**Ребенок и виртуальная реальность**

Взаимодействие ребенка с виртуальной реальностью беспокоит и родителей и педагогов. Иногда вопрос встает радикально: стоит ли вообще знакомить ребенка с прелестями компьютерной жизни? Ведь  нередки случаи, когда игры засасывают пользователя настолько, что он не может представить себе другой жизни. Он ест, не отходя от клавиатуры, мало спит, его глаза покраснели от ежедневной нагрузки, а пальцы вечно ищут компьютерную мышку. Реальность за пределами компьютерного пространства для него скучна и бессмысленна, социальные игры не интересны, так же как и радости отдыха на природе и шумные вечеринки друзей. Он заключенный пикселей на жидкокристаллическом мониторе. Картина более чем печальная, особенно если зависим от компьютера ребенок. Многие родители боятся, что подобное случится с их ребенком. Действительно, их опасения обоснованны, виртуальность даже излишне привлекательна для детей, психика которых очень быстро приспосабливается к окружающей среде, за счет чего возникает скорое привыкание и зависимость. Но жесткий запрет не спасет от опасности компьютерной зависимости, скорее наоборот, когда, наконец, произойдет встреча ребенка с персональным компьютером, он будет к ней совершенно не подготовлен. Много лучше будет, если это знакомство произойдет под чутким контролем родителей. Для ребенка часы, проведенные за компьютером одни из самых счастливых. С чудесными возможностями компьютера не сравнятся ни телевизор, ни новые ролики. Когда находишься в виртуальном мире, время течет в десятки раз быстрее, неважно смотришь ли ты смешные мультфильмы или проходишь очередной уровень любимой игры. Ребенок не замечает, сколько часов он уже провел за компьютером, поэтому дозировать время работы за компьютером следует родителям. Если у вас нет возможности постоянно отслеживать минуты, проведенные в виртуальности, то вам поможет специальное программное обеспечение, созданное специально, чтобы дети занятых  бытовыми хлопотами родителей, при использовании компьютера не оставались предоставленными самим себе. Программы подобного рода,  создают двойную пользовательскую систему, для взрослого и ребенка. Работа в детском режиме ограничена, вы сами ставите контрольные точки: сколько времени в день ребенок может пользоваться компьютером, когда он должен сделать перерыв, длительность которого так же выбирается вами. По истечении выделенного срока, детский пользователь выключается, а чтобы войти в родительский требуется ввести пароль. Выключить программу может только родитель, находясь  в своем режиме, ребенок не сможет продлить уже вредное удовольствие. Использование подобных программ дарит множество преимуществ, но полностью полагаться на него неблагоразумно, ведь ваша цель в первую очередь научить ребенка правильно пользоваться компьютером, чтобы в дальнейшем он мог самостоятельно заботиться о своей безопасности. Юный пользователь должен понимать, почему его «компьютерное» время ограничивают, объяснив причины установки программы, вы не только оградите себя от лишних разногласий со своим чадом, но и дополнительно его защитите.

**Классификация киберугроз**

**Рассмотрим наиболее распространенные типы угроз в интернете:**

**Контентные риски.** Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

**Неподобающий контент**. В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анарексии и булимии, суицида, азартных игр и наркотических веществ.

**Незаконный контент**. В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

**Электронная безопасность.** Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера  с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

**Вредоносные программы**. Вредоносные программы — это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов:

**Спам.** Спам — это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

**Кибермошенничество.** Кибермошенничество — это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма,[**фишинг**](http://content-filtering.ru/Eduandinet/risks/fishing/), вишинг и фарминг.

**Коммуникационные риски**. Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

**Незаконный контакт**. Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

**Киберпреследования**. Киберпреследование — это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также,  киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

**Классификация интернет угроз**

**Комплексное решение в области использования сети Интернет**

Опираясь на мировой опыт и анализируя ситуацию в России можно сказать, что решение вопроса по обеспечению безопасного использования Интернет представляет комплексное решение.

Оно включает в себя:

* Административные (нормативно-правовые) меры, которые обеспечивает государство посредством создания/изменения законопроектов.
* Воспитание и обучение пользователей эффективной работе с информацией, которым занимаются специальные ресурсы (в том числе наш). Обучением работе в Интернете детей должны так же заниматься родители и педагоги.

Всем известно, что Интернет бесценный источник информации, это уникальное средство общения, которая предлагает всем пользователям широкий спектр занятий и возможностей. Но проблема в том, что не все пользователи осознают опасность, что в любой момент могут стать жертвами вредоносной программы, шпионской ПО, фишингу и других Интернет-угроз.

