные о сим-карте.

3 апреля 2021 года пользователь хакерского форума бесплатно опубликовал в Интернете записи сотен миллионов пользователей Facebook.
По сообщению Business Insider, опубликованные данные содержат более 533 миллионов пользователей Facebook из 106 стран, в том числе более 32 миллионов записей о пользователях в США, 11 миллионов записей пользователей в Великобритании и 6 миллионов записей пользователей в Индии. Особо опасным является содержание утекших данных.
Записи содержат следующую информацию: телефонные номера, Facebook ID, имена и фамилии, местоположения, даты рождения, биографии, адреса электронной почты.

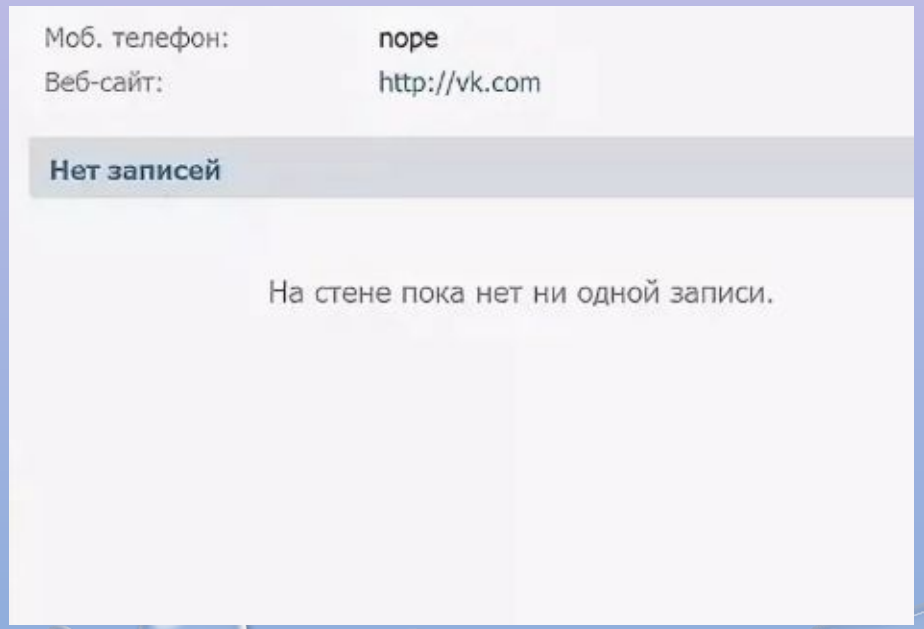
Правила, позволяющие сделать жизнь безопаснее



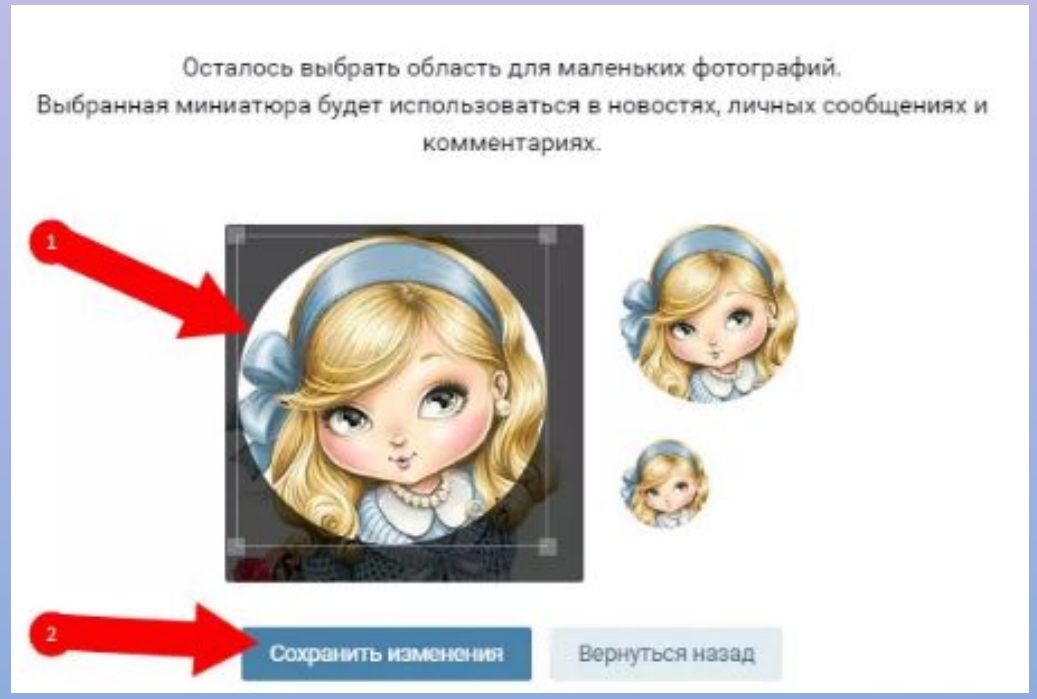
Придумывайте как можно более сложный и длинный пароль. Проявите фантазию в создании своего пароля: не стоит использовать в качестве пароля дату рождения, клички животных и др. Используйте название стихотворения, дату какого-нибудь события в истории и многое другое. Добавляйте в свой пароль символы, иностранные буквы, цифры. Для каждой социальной сети придумывайте свой пароль — так безопасность ваша и ваших страниц будет увеличена.



