**БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ**

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Интернет — это не только кладезь возможностей, но и источник угроз.

Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них — дети, которые могут не знать об опасностях мировой паутины. Очень большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности. Сегодня мы попробуем ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и «Как их избежать?».

Интернет прочно вошел в жизнь практически каждого человека. Очень многие уже не представляют свою жизнь без этого достижения техники. Однако это достижение рождает множество проблем, которые требуют незамедлительного решения.

Интернет – это глобальная вычислительная сеть, объединяющая множество региональных, ведомственных, частных и других сетей каналами связи и едиными для всех ее участников правилами пользования. По Интернету происходит поиск информации, рассылаются пресс-релизы, устраиваются конференции, выставки, интервью и т.д. Обычный, «домашний» пользователь имеет все шансы заказать по Интернету любой товар с доставкой на дом, узнать погоду, познакомиться, пообщаться.

***Угрозы Интернета:***

·угроза заражения вредоносным программным обеспечением;

·доступ к нежелательному содержимому;

·неконтролируемые покупки;

· контакты с незнакомыми людьми с помощью чатов или электронной почты.

Интернет — это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что, как и наш реальный мир, всемирная паутина может быть и весьма опасна.

***Контентные риски.***

Это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

***Коммуникационные риски***

Связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

***Интернет зависимость***

«Интернет зависимость» – это широкий термин, обозначающий большое количество проблем поведения и контроля над влечениями.
Некоторые признаки виртуальной зависимости:

· Пристрастие к виртуальным знакомствам – избыточность знакомых и друзей в сети Интернет.

· Навязчивая потребность в сети – игра в онлайновые азартные игры.

· Информационная перегрузка (навязчивый web-серфинг) – бесконечные путешествия по сети, поиск информации по базам данных и поисковым сайтам.

***Электронные риски.***

Это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

**ТРИ правила, которые помогут избежать опасностей.**

***Пароли***

Используйте всегда индивидуальные и сложные пароли, состоящие из букв, цифр и специальных символов. Исключите использование паролей по умолчанию, не сохраняйте пароли в ваших гаджетах и браузерах. Почему мы говорим об этом в первую очередь? Статистика говорит о том, что люди мало уделяют внимания парольной политике.

Третий год подряд самым популярным паролем в мире является «123456». Подобрать такой пароль к вашим порталам и персональным данным злоумышленнику не доставит труда.
Регулярно осуществляйте смену паролей, обеспечивая каждый раз их конфиденциальность. Это ваш самый большой секрет, как ключ от замка входной двери в ваш дом.
Правило первое: «Ключ от дома должен быть секретным, надежным, и только вашим, личным».

***Вирусы и антивирусы***

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть средства со счета. Программы «Черви», «Трояны», «Шпионы» — их множество разновидностей и красивых названий, а суть одна – все это вредные вирусы!
Для защиты компьютера на нем устанавливаются специальные защитные программы и фильтры. Использовать можно только лицензионное программное обеспечение с актуальными обновлениями.
Устанавливать надо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия вашего антивируса.
Не качайте программные продукты из сомнительных источников (файлообменных сетей и торрентов). Не открывайте и не сохраняйте подозрительные файлы – сразу удаляйте. Не отвечайте на непонятные вам рассылки.

И главное — не посещайте ресурсы с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения любого толка. Сомневаетесь – не нажимайте «да» или «ENTER».
Здесь можно провести простую параллель – держимся подальше от вирусов, моем руки регулярно, хорошим и качественным мылом. При любой сомнительной ситуации: «Моем руки с мылом, к вирусам не прикасаемся».

***Персонализация***

Никому не передавайте свои конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы», если их создать, могут тянуться за вами всю жизнь. Могут навредить вам на пути к достижению поставленной цели. Игнорируйте в сети Интернет подобные запросы.
Получается странно – дома и на работе мы храним свои документы в сейфе, закрываем на ключ. Мы понимаем их важность. А потом по непроверенному запросу открываем сейф, достаем документы, фотографируем и посылаем посредством ресурсов в сети Интернет. Количество лиц, которые могут получить доступ к таким посланиям, даже трудно прогнозировать.
Давайте запомним третье правило: «Наши документы всегда в сейфе».

Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет общение будет приносить пользу. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Даже когда мы испытываем жажду, мы не будем пить из грязной лужи. Также и в среде Интернет, случайно оказавшись в месте, которое производит отталкивающее впечатление агрессивного и замусоренного, лучше покинуть его, переборов чувство любопытства. Это защитит вас от негативных эмоций, а ваш компьютер – от вредоносного программного обеспечения.

У интернет-мошенников ничего не получится, если только мы сами не откроем им дверь – не сообщим им наши пароли, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям.

|  |
| --- |
| **Памятка****по безопасному****поведению в Интернете**Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, вы должны предпринимать следующие меры предосторожности при работе в Интернете:* Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
* 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.
* Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
* Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
* Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
* Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
* 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.
 |