Конечно, существуют очень много опасных угроз информационной безопасности, однако обеспечить онлайновую безопасность и уменьшить риск возникновения проблем к минимуму очень легко – просто нужно знать, чего нельзя делать в Интернете и как вести себя в определенных ситуациях. На этом занятии вы найдёте список наиболее частых ошибок пользователей при работе с компьютером и их решения — полезные рекомендации, соблюдая которых, можете сделать свой веб-серфинг максимально безопасным и более приятным.

**Не игнорируйте антивирусные программы и брандмауэры**.

***Ошибка***: многие пользователи не устанавливают антивирусные программы и/или фаерволы думая, что это бесполезно, неудобно или просто им лень.

***Решение:***чтобы быть в безопасности, Вы должны установить и антивирус, и брандмауэр, так как только вместе эти программы обеспечивают наилучшую защиту. Если Вы решили купить антивирус/фаервол, рекомендую, во-первых, скачать демо-версии, таким образом, Вы сможете сами посмотреть и анализировать, устраивает ли Вас выбранная программа.

**Не используйте записи с правами Администратора.**

***Ошибка***: войти в систему и/или запускать стандартные приложения под учетной записью с правами администратора.

***Решение***: в таких случаев, вероятность заражения и взлома ПК очень высока, вот почему нужно создать как минимум две записи: одну с административными правами для выполнения административных задач, а остальные с правами обычного пользователя.

1. **Не забудьте устанавливать обновлении программного обеспечения.**

***Ошибка:*** пользователи забывают установить обновления программного обеспечения или хуже, не хотят этого сделать.

***Решение:*** необходимо установить автоматическую загрузку обновлений и не забывать, что апдейты являются обязательными, конечно, если для Вас безопасность и стабильность играет важную роль.

1. **Не открывать вложения в электронных письмах от незнакомых людей**.

***Ошибка:*** открывать вложенные в электронные письма файлы, особенно если они получены от неизвестных отправителей.

***Решение:*** не зная, кто отправитель и что именно находится во вложенных файлах, не следует открывать такие письма, так как во многих таких случаев к сообщению прикреплены вредоносные файлы.

1. **Не указывать личную и финансовую информацию на общедоступном компьютере**.

***Ошибка***: вводить свои пароли на общедоступном компьютере (Интернет-клуб), ведь там гораздо выше вероятность, что информация попадет в руки злоумышленников — например, пользователь забудет выйти из учетной записи или не удалит информацию в истории/куки браузера. Не следует также забывать о том, что на общедоступном компьютере может быть установлено шпионское ПО, а посторонние люди всегда могут заглядывать через плечо, наблюдая за вашими действиями.

***Решение***: не вводить финансовую информацию, пароли и другие личные данные на общедоступном компьютере, однако в случае необходимости, используйте виртуальную клавиатуру. Также не забывать удалять кеш, история и куки своего веб-серфинга, после завершения работы на компьютере.

**Не загружать бесплатное программное обеспечение (freeware) с неизвестного сайта.**

***Ошибка***: увидев упоминание новой программы, часто пользователи начинают ее загружать и устанавливать на своём компьютере, рискуя тем самым заполучить вредоносное ПО.

***Решение:***перед загрузкой программы стоит удостовериться, что она упоминается на серьезных сайтах — таких как Cnet.com или Download.com.

1. **Не открывайте подозрительные файлы.**

***Ошибка:*** скачивая многообещающий файл, многие пользователи забывают о безопасности своего персонального компьютера.

***Решение***: прежде чем запускать подозрительный файл, нужно сканировать его на наличие вредоносных программ, используя разные антивирусные программы. Для этого рекомендую использовать[**бесплатные онлайн-антивирусы**](http://www.securrity.ru/online_antiviruses.html) и убедится что файл чист.

1. **Не использовать одинаковый пароль для нескольких сайтов или учетных записей.**

***Ошибка***: использовать легкий праоль и/или один и тот же пароль для всех своих учетных записей в онлайне.

***Решение:*** не следует использовать легко запоминающиеся пароли, вместо этого, используете **[онлайн генератор паролей](http://www.securrity.ru/genpwdz.html)** чтобы сгенерировать безопасный, надёжный и уникальный набор символов — для одной учётной записи.

