+16

Муниципальное бюджетное учреждение культуры
«Лысьвенская библиотечная система»
Центральная библиотека
Центр социально-правовой информации

# БЕЗОПАСНЫЙ ИНТЕРНЕТ


Информационная памятка

Лысьва
2018

32.973
Б 40
Безопасный Интернет: информ. памятка / МБУК «Лысьвенская БС». – Лысьва: [б.и.], 2018 . – 12 с.

Безопасность в интернете – очень важная проблема нынешнего времени. И касается она всех, от детей до пенсионеров. Она становится все актуальнее в связи с массовым приходом в интернет пользователей, не подготовленных к угрозам, поджидающим их. Поэтому данная памятка и будет посвящена такому вопросу, как безопасность в сети интернет. Ведь страдает не один пользователь, а и многие другие, объединенные в одну глобальную структуру.

Памятка рекомендована для большого круга читателей.

### *Опасности, подстерегающие нас в сети*

Если сказать кратко, то существуют две основные возможности того, как может ваш компьютер стать жертвой.

Первое – вы сами, странствуя по различным сайтам или устанавливая программное обеспечение с непроверенных источников, а иногда и с проверенных, заражаете свой компьютер.

Второе – возможна также ситуация, когда злоумышленники преднамеренно, с помощью, например, троянских программ или вирусов, делают ваше устройство источником опасности. В результате всего этого компьютер, иногда даже тайно от своего владельца, начинает выполнять рассылку спама, участвует в DDoS-атаках на различные сайты, крадет пароли. Бывает и так, что провайдер вынужден принудительно отключить такое устройство от глобальной сети.

Получается, что если пользователь не осведомлен о том, что представляют собой основы безопасности в сети интернет, придется ему тяжело.

### *Зачем нужен злоумышленникам доступ к компьютеру пользователя?*

Зря обычный пользователь думает, что его компьютер никому не нужен. Это раньше хакеры часто писали вирусы просто ради интереса, сейчас же это делается почти всегда с коммерческой выгодой. Лет 20 тому назад злоумышленник получал удовольствие от того, что мог просто отформатировать жесткий диск. Или сделать так, что при включении компьютера вместо стандартного рабочего стола появятся какие-либо прикольные картинки. Сейчас же они делают все возможное, чтобы владелец ПК как можно дольше не знал о том, что его устройство заражено и втайне от него выполняет дополнительные функции. Для чего все это делается? Кроме того, о чем было сказано выше, хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в социальных сетях, форумах. Случается так, например, что вы ложитесь спать с 20 000 рублей на электронном кошельке, а утром получаете СМС-сообщение о том, что денег на нем уже нет. А с почты все ваши контакты, да и не только,

получают спам-письма, а то еще и трояны. Хакеры могут объединить множество зараженных компьютеров в единую мощную сеть, провести DDoS-атаку даже на мощные государственные серверы.

Из самого простого, но также приносящего деньги: заблокируют работу операционной системы и потребуют деньги за устранение проблемы. И, кстати, деньги возьмут, но компьютер оставят заблокированным. Так что безопасность в сети интернет должна стать основой вашей работы в ней.

### *Как злоумышленники проникают в компьютер?*

Для того чтобы взломать защиту ПК, даже если она есть, хакеры применяют целый ряд способов, и пользователи зря думают, что, просто установив антивирус, они избавились от опасности, например, подцепить вредоносную программу. Поэтому, прежде чем искать информацию о том, как правильно соблюдать безопасность в сети интернет, нужно понять, а откуда берутся вирусы и трояны.

Несколько основных путей их проникновения и методы воровства различной информации:

Первый метод называется социальной инженерией. Благодаря различным психологическим приемам, уловкам и доверчивости пользователей хакеры присылают вам вполне безобидный файл или письмо, а вы сами и запускаете троянчик в нем. Или же по просьбе якобы администрации сервиса выдаете все свои пароли и явки.

Второй метод – предлагается разное бесплатное программное обеспечение, пиратские диски, где спрятано множество вирусов, троянов и тому подобной гадости. В ПО, в том числе и из самых надежных проверенных источников, постоянно появляются дыры в безопасности. Это относится и к операционным системам. Вот злоумышленники внимательно и следят за такими моментами, стараются их не упустить, а использовать в собственных целях. Зайдете на какую-нибудь страничку сто раз проверенного сайта и раз - ваше устройство заражено.