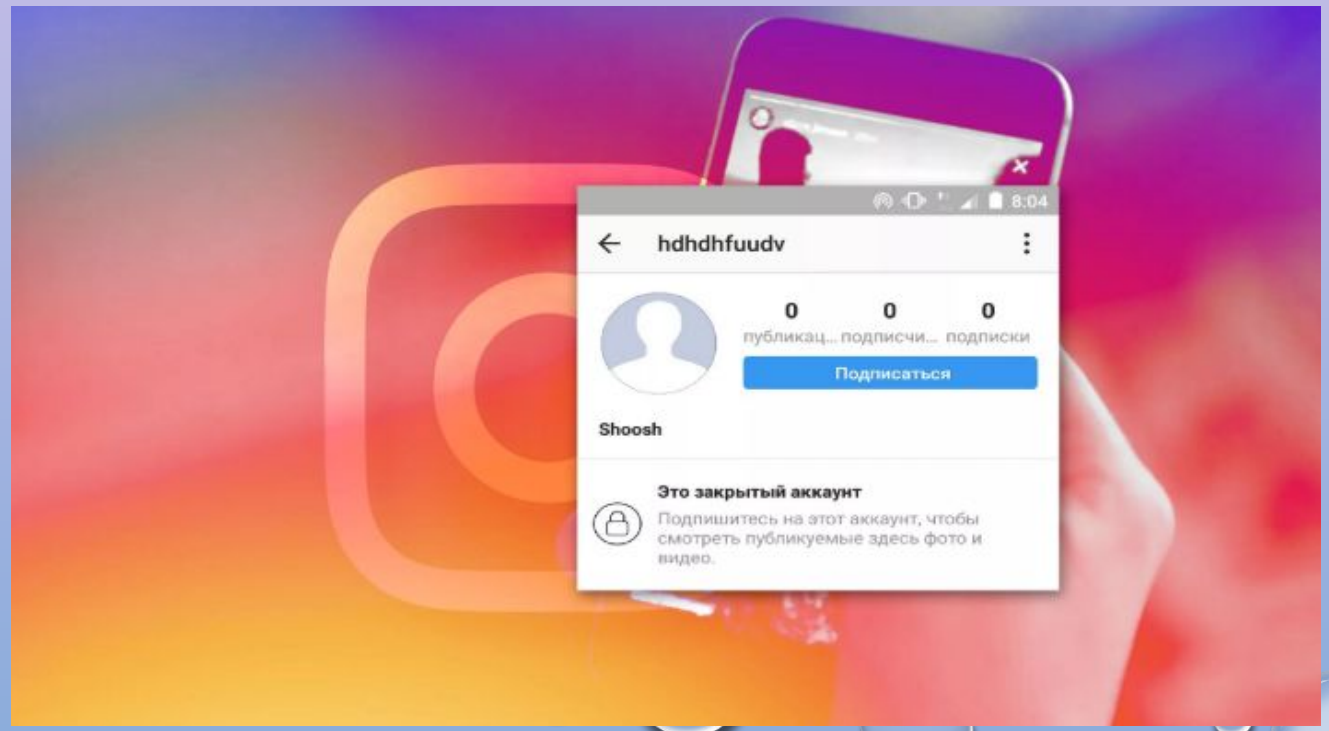
В своем профиле пишите как можно меньше о себе, ваших поездках, номерах телефонах и др. В такой социальной сети, как Instagram, пользователи рассказывают о своем распорядке дня, своем местоположении, личной информации о себе и так далее.