**Не опубликовать личную информацию в публичных местах.**

***Ошибка:*** публикация личных данных в социальных сетях.

***Решение:*** просто не делать этого, так как раскрытие личной информации может повредить и в карьере, и в личной жизни, а злоумышленникам будьте облегчить деятельность

**Не передавать личные данные через открытые Wi-Fi хот-споты.**

***Ошибка***: передавать важные данные через открытые точки доступа Wi-Fi.

***Решение:*** если необходимо пользоваться открытым Wi-Fi-хотспотом, стоит, как минимум, установить брандмауэр и задать в нем наивысший уровень защиты. Кроме того, в этом случае не стоит передавать финансовую информацию, так как перехватить её — для хакеров не составляет труда

**Не доверять людям, с которыми никогда не встречались лично.**

***Ошибка***: доверяться виртуальным знакомым до личной встречи

***Решение:*** интернет-мошенники часто охотятся за своими жертвами в социальных сетях, притворяясь очень хорошими людьми, которые готовы в любое время помочь Вам. Также, покупая что-то с помощью Интернета у конкретного человека (например, через объявление), лучше заплатить наличными, а на онлайновом аукционе — тщательнее проверять репутацию продавца

1. **Не нажимать на всплывающие окна.**

***Ошибка:*** нажимать на всплывающие окна, чтобы отказаться от чего-то.

***Решение:*** запретить браузерам отображать всплывающие окна или отключить javascript.

**Не стоит доверять всей полученной информации.**

***Ошибка:*** получив электронное письмо, в котором сказано, например, о выигрыше, смерти Бритни Спирс, ядерной войне или других маловероятных вещах, — открывать его и/или рассказывать об этом знакомым, отправляя копию этого сообщения

***Решение***: просто удалите их (лучше нажимая на кнопку «Сообщить о спаме»), так как такие письма следует воспринимать со здоровой долей скептицизма, чаще всего это обычный спам, в худшем случае еще и разносящий вирусы.

1. **Не покупать ничего на незнакомых сайтах.**

***Ошибка***: купить что-то на веб-сайте, о котором Вы никогда раньше не слышали.

***Решение***: предоставляя личную и финансовую информацию, необходимую для заключения сделки, нужно, по крайней мере, убедиться, что она отправляется через безопасное соединение. В идеале следует иметь отдельную кредитную карту только для покупок в Сети.

**Не вводить конфиденциальную информацию при использованию прокси серверов.**

***Ошибка:*** вводить свои пароли на каком-либо сайте используя анонимные прокси сервера.

***Решение***: лучше никогда де использовать недоверчивые анонимные прокси сервера.

1. **Не установить дополнительные плагины для просмотра контента.**

***Ошибка:*** иногда, для того чтобы посмотреть «эксклюзивные» материалы, пользователям предлагается установить дополнительные плагины. Однако, вместо плагинов пользователь получает комплект вредоносных компонентов.

***Решение:***не установить плагины о которым раньше никогда не слышали, тем более если нужно установить это ПО для просмотра шокирующих видеоматериалов или тому подобных. В принципе для нормальной работы интернет-браузера нужно установить следующие плагины:

* *Adobe Reader*
* *Adobe Flash Player*
* *Shockwave*
* *Java*
* *QuickTime*
* *RealPlayer*
* *Windows* *Media* *Player*

**Не скачивать антивирусы, которые оповещают что Ваш компьютер инфицирован**.

***Ошибка:*** загружать/установить антивирусные программы, которые, при простым открытием веб-страницы оповещают, что компьютер заражён.

***Решение***: включить блокирование всплывающих окон или лучше, отключить яваскрипт (javascript). И все же, если получили такое уведомление, просто игнорируйте её, а для безопасности — сканируйте компьютер на наличие.

1. **Не сообщать никому свои пароли или конфиденциальные данные.**

***Ошибка***: отправить пароли или сообщить Ваши данные Администрации сайта/банки/провайдера, которая заявляет, что будет заблокировать Ваш счет в случае невыполнения требований

***Решение***: нужно игнорировать подобные письма, в которых сообщается что, если не сообщите Ваши данные в течение недели, Ваш счет будет заблокирован. Если Вы решили открыть URL-адреса из таких сообщений, во-первых, проверяйте, если действительно ссылки, открывают упомянутый сайт, а не какой-нибудь IP-адрес или ссылка похожая на URL оригинального сайта.