Третий метод получил особое распространение в последнее время. Это фишинг, когда создаются поддельные сайты. И вы вместо странички своего банка оказываетесь на его поддельной копии. О том, что может быть дальше, говорить не будем, сами догадаетесь.

### *Начальная защита компьютера пользователя*

В идеале, купив ПК, пользователь должен выполнить целый ряд операций, прежде чем броситься бороздить бесконечные просторы сети. Некоторые советы безопасности в интернете: несмотря на то что Windows имеет встроенный файрволл, рекомендуется установить более надежный, так как имеющийся - далеко не самый лучший. Выбирайте платный или бесплатный, исходя из их рейтингов. Следующий шаг – установка антишпионского и антивирусного ПО. Нужно сразу же его обновить и настроить на автоматическое обновление. Также оно должно запускаться автоматически, вместе с ОС. И постоянно, в фоновом режиме, работать. И обязательно проверяйте любую

устанавливаемую программу. Как только появляются обновления для Internet Explorer и других используемых вами браузеров, тут же скачивайте их и устанавливаете. Отключайте все неиспользуемые службы на своем устройстве, это уменьшит шансы для хакеров получить к нему доступ.

Теперь немного информации о том, как обеспечить безопасность работы в сети интернет. Удаляйте сразу же все письма подозрительного содержания, не вздумайте открывать файлы из неизвестных источников. Игнорируйте все предложения легкого заработка, никому не высылайте свои пароли, не переходите по подозрительным ссылкам. Используйте только сложные пароли, состоящие из сложного набора цифр, букв и символов. Для каждого случая назначайте свой, оригинальный. Выходя в сеть из мест общего пользования, будьте аккуратны и осторожны. Это же касается и использования прокси-серверов. Желательно не проводить никаких банковских и других подобных операций из таких мест. Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее. Нежелательно посещать сайты для взрослых или подобные им ресурсы. Велика вероятность подхватить троян. Следите за интернет-траффиком, даже если он безлимитный. Если он без особой причины значительно увеличился, это может быть признаком активности вируса. Если будете соблюдать эти минимальные правила безопасности в сети интернет, то избежите многих проблем. Это, конечно, далеко не все. Опасностей столько, что нельзя о них забывать ни на минуту.

**Кратко о некоторых мерах предосторожности:** если с вашего банка пришло письмо с проверкой пароля, не вздумайте им его отправлять. Банки никогда таких запросов не делают. Все почтовые программы имеют фильтр от спама. Доверяйте ему. Получив письмо о выигрыше в миллион рублей или наследстве в пять миллионов долларов, удаляйте их сразу же. Рекомендуется устанавливать комплексную защиту. Она надежнее, чем антивирус – от одного производителя, файрволл – от другого, а антишпионская программа – от третьего. Отдавайте предпочтение платным версиям. Так как Opera и Internet Explorer – самые распространенные браузеры, для них и вирусов существует более всего. Используйте альтернативные варианты: Apple Safari, Google Chrome и Mozilla Firefox. Не пользуйтесь нелицензионным программным обеспечением, так как в нем изначально может быть установлено шпионское ПО. Если делайте покупки в онлайн-магазинах, то пользуйтесь только проверенными вариантами. Это же относится и к любому иному онлайн-сервису. Выполняйте все эти требования, и тогда безопасность в сети интернет будет более-менее гарантирована.

### *Дети и интернет*

В связи с развитием современных технологий все большее количество детей получает возможность выхода в интернет. И если раньше они в основном играли в игры, даже не выходя в сеть, то теперь все совсем по-другому.

Поэтому появилась новая задача – обеспечить безопасность детей в сети интернет. Это достаточно сложно, так как Всемирная паутина изначально развивается полностью

бесконтрольно. В ней есть очень много информации, доступа к которой у детей быть не должно. Ко всему прочему, их нужно научить, как не "наловить" вирусов и троянов. Кто же им поможет с этим, как не взрослые. К тому же очень важна и информационная безопасность в сети интернет, так как дети – совсем неискушенные пользователи. Они легко могут попасться на удочку опытного мошенника или злоумышленника.

### *Как научить детей правильно пользоваться интернетом*

Самый первый совет заключается в том, что первые сеансы в сети ребенок должен проводить с кем-нибудь из взрослых. Желательно пользоваться такими программами, как "Родительский контроль", чтобы контролировать все действия детей в интернете. Нужно ограничивать самостоятельное использование почты и чатов, ведь это может быть даже опасно. Так как там, например, педофилы могут искать себе жертв.

