Информационная безопасность рекомендации школьникам

*Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с интернетом и даже использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.*

Как не подцепить вирус

1. Не открывай материал, присланный незнакомцами.
2. Не открывай сомнительный файл с вложениями, даже если ты получил его от своего знакомого. Свяжись с другом, от которого ты получил сообщение, и уточни у него, действительно ли он является автором послания
3. Не запускай и не скачивай файлы (например, музыку, фильмы, игры) из сомнительных источников.
4. Старайся не нажимать на рекламные баннеры, даже если они кажутся тебе очень заманчивыми.
5. Старайся не посещать сомнительные сайты или ресурсы.
6. Для защиты от спама:
   * Не выдавай в Интернет своего реального электронного адреса, есть риск использования твоего почтового ящика в качестве рассылки спама.
   * Старайся чаще менять пароли к электронной почте, к страничке в социальной сети и др.
7. Заведи себе два адреса — частный, для переписки (приватный и малоизвестный, который ты никогда не публикуешь в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее).
8. Если ты не пользуешься компьютером, старайся отключать его от соединения с Интернетом.

Борьба с вирусами

1. Не сохраняй на своем компьютере неизвестные файлы. Подозрительные сообщения лучше немедленно удалять:
   * удали сообщение из папки Входящие;
   * удали сообщение из папки Удаленные (Корзина);
   * выполни над папками операцию "Сжать" (Файл/Папка/Сжать все папки).

*Если твой компьютер заражен:*

1. Отключи компьютер от интернета и локальной сети.
2. Не пытайся самостоятельно решить проблему, не жми на все кнопки подряд, посоветуйся со взрослым.
3. Или если необходимо, обратись за помощью в службу технической поддержки производителя установленного на твоем компьютере антивирусного ПО.

*Если ты уверенный пользователь компьютера:*

1. Загрузи компьютер в безопасном режиме (включи компьютер, нажми и, удерживая клавишу F8, выбери Безопасный режим (Safe Mode) в открывшемся меню).
2. Проведи полную антивирусную проверку компьютера.
3. Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.

*Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: хакер незаконно получает доступ к личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб. Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.*

Предупреждение кибермошенничества

1. Ни под каким предлогом не выдавай незнакомым людям свои личные данные (домашний адрес, номер телефона и т.д.) и пароли.
2. Перед тем, как воспользоваться развлекательными услугами Интернета (скачать музыку, фильм и т.д.), проверь, что после этого тебя не попросят заплатить деньги.
3. Не верь всему, что видишь в Интернет.
4. Старайся остерегаться новых предложений и услуг, все они требуют вложения крупной суммы денег (например, местонахождение человека по номеру его мобильного, повышение рейтинга в социальной сети и т.д.)
5. Советуйся со взрослыми перед тем, как загрузить, скачать или установить ту или иную услугу.
6. Очень внимательно выбирай сайты, на которых ты хочешь сделать покупки и удостоверься в их надежности. Собери как можно больше информации о сайте, спросив, например, название, адрес и номер телефона центрального офиса, описания общих положений контракта и, особенно о том, как отменить заказ; кроме того выясни о защите и управлении личными данными и безопасности оплаты; и сравни цены, отыскав такой же предмет на других сайтах.
7. Если ты получил неожиданное электронное письмо, в котором тебе предлагается невероятно выгодная сделка, вероятность того, что это мошенничество, очень велика.

Борьба с кибермошенничеством

1. Если компьютер подцепил вирус, не отправляй смс сообщение, даже если тебе обещают таким образом очистить компьютер от вредоносных программ или разблокировать компьютер.
2. В случае взлома страницы в социальной сети — смени пароли.
3. Обратись за советом к взрослому.

*Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.*

Предупреждение кибербуллинга

1. Не сообщай свои данные агрессору (реальное имя, фамилию, адрес, телефон, номер школы и т.п.). Когда злоумышленнику становятся известны твои анкетные данные, происходит так называемый «троллинг» или травля.
2. Не открывай доступ к своей страничке незнакомым людям.
3. Следи за информацией, которую ты выкладываешь в Интернете
4. Придерживайся правил сетевой этики, не отвечай грубо на сообщения, этим ты можешь спровоцировать собеседника. Игнорируй сообщения от незнакомых, агрессивных и подозрительных личностей. Нужно понимать, что онлайн-общение не является приватным. Другие пользователи могут скопировать, распечатать или переслать твою личную переписку.
5. Если ты видишь или знаешь, что твоего друга запугивают, поддержи его и сообщи об этом.
6. Не посылай сообщения или изображения, которые могут огорчить кого-нибудь.

Борьба с кибербуллингом

1. Не предпринимай самостоятельных действий по наказанию агрессора
2. Немедленно обратись за советом к родителям или в специальные организации за помощью
3. Сделай снимок экрана с оскорблениями (screen-shot) и перешлите его модераторам ресурса.
4. Или напиши письмо в техподдержку с просьбой удалить аккаунт хулигана. Важно помнить, что адекватно отреагировав на неприятное сообщение, оповестив администрацию ресурса о киберхулигане, можно обезопасить от него, не только себя, но и остальных пользователей.
5. Если же преследование происходит лично, с помощью электронной почты, сервисов мгновенных сообщений (ICQ, Google talk и т.д.) или IP телефонии (Skype) избавиться от неприятного собеседника можно нажав клавишу «игнорировать» (или «черный список»). У большинства программ, предназначенных для общения, существует такая или аналогичная функция.

*Груминг — установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече.*

Предупреждение груминга

1. Следи за информацией, которую ты выкладываешь в Интернете. Не выкладывай свои личные данные в Интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.). Помни, любая информация может быть использована против тебя, в том числе в корыстных и преступных целях
2. Используй псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), пользовании он-лайн играми и других ситуациях
3. Не размещай и не посылай свои фотографии незнакомцам
4. Будь осторожен при общении с незнакомыми людьми. Старайся рассказывать как можно меньше информации о себе.

Борьба с грумингом

1. Если новый знакомый пытается говорить с тобой на неприятные или пугающие тебя темы и говорит об этом как о секрете, который останется только между вами – немедленно сообщи об этом родителям или старшим
2. Сделай снимок с экрана (screen-shot)
3. Никогда не соглашайся на личные встречи с незнакомцами. Твои собеседники могут оказаться совсем не теми, за кого себя выдают. Или приходи на встречу только со взрослым