ПРАВИЛА БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Рассмотрим распространенные опасности и правила борьбы с ними:

Преступники в интернете: что можно сделать для снижения опасности

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию.

КАК УЗНАТЬ, НЕ СТАЛ ЛИ РЕБЕНОК ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

- Ребенок проводит много времени в Интернете.
- В компьютере появились материалы откровенного содержания.
- Ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам незнакомы.
- Ребенок получает письма, подарки или посылки от неизвестного вам лица.
- Ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый.
- Ребенок использует чью-то чужую учетную запись для выхода в Интернет.

ЧТО ДЕЛАТЬ, ЕСЛИ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

- Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либо свидетельств об общении с сексуальной окраской – это настораживающие признаки.
- Контролируйте доступ ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.
- Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.
- Если ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

Вредоносные и нежелательные программы в интернете

ЧТО ТАКОЕ ВИРУС?

Вирус – это программа, которая может проникнуть в компьютер различными путями (через электронную почту, Интернет, различные виды дисков и т.д.) и вызвать эффекты, начиная от просто раздражающих до очень разрушительных, способны размножаться, заражая другие файлы и программы.

ЧТО ТАКОЕ НЕЖЕЛАТЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ?

Под выражением «нежелательное программное обеспечение» понимаются программы, которые выполняют на компьютере некие задачи без вашего согласия. Они могут показывать рекламные сообщения, объявления или собирать личные данные о вас и вашей семье.

ВРЕДОНОСНЫЕ ПРОГРАММЫ МОГУТ ВЫПОЛНЯТЬ СЛЕДУЮЩИЕ ДЕЙСТВИЯ:

- устанавливать соединение с вашего компьютера наружу;
- разрешать управление вашим компьютером извне;
- собирать вашу конфиденциальную информацию (шпионские программы);
- отображать нежелательную и рекламную информацию (рекламные программы);
- отслеживать нажатие клавиш (кейлоггеры);
- гарантировать повторное заражение даже после очищения (руткит).

КАК СНИЗИТЬ РИСК ЗАРАЖЕНИЯ?

Необходимо постоянно улучшать защиту компьютера. Есть три основных шага, которые необходимо сделать, чтобы обеспечить защиту своего компьютера:

- применяйте межсетевой экран;
- выполняйте обновления;
- применяйте новейшие антивирусные программы.

Материалы нежелательного содержания: как избежать?

ЧТО ЗНАЧИТ НЕЖЕЛАТЕЛЬНОЕ СОДЕРЖАНИЕ.

Материалы порнографического, ненавистнического содержания, материалами суицидальной направленности, сектантские материалы, ненормативной лексики.

КАК ПОМОЧЬ ДЕТЯМ ИЗБЕЖАТЬ НЕНАВИСТНИЧЕСКИХ МАТЕРИАЛОВ?

- Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®).
- Контролируйте использование Интернета и наблюдайте за детьми.
- Научите детей критически относиться к содержанию онлайновых материалов и не доверять им.

Интернет-мошенничество и хищения данных кредитной карты

«Интернет-мошенники» – хакеры применяют технику «phishing», состоящую в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

СНИЖЕНИЕ РИСКА ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ.

- Самостоятельно набирайте в обозревателе адрес веб-сайта или пользуйтесь ссылкой из «Избранного» (Favorites);
- Никогда не щелкайте на ссылку, содержащуюся в подозрительном электронном письме.
- Как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации
- Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.

ЧТО ДЕЛАТЬ В СЛУЧАЯХ ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ?

- Измените пароли.
- Поставьте в известность отдел обслуживания клиентов соответствующих организаций.
- Поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета.
- Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.
- Записывайте и сохраняйте абсолютно все.
- После выполнения всех действий всегда делайте копии документов.

Памятка для детей по безопасному поведению в интернете

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, предпринимайте следующие меры предосторожности при работе в Интернете:

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

2. Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

3. Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.

4. Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

5. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

6. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям!

7. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.