**Рекомендации по защите от интернет мошеничества**

1. Никогда не отвечайте на сообщения электронной почты, запрашивающие личные сведения. Следует особо подозрительно относиться к сообщениям электронной почты от предприятий или частных лиц, запрашивающим личные сведения, а также сообщениям, содержащим ваши личные сведения с просьбой обновить или подтвердить их. Лучше воспользоваться телефонным номером, указанным в выписке, для звонка в соответствующую организацию; не следует звонить по номеру, указанному в сообщении электронной почты. Аналогичным образом, никогда не сообщайте свои личные сведения по телефону при несанкционированных звонках.
2. Не щелкайте ссылки в подозрительных письмах. Не щелкайте ссылки в сообщениях электронной почты, вызывающих подозрение. Такие ссылки могут быть опасны. Лучше посетить соответствующий веб-узел, введя URL-адрес в обозревателе или использовав ссылку в папке «Избранное». Не копируйте и не вставляйте ссылки из сообщений в обозреватель.
3. Используйте надежные пароли и часто меняйте их. Надежные пароли должны сочетать буквы в нижнем и верхнем регистре, цифры и символы (если учетная запись допускает их использование). Это делает их более защищенными. Не используйте слова из словаря. Используйте разные пароли для каждой учетной записи и часто меняйте их. Запомнить все пароли сложно.
4. Не отправляйте свои личные сведения в обычных сообщениях электронной почты. Обычные сообщения электронной почты не зашифрованы. Их отправку можно сравнить с отправкой почтовой открытки. Сотрудничайте только с теми компаниями, которым вы доверяете. Пользуйтесь услугами известных, признанных компаний, имеющих хорошую репутацию. На веб-узле компании должно быть опубликовано заявление о конфиденциальности, в котором явным образом оговаривается, что компания не будет передавать ваше имя или личные сведения другим людям.Убедитесь, что на веб-узле используется шифрование. Веб-адрес, указанный в адресной строке обозревателя, должен иметь префикс https:// вместо обычного http://.
5. Защитите свой компьютер. Важно использовать брандмауэр, регулярно обновлять программное обеспечение и пользоваться антивирусными программами, особенно при подключению к Интернету с помощью кабельного или DSL-модема.
6. Контролируйте финансовые операции. Проверяйте подтверждения заказов, а также выписки по кредитным картам и банковским счетам немедленно по получении, чтобы убедиться, что с вас взимаются средства только за проведенные операции. Немедленно сообщайте о любых нарушениях, связанных со счетами, по номеру телефона, указанному на банковской выписке. Использование только одной кредитной карты для покупок через Интернет упрощает отслеживание финансовых операций.
7. Используйте кредитные карты для финансовых операций через Интернет. В большинстве регионов личная ответственность пользователя при взломе кредитной карты существенно ограничена. При использовании прямого дебета с банковского счета или дебетовой карты, напротив, личная ответственность пользователя может равняться полному балансу банковского счета. Кроме того, для покупок в Интернете лучше использовать кредитную карту с небольшим кредитным лимитом, поскольку это позволяет ограничить сумму, которая может быть похищена в случае взлома кредитной карты. Также несколько крупных эмитентов кредитных карт теперь предлагают своим клиентам возможность использования номеров виртуальных одноразовых кредитных карт для покупок в Интернете, действующих в течение одного-двух месяцев.

**Ловушки интернета. Примеры и методы защиты от них.**

1. ***Классические почтовые угрозы***

Допустим, Вы новичок в интернете. Общение с ним Вы, скорее всего, начнете с того, что заведете себе учетную запись в системе электронной почты. Действующий адрес электронной почты необходим не только для переписки с друзьями и близкими, он также потребуется Вам для того, чтобы совершать покупки через интернет или регистрироваться на форумах или в социальных сетях. К сожалению, точно так же, как Ваш почтовый ящик может быть забит ненужными рекламными листовками, ящик электронной почты может оказаться заполненным нежелательными сообщениями. Спам составляет до 89% всех электронных сообщений. Это сообщения, которые вас совершенно не интересуют: Вам предлагают кредиты под низкие проценты, море продуктов и услуг. Такого рода предложения ни в коей мере не легитимны, и сообщения нередко содержат ссылки на сайты, зараженные вирусами, троянскими или другими опасными программами. Такие сообщения необходимо удалять, не открывая, — в этом случае они не смогут нанести вред вашему компьютеру — Вам лишь придется потратить время на их удаление. Легко сказать, что эти письма нужно просто удалять, — иногда искушение их открыть так велико. Киберпреступники умны: они проявляют особую активность накануне таких больших праздников, как Рождество, Пасха и, конечно же, День святого Валентина. Этот праздник — особенно хорошая возможность для мошенников, ведь именно в день Святого Валентина можно, не стыдясь, сказать о своих чувствах, даже если Вы едва знакомы. Если бы Вы получили сообщение в День святого Валентина с темой «Я тебя люблю», Вы ведь открыли бы его? Киберпреступники используют для своих целей не только праздники и «горячие» темы. Интернет часто называют вершиной развлекательных технологий — он изобилует сайтами, на которых размещены исключительно забавные статьи, картинки и видеоролики. Нам всем иногда хочется отвлечься и отдохнуть, и этим пользуются киберпреступники, рассылая сообщения с интересными заголовками, например: «Смотри смешное видео!» или «Забавное фото!». Однако надо обязательно удержаться от искушения открыть приложенный файл: с 99,99% вероятности он может содержать программы, способные нанести вред данным, хранящимся на вашем компьютере, отслеживать Вашу активность в Сети или попросту украдут у Вас что-нибудь…

