

Памятка для учащихся и родителей

Общая безопасность в интернете.

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы — например, вирусное программное обеспечение (далее — вирусы), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы.

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Рекомендации:

Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.

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

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

Не подключать к своему компьютеру непроверенные съемные носители.

Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Мошеннические письма.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Рекомендации:

Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.

Игнорировать такие письма.

Памятка для учащихся и родителей

Получение доступа к аккаунтам в социальных сетях и других сервисах.

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи следующими способами:

Заставить ввести свои данные на поддельном сайте.

Подобрать пароль, если он не является сложным.

Восстановить пароль с использованием “секретного вопроса” или введенного ящика электронной почты.

Перехватить пароль при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. **Фишинг** (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации:

Использовать сложные пароли (сложные пароли 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 сообщать свой пароль.

Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.

Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).

Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

Памятка для учащихся и родителей

Безопасность в сети Интернет

Правило 1. Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2. Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Правило 3. Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Правило 4. Не позволяйте ребенку встречаться с онлайн-знакомыми без разрешения. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий 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 и договориться о встрече.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. Предупреждение кибербуллинга: Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Правило 5. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Правило 6. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Памятка для классных руководителей

Рекомендации по обеспечению безопасности учащихся в Интернете.

Поговорите с учащимся о безопасности в Интернете. Объясните основные правила, возможности различных технологий и последствия нарушений. Самое главное: убедите, что в любой непонятной или пугающей ситуации ему следует обращаться к педагогам, чтобы найти безопасное решение.

1. **Используйте компьютер и смартфон вместе с детьми.** Это хороший способ научить их правилам безопасности в Интернете. При этом дети поймут, что решать возможные проблемы лучше всего вместе.
2. **Расскажите детям больше о сайтах и сервисах в Интернете.** Поговорите о том, что их интересует в Интернете и какие страницы им можно посещать.
3. **Безопасные пароли.** Помогите своей семье приобрести правильные привычки в отношении паролей. Расскажите об их использовании. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.
4. **Используйте настройки конфиденциальности и управления доступом.** В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации. Поговорите с членами своей семьи и определите, о чем не следует рассказывать всем. Научите детей уважать конфиденциальность друзей и родных.
5. **Проверьте возрастные ограничения.** Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет. Прежде чем ваш ребенок регистрируется на том или ином сайте, самостоятельно проверяйте условия его использования и соответствие материалов правилам, принятым в вашей семье.
6. **Научите детей ответственному поведению в Интернете.** Помните золотое правило: то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.
7. **Посоветуйтесь с другими взрослыми.** Привлеките к обсуждению этой темы друзей, родственников и коллег. Другие родители и специалисты по работе с детьми могут оказать вам неоценимую помощь в том, как научить

детей и родственников правильному использованию самых разных информационных технологий.

8. **Защитите свой компьютер и личные данные.** Используйте антивирусное программное обеспечение и регулярно его обновляйте. Поговорите со своей семьей о типах личной информации – например, номер социального страхования, номер телефона или домашний адрес – эти данные не должны быть размещены в Интернете. Научите свою семью не принимать файлы или открывать вложения в электронной почте от неизвестных людей.
9. **Не останавливайтесь на достигнутом.** Безопасность в Интернете требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе. Пересматривайте правила пользования Интернетом в семье, следите за тем, как ваши близкие осваивают новые технологии, и время от времени давайте им советы.

Признаки компьютерной зависимости:

- когда родители просят отвлечься от игры на компьютере, ребенок демонстрирует острый эмоциональный протест;
- ребенок раздражается при вынужденном отвлечении;
- ребенок не может спланировать окончание игры на компьютере;
- ребенок постоянно просит деньги для обновления программного обеспечения компьютера и приобретения новых игр;
- ребенок забывает о домашних делах и приготовлении уроков;
- у ребенка сбивается режим дня, режим питания и сна, он перестает заботиться о собственном здоровье;
- чтобы постоянно поддерживать себя в бодрствующем состоянии, ребенок начинает злоупотреблять кофе и другими энергетическими напитками;
- прием пищи происходит без отрыва от игры на компьютере;
- ощущение эмоционального подъема во время игры на компьютере;
- ограничение общения постоянным обсуждением компьютерной тематики с окружающими;
- нетерпение, предвкушение и продумывание заранее своего возвращения к компьютеру.
- нередко развивается бессонница и нервное истощение.