Перед тем как выложить фотографию, внимательно посмотрите на каждую деталь: на свой внешний вид, на окружающую местность, людей, находящихся рядом с вами, и многое другое.



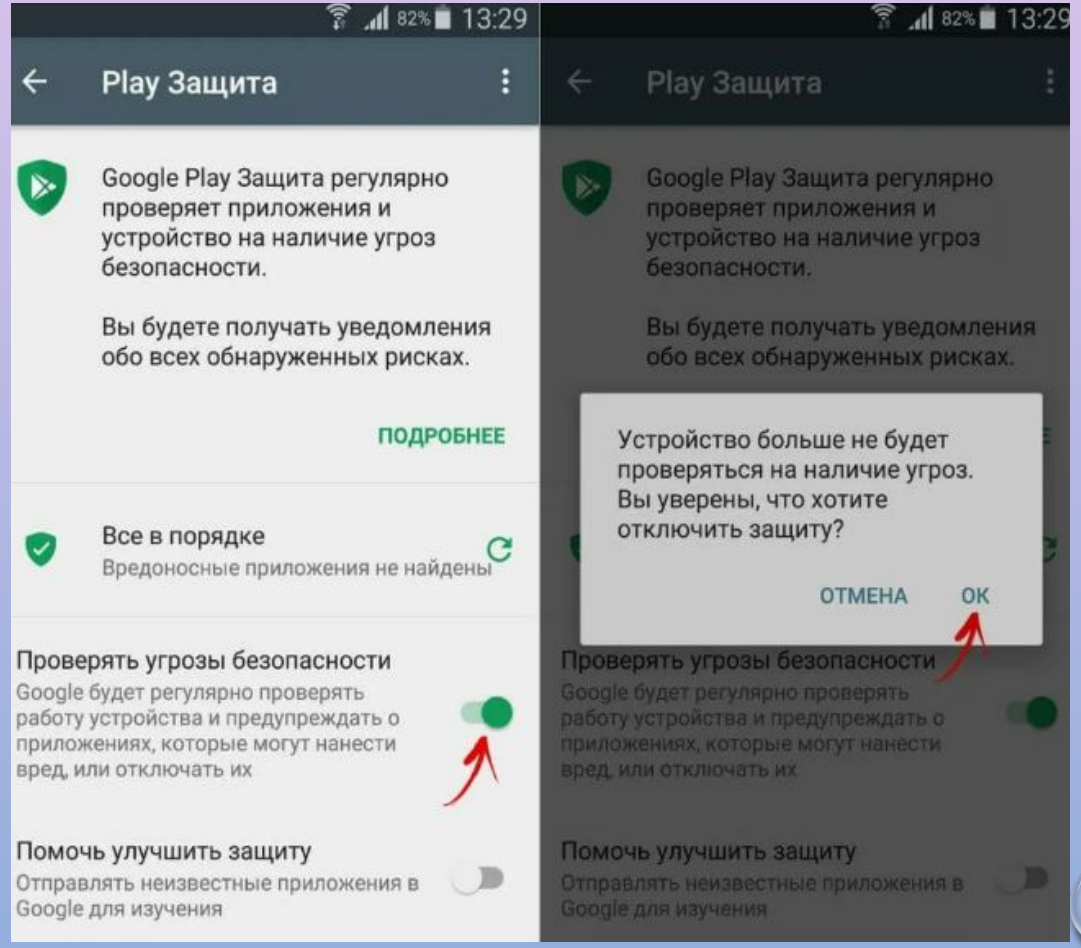
Конфиденциальность. Установите параметры конфиденциальности. Незнакомые вам люди не должны видеть важные сведения о вас, которые могут быть расположены на странице.