***Фишинг***

Пожалуй, одним из наиболее известных видов мошенничества является фишинг. Вы получаете сообщение, в котором вас просят перейти по указанной ссылке и ввести личную информацию: пароль, номер банковского счета и т.д. Сообщение может выглядеть так, как будто оно пришло от банка, интернет-магазина eBay, платежной системы, например, PayPal и.т.д. Как бы убедительно ни выглядело сообщение, это все равно фальшивка: если вы нажмете на ссылку и введете запрашиваемую информацию, Ваши данные окажутся в руках киберпреступников, и те смогут использовать их в своих целях. Многие банки приняли дополнительные меры по безопасности для предотвращения попыток фишинга, в результате чего фишинговых сообщений, нацеленных на наиболее популярные банки, становится меньше. Однако это не значит, что такой вид мошенничества больше не используется — он всего лишь видоизменился в соответствии с веяниями времени.

Фишинговые сообщения — явление глобальное: один и тот же базовый текст переводится на разные языки, а само сообщение конструируется таким образом, чтобы выглядеть так, как будто это письмо от известного банка или финансовой организации. Мошенники кладут много сил на разработку дизайна сообщений, и нередко бывает сложно отличить использованные в них логотипы и цвета от оригинала. С другой стороны, текст часто изобилует грамматическими и орфографическими ошибками, что должно сразу же насторожить пользователя.

Помимо этого, если отправитель сообщения обращается к вам «Уважаемый клиент» вместо того, чтобы назвать Вас по имени, то это явный показатель фишинга. Сейчас, когда даже информационные рассылки могут быть персонализированы, очень маловероятно, что отправитель легитимного сообщения не будет использовать в обращении Ваше имя. И наконец, легитимные банки никогда не запрашивают PIN-код, код авторизации операции (TAN) или другую конфиденциальную информацию, тем более через электронную почту. Как мы уже говорили, от фишинговых атак могут пострадать не только банки. В последнее время многие фишинговые сообщения рассылаются для сбора информации об учетных записях в электронных платежных системам типа PayPal или сайтах-аукционах типа eBay.

Фишинг составляет 0,94% всех спам-сообщений, и целых 60% таких сообщений нацелены на PayPal. Такие сообщения зачастую содержат угрозы о том, что счет может быть закрыт по той причине, что он якобы не использовался в течение какого-то времени. Для того чтобы сохранить учетную запись, Вам предлагается войти в систему. А для этого, конечно же, в письме Вам услужливо предоставляется ссылка. При переходе по ссылке Вы попадаете на страницу, которая выглядит, как сайт соответствующей платежной системы, после чего Вас просят ввести логин и пароль.  
Несмотря на свою схожесть с оригиналом, такой веб-сайт — фальшивка. Никогда не пользуйтесь полученными по электронной почте ссылками на страницы, где Вас просят ввести конфиденциальную информацию. Используйте закладки в Вашем браузере или сами вводите адрес в адресной строке Вашего браузера. Даже если ссылка кажется верной, сценарий javascript, выполняющийся в фоновом режиме, может открыть адрес, который полностью отличается от отображаемого.

*3****. Мошенничество в социальных сетях***

Такие социальные сети как Одноклассники, Вконтакте, Facebook или MySpace пользуются особой популярностью у молодых людей. Эти сайты позволяют поддерживать связь с друзьями, обмениваться информацией, а также искать новых друзей.

