**Правила безопасности при использовании социальных сетей**

1. **Установите комплексную систему защиты**. Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

2. **Пользуйтесь браузерами** MozillaFirefox, GoogleChrome и AppleSafari. Большинство червей и вредоносных скриптов ориентированы под InternetExplorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

3. **Не отправляйте SMS-сообщения**. Очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS. При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

4. **Используйте сложные пароли**. Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

5. **Старайтесь не использовать функцию запоминания паролей**, которую предлагают многие почтовые ящики и социальные сети.

6**. Проявляйте осторожность при переходе по ссылкам**, которые вы получаете в сообщениях .

7. **Если вам пришло сообщение с незнакомого адреса**, его лучше не открывать. Подобные письма могут содержать вирусы.

8. **При регистрации на сайтах, старайтесь не указывать личную информацию**

9. **Нежелательные письма от незнакомых людей называются «Спам»**. Если вы получили такое письмо, не отвечайте на него.

10. **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.

11. **Не добавляйте в друзья в социальных сетях всех подряд**.

**Памятка о правилах безопасного пользования детей интернетом и мобильной связью**

1. Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Прежде чем начать дружить с кем-то в Интернете, поставьте в известность родителей, спросите у них, как безопасно общаться.

3. При регистрации на сайтах старайтесь не указывать личную информацию т.к. она может быть доступна незнакомым людям. Где Вы живете, в какой школе учитесь, номер телефона должны знать только друзья и родственники.

4. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.

5. Нежелательные письма от незнакомых людей называются «спам». Если получили такое письмо, не отвечайте на него, покажите его родителям. В случае, если ответите на подобное письмо, отправитель будет знать, что Вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам «спам».

6. Если Вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

7. Необходимо знать, что если публикуете фото - видеоматериалы, каждый может посмотреть их.

Памятка для пользователей

**Как уберечь компьютер от заражения вирусом**

• Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

**Как защитить свои личные данные**

• Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

• Никому не сообщайте свой пароль. • Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.

• Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).

• Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

• Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

**Как не попасться на удочку смс-мошенников**

• Не отправляйте смс на незнакомые телефонные номера, за оправку таких смс могут взимать плату.

• Переводите деньги только на известные телефонные номера.

• Не вводите телефонный номер на незнакомых сайтах.

**Как избежать мошенничества при платежах**

• Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.

• Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.

• Храните банковскую карту в надежном месте.

• Не держите записанные пароли и коды рядом с картой.

• Заведите отдельную карту для покупок в интернете.

• Используйте для покупок в интернете только личный компьютер.

• Регулярно обновляйте антивирусную защиту компьютера.

• Старайтесь делать покупки в известных и проверенных интернет-магазинах.

• Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан

протокол https. Только этот протокол обеспечивает безопасную передачу данных.

• Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.

• Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.

• Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

**Памятка для обучающихся начальной школы**

Ты должен это знать:

* Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
* Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
* Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься и номер твоего телефона должны знать только родители и друзья.
* Никогда не отправляй свои фотографии людям, которых не знаешь лично. Компьютерный друг мог говорить о себе неправду. Ты ведь не хочешь, чтобы у незнакомого человека была твоя фотография, с которой он сможет сделать все, что захочет.
* Не встречайся с людьми, с которыми познакомился в Интернете, без родителей. Многие люди выдают себя не за тех, кем являются на самом деле.
* Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов - читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.
* Если тебя кто-то расстроил или обидел, обязательно расскажи об этом родителям.

Полезные ссылки:

1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon\_ metsa.html – о правилах безопасного поведения в сети Интернет с элементами интерактива;

2) http://www.nachalka.com/node/948 - учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;

3) http://content-filtering.ru/aboutus/ - информационно-аналитический ресурс «Ваш личный Интернет».