Несколько рекомендаций относительно того, как можно постараться обеспечить максимально безопасность детей в сети интернет.

Сделайте так, чтобы дети делились с вами всеми своими неудачами и успехами при освоении интернета. Научите ребенка рассказывать обо всем, что вызывает у него беспокойство. Расскажите, как соблюдать конфиденциальность, помогите выбрать регистрационные данные, не разглашающие реальных, ведь информационная безопасность в сети интернет – залог того, что удастся избежать многих неприятностей. Объясните, что в виртуальном пространстве не нужно никому называть свою фамилию, домашний адрес, номер школы и т. п. Научите, что нет разницы между поступками в реальной жизни и в интернете. Посоветуйте не встречаться с друзьями из сети, так как ожидания могут быть обмануты, не верить всему тому, что им говорят/пишут. Обязательно установите специальное ПО и контролируйте своих детей.

Когда вашему ребенку 14-16 лет, маловероятно, что вы сможете больше его разбираться в компьютерах, интернете и всех подобных вещах. Хотя, конечно, о контроле и влиянии на него забывать нельзя. Тем более надо помнить о такой проблеме, как обеспечение безопасности в сети интернет. Ведь, если компьютер общий, или все устройства подключены к единой домашней сети, то и угрозы будут общими. К тому же просматривать отчеты о деятельности ребенка вы всегда сможете. Рекомендуется не конфликтовать с ребенком по этому поводу, а пробовать общаться и находить общий язык. Несмотря на возражения, постарайтесь заставить принять правила пользования интернетом, скажите, какие сайты нельзя посещать. ПК, имеющий выход в сеть, должен быть установлен в общей комнате. Это будет немного сдерживать вашего ребенка. Установите ПО, блокирующее нежелательные сайты, не разрешайте без согласования с вами устанавливать любые программы. И не забывайте следить за тем, чтобы дети не стали зависимыми от интернета. Надеемся, что наши советы помогут защитить ваши компьютеры от угроз.

*Материалы с сайта http://fb.ru/article/159338/bezopasnost-v-seti-internet-informatsionnaya-bezopasnost-v-internete*

## Правила работы в сети Интернет

1. Не входите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.

3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.

4. Никогда не посылайте никому свой пароль.

5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник).

7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.

9. Не всей информации, которая размещена в Интернете, можно верить.

10. Не оставляйте без присмотра компьютер с важными сведениям на экране.

11. Не сохраняйте важные сведения на общедоступном компьютере.

## Памятка для родителей по теме «Безопасный Интернет»

1. Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Выберите время для неконфликтного совместного просмотра интернет-страниц.

2. Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.

3. Если ваши дети регистрируются на форумах, в чатах или сетевых играх, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.

4. Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.

5. Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы.

6. Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения нисколько не изменяются.

7. Добейтесь от детей уважения к собственности других пользователей Интернета.

8. Убедите детей в том, что они не должны встречаться с интернет-друзьями лично. Скажите, что интернет-друзья могут на самом деле быть не теми, за кого они себя выдают.

9. Объясните детям, что верить всему, что они видят или читают в интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации, им следует обратиться за советом к вам.

10. Продолжайте контролировать действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб-узлы посещают ваши дети, и узнавать, что они там делают.

11. Если ваши дети пользуются чатами, вам следует знать, какими именно, и с кем они там беседуют. Лично посетите чат, чтобы проверить, на какие темы ведутся дискуссии.

13. Компьютер, подключенный к Интернету, должен находиться в общей комнате; по возможности не устанавливайте его в спальне ребенка.

14. Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если дети пользуются компьютерами в местах, находящихся вне вашего контроля, – общественной библиотеке, школе или дома у друзей – выясните, какие защитные средства там используются.

## Уважаемые пользователи!

***Центр социально-правовой информации***
*Центральной*
*библиотеки предоставляет*
**доступ в Интернет**

У нас вы можете воспользоваться:
**- ресурсами СПС Консультант Плюс**
**- документами органов местного самоуправления**

**Адрес: Пермский край, г. Лысьва, ул. Коммунаров,20**

**Режим работы: с 10 час. до 18 час.**
**Выходные дни: суббота**
**июнь-август: суббота, воскресенье**
**Телефоны: (34249)2-66-96**
sspi_lysva@mail.ru

Сост. О. Н. Десяткова Тираж 20 экз.
**E-mail:** mpb_lysva@mail.ru ;
**http:// lysva-library.**