

Основы безопасного использования социальных сетей.

Памятка для детей и их родителей.

Современный мир просто невозможно представить без компьютера, планшета, смартфона и, конечно же, без Интернета. Глобальная сеть дала нам многое: возможность молниеносно передавать информацию на расстояние, возможность оперативно узнавать новости со всего мира, возможность непрерывно общаться с людьми, даже если они находятся за тысячи километров от нас. Именно поэтому каждый человек ежедневно много времени проводит в интернете и аудитория интернета неумолимо растет, все больше детей и подростков создают аккаунты в социальных сетях, используют поисковые браузеры. Все это сопряжено с угрозой компьютерной безопасности.

В этой статье мы рассмотрим вопросы безопасного использования детьми и подростками таких социальных сетей, как «ВКонтакте», «Одноклассники», «Instagram».

Итак, какие же угрозы поджидают пользователей социальных сетей, особенно, если этими пользователями оказываются дети и подростки?

1. Киберхулиганы. Некоторые люди могут использовать интернет, чтобы запугивать или изводить других людей.
2. Хищение личной информации и вторжение в частную жизнь. Дети могут неосознанно оставлять конфиденциальную информацию о себе и своей семье.
3. Заражение компьютера (телефона, планшета) вредоносными программами. Это может произойти, если ребенок, например, перейдет по ссылке на неизвестный сайт.
4. Вовлечение в опасные или неприличные группы и сообщества.

Чтобы обезопасить себя, не стать жертвами «интернетных» хулиганов и пользоваться социальными сетями с удовольствием, предлагаем детям и их родителям воспользоваться несколькими простыми советами. Для начала напомним, что при регистрации в любой социальной сети нужно создать надежный пароль. Лучше всего воспользоваться генераторами паролей, но можно создать свой пароль, пользуясь следующими правилами:

- не используйте для пароля личные данные, которые могут быть известны не только вам (например, номер телефона, адрес, вашу фамилию или дату рождения);

- выбирайте для создания пароля символы разного регистра, чередуйте их с цифрами;
- не используйте один и тот же пароль для разных сайтов;
- периодически меняйте старый пароль.

Советы по безопасности для пользователей сети «Instagram»:

- не выкладывайте на всеобщее обозрение фотографии, содержащие личную информацию о вас или ваших близких;
- не размещайте на своей страничке слишком много фотографий, подробно иллюстрирующих вашу личную жизнь, или фотографий, которые могут вас скомпрометировать;
- сделайте ваш аккаунт закрытым, для этого зайдите в Параметры-Аккаунт и нажмите кнопку «Закрытый аккаунт». Эта функция позволит вам самим решать, кто из пользователей сети сможет просматривать ваши фотографии;
- добавляйте в подписчики вашей странички только тех людей, кого вы знаете и кому доверяете;
- не подписывайтесь на странички сомнительных пользователей или групп.

Советы по безопасности для пользователей сетей «ВКонтакте» и «Одноклассники»:

- не размещайте в своем профиле конфиденциальную информацию о себе и своих близких;
- не указывайте в профиле номер своего телефона, адрес;
- не размещайте на своей страничке слишком много фотографий, подробно иллюстрирующих вашу личную жизнь, или фотографий, которые могут вас скомпрометировать;
- обязательно сделайте свою страничку закрытой, для этого зайдите в Настройки-Приватность-Прочее и укажите, что вашу страничку могут просматривать только зарегистрированные пользователи, далее установите такие настройки, чтобы просматривать вашу страницу и поддерживать связь с вами могли только ваши друзья;
- добавляйте в друзья только тех людей, кого вы знаете лично;
- если кто-то из пользователей сети посылает оскорбления в ваш адрес, шлет вам спам или приглашает в различные сомнительные сообщества, вы можете установить для него ограничение просмотра вашей страницы и связи с вами, для этого зайдите в Настройки-

Черный список, нажмите кнопку «Добавить в черный список» и введите имя пользователя;

- не переходите по ссылкам, если не доверяете тому человеку, который вам их отправляет;
- если кто-то из ваших друзей начинает посылать вам сообщения странного содержания, неожиданно просить ваш номер телефона или обращаться с просьбой положить денег на его номер, не объясняя причин, скорее всего, вам пишет не друг, а мошенник, «взломавший» чужую страничку. Ни в коем случае не давайте мошенникам номер телефона, не переводите деньги, можете даже не отвечать ему. Предупредите вашего знакомого о «взломе» его аккаунта или пожалуйте администрации сайта;
- не вступайте в различные сомнительные или опасные сообщества и группы, оправдывая это тем, что вам просто интересно! Вы даже не заметите, как мошенники в сети завладеют вашим сознанием и заставят делать что-то для собственной выгоды или во вред вам!

Уважаемые родители, помните, что именно вы в первую очередь должны заботиться о безопасности ваших детей. Конечно, все мы идем в ногу со временем и понимаем, что не можем полностью запретить детям пользоваться интернетом, но мы можем обезопасить их и самих себя от различных неприятностей. Контролируйте использование вашими детьми социальных сетей, проверяйте, какую информацию они размещают и объясняйте, почему размещение некоторых сведений может быть опасным. Не игнорируйте сведения о том, в каких сообществах состоят ваши дети, чтобы вовремя уберечь их от рук мошенников и хулиганов.