Правила безопасности при использовании социальных сетей

Социальные сети, такие как Одноклассники, Вконтакте, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием. Хакеры, спамеры, разработчики вирусов, похитители личных данных и другие мошенники не дремлют. Эти советы помогут вам защитить ваши персональные данные при работе с социальными сетями.

- Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей. Не следует бездумно открывать все ссылки подряд - сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.
- Контролируйте информацию о себе, которую вы размещаете. Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля, система может предлагать ответить на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или старайтесь не использовать личные сведения, которые легко найти в сети.
- Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано. Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями
- Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки. Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
- Не добавляйте в друзья в социальных сетях всех подряд. Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.
- Не регистрируйтесь во всех социальных сетях без разбора. Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которой требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.
- Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены. На большинстве сервисов вы

можете в любой момент удалить свою учетную запись, но, не смотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.

- Проявляйте осторожность при установке приложений или дополнений для социальных сетей. Многие социальные сети позволяют загружать сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться также серьёзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.
- Старайтесь не посещать социальные сети с рабочего места. Любая социальная сеть может стать средой для распространения вирусов и других вредоносных или шпионских программ.

Забота о своей репутации в Интернете

Вполне вероятно, что у вас уже есть какая-то репутация в Интернете, даже если вы этого не хотите. На веб-сайтах в Интернете люди смогут найти информацию о вас. Вам следует знать о своей репутации в Интернете, чтобы вы могли защитить ее. Это важно как для детей, так и для взрослых.

Информация в Интернете может всплыть даже через несколько лет после ее публикации.

- Не смешивайте в Интернете свою личную и общественную жизнь. Используйте различные адреса электронной почты для различных действий в сети, это позволит вам разграничить вашу личную и общественную жизни.
- Задумайтесь при выборе фотографий.
- Следите за своей речью и тем, что вы публикуете. Следует всегда исходить из того, что все, что вы напишите в Интернете, сможет прочитать любой.
- Предпринимайте действия. Если вы найдете в Интернете неприглядную, неловкую или ложную информацию о себе, обратитесь к владельцу или администратору сайта с просьбой ее удалить.
- Храни свои персональные данные в тайне, особенно при общении во взрослых социальных сетях. Используй ник вместо своего настоящего имени на любом онлайн-сервисе, где много незнакомых людей может прочитать твою информацию. Спроси своих родителей прежде, чем сообщать кому-либо в интернете свое имя, адрес, номер телефона или любую другую персональную информацию.
- Дважды подумай прежде, чем разместить или рассказать о чем-нибудь в онлайн-среде. Готов ли ты рассказать об этом всем, кто находится в онлайне: твоим близким друзьям, а также посторонним людям? Помни, что, разместив информацию, фотографии или любой другой материал в сети, ты уже никогда не сможешь удалить его из интернета или помешать другим людям использовать его.

Принятие приглашений/дружбы

Большинство людей, с которыми ты общаешься в онлайн-среде, вероятно, уже являются твоими друзьями в реальной жизни. Ты также можешь установить контакт с друзьями твоих друзей. Очень часто это может быть забавным, однако готов ли ты действительно считать “другом” и поделиться информацией с фактически незнакомым тебе человеком, так же как ты делишься со своими лучшими друзьями?

В сети ты можешь общаться с людьми, ранее тебе неизвестными. Ты можешь получать просьбы от незнакомцев, которые хотели бы, чтобы ты включил их в твой список контактов и иметь возможность видеть твой профиль, но тебе не обязательно принимать их. Нет ничего плохого в том, чтобы отклонить приглашения, если ты в них не уверен. Получение большего количества контактов не является целью общения в социальной сети.

Это важно!

- Игнорируй плохое поведение других пользователей, уйди от неприятных разговоров или с сайтов с некорректным содержанием. Как и в реальной жизни, существуют люди, которые по разным причинам ведут себя агрессивно, оскорбительно или провокационно по отношению к другим или хотят распространить вредоносный контент. Обычно лучше всего игнорировать и затем заблокировать таких пользователей.
- Не размещай ничего такого, о чем ты бы не хотел, чтобы узнали другие, чего ты бы никогда не сказал им лично.
- Если тебя запугивают в онлайновой среде:

-игнорируй. Не отвечай обидчику. Если он не получает ответа, ему может это наскучить и он уйдёт;

-заблокируй этого человека. Это защитит тебя от просмотра сообщений конкретного пользователя;

-расскажи кому-нибудь. Расскажи своей маме или папе, или другому взрослому, которому доверяешь.

-сохрани доказательства. Это может быть полезным для поиска того, кто пытался тебя запугать. Сохрани в качестве доказательств тексты, электронные письма, онлайн-разговоры или голосовую почту.

- Сообщи об этом родителям, администрации школы, педагогам. Помни о Телефоне доверия (СПЦ Ошмянского района) 7-07-58. Областной телефон доверия 170. Телефон республиканской телефонной "горячей линии" - телефон доверия для детей (оказание психологической помощи несовершеннолетним, попавшим в кризисную ситуацию - телефон доверия для детей) 88011001611.

Специалисты подскажут тебе, как лучше поступить!

Не забудь выделить время для реальной жизни, для твоих друзей, занятий спортом и другой интересной деятельности!!!