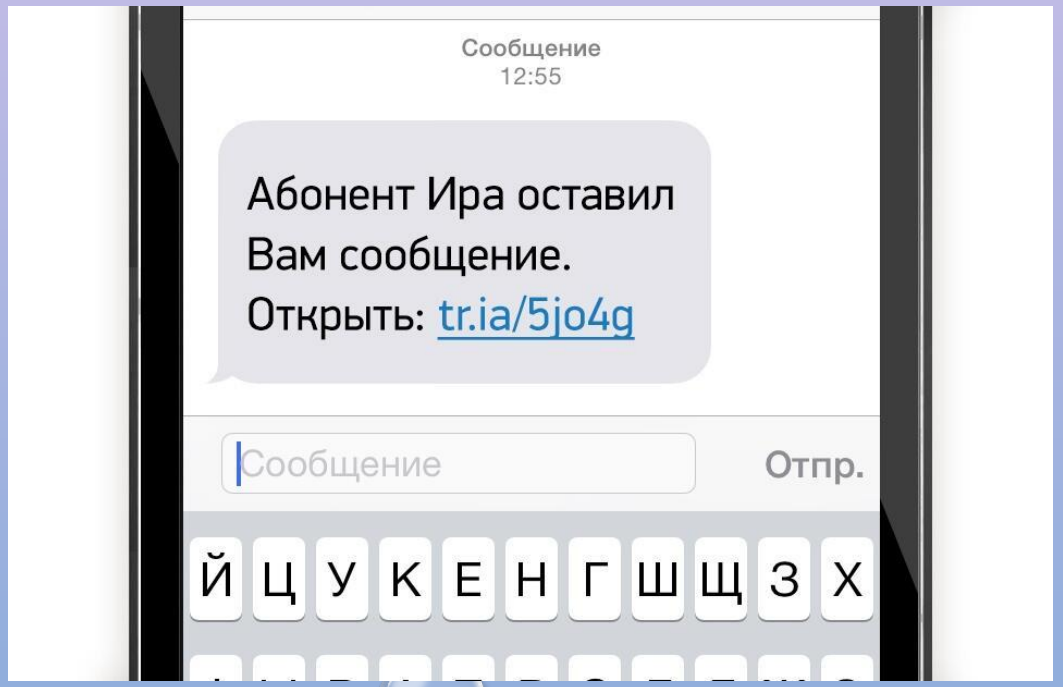
Используйте только надежные и проверенные браузеры, не забывайте про брандмауэр и антивирусную программу. Также не переходите на социальную сеть по случайным ссылкам из Интернета.

Никогда не переходите на незнакомые ссылки, которые присылают неизвестные вам люди. Не открывайте подозрительные сообщения. Мошенники с легкостью подлавливают таким образом людей и информацию о них, вплоть до взлома вашей страницы.

Перед тем как установить то или иное приложение, тщательно узнайте о нем и его безопасности, чтобы не попасться на уловку.

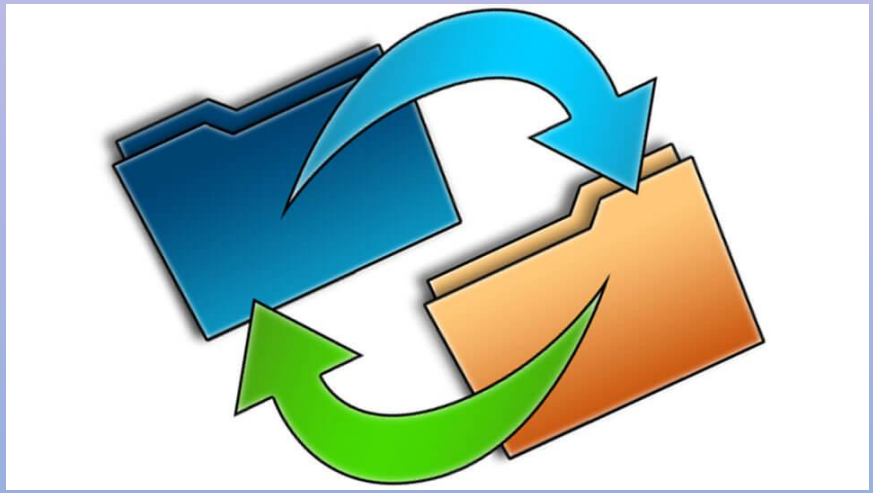


Общаясь с друзьями в сетях, будьте внимательны. Их страницы могут быть взломаны. На любое подозрительное сообщение от друга отреагируйте немедленно. Позвоните другу и убедитесь, он ли это вам отправил.



С осторожностью относитесь к выбору друзей. Если к вам добавляется незнакомый человек или присылает вам сообщение, тщательно подумайте, стоит ли отвечать ему. Быть может, это серьезно навредит вам.

Не используйте файлообменные сайты для получения пиратских программ, ведь вместо них может быть вирус.



Будьте осторожны при использовании Wi-Fi. Обычно почти каждый человек, увидев то, что нашлась бесплатная точка доступа, сразу подключаются к ней. А это может подвергнуть вас опасности. Если у вас есть возможность пользоваться сетью Virtual Private Network, которая позволяет вам работать в защищенной частной сети при общедоступном подключении, то обязательно воспользуйтесь.


БУДЬ
БДИТЕЛЬНЫМ! БДИТЕЛЬНЫМ!