Также существуют и социальные сети для пользователей постарше; они используются для установления и поддерживания деловых контактов или поиска школьных друзей. Какой бы сайт Вы ни использовали, Вас везде может подстерегать опасность.

Предположим, что Ваш близкий друг просит Вас о помощи. Скорее всего, Вы сразу же согласитесь помочь. А теперь перенесем эту ситуацию в контекст социальной сети. Друг посылает Вам сообщение о том, что он застрял в лондонском аэропорту Хитроу, ему угрожали оружием и ограбили. Он остался без денег, кредитной карточки и билета на самолет и просит переслать ему $400 через Western Union, чтобы он смог добраться домой. Возможно, Вы зададите себе вопрос, почему деньги необходимо перевести именно через Western Union? Друг утверждает, что для него это единственный способ их получить. Вы спрашиваете, как ему позвонить, но, естественно, его телефон украли. У Вас закрадывается все больше и больше подозрений — друг ведет себя странновато и использует выражения, которые Вы никогда раньше от него не слышали. Возможно, причиной тому — сложная ситуация, в которую он попал. Так как вам небезразлична судьба друга, и вы не хотите, чтобы вас мучили угрызения совести, в итоге Вы переводите деньги. И после этого он пропадает. Что же на произошло на самом деле?

В настоящее время этот вид мошенничества очень популярен и эффективен, так как о нем еще относительно мало известно. Объяснение достаточно простое: киберпреступники получают доступ к учетной записи Вашего друга и пытаются вытянуть деньги из всех, кто находится в его списке контактов. Если Вы часто пользуетесь социальными сетями, количество ваших друзей может насчитывать несколько сотен, и Вы не всегда в курсе, где они находятся в данный момент, что делает такую историю более правдоподобной. Однако в вышеописанном случае налицо признаки попытки мошенничества. Европеец, находясь в Лондоне, вряд ли станет просить другого европейца прислать американские доллары. То же самое относится к используемому языку и выражениям. Если Вы получаете такое сообщение, свяжитесь с другом напрямую. Даже если в сообщении он пишет, что его мобильный телефон украли, все равно попытайтесь набрать его номер: Вы будете приятно удивлены, когда он возьмет трубку и Вы не только сможете поболтать с ним, но также узнаете, что никакого сообщения он не посылал.

Чтобы защитить свою учетную запись в социальной сети от использования мошенниками, необходимо следовать нескольким несложным правилам. Один из возможных способов защиты Вашей учетной записи связан с тем, как устроена система восстановления пароля.

При регистрации в социальной сети обычно Вам предлагается ответить на «секретный вопрос». Если Вы забудете пароль, Вы сможете создать новый, ответив на заданный вопрос. Никому не сообщайте свой логин и пароль. Кроме того, не попадайтесь на удочку мошенников, рассылающих фишинговые сообщения (описаны выше) и используйте современный антивирус с актуальными антивирусными базами: это поможет вам избежать попадания на Ваш компьютер троянских программ, которые могут выкрасть пароль и переслать его киберпреступникам.

***Фильмы, игры, музыка и… вредоносные программы***

Если Вы только начинаете пользоваться интернетом, скорее всего, вы начнете с поиска фильмов, музыкальных файлов, ТВ-передач или компьютерных игр.

Помимо правового аспекта загрузки такого контента, о котором уже много писали, необходимо обратить внимание и на другие вопросы. Если Вы ищете контент такого рода, возможно, одноранговые сети покажутся Вам самым легким способом получить его, и Вы загружаете программу, которая поможет Вам зайти в сеть и качать все, что вам нужно. Хотя вы где-то читали, что такие файлы могут содержать вирусы, вы просто игнорируете этот факт. Однако вы поступаете так на свой собственный страх и риск. К примеру, к играм часто прилагаются инструменты для взлома, используемые для того, чтобы обойти защиту от копирования. Хакеры предоставляют такие инструменты, так как, по их мнению, любой контент должен быть бесплатным или потому что хотят произвести впечатление на хакерское сообщество.

Что касается самих загрузочных файлов, они могут содержать вредоносное ПО. Киберпреступники хорошо знают о наличии огромного рынка бесплатного контента и, маскируя вредоносные программы под популярные файлы или просто добавляя к популярным файлам вредоносные программы, они увеличивают число потенциальных жертв.

Например, вместе с игрой может загружаться банковская троянская программа — хотя молодые люди нечасто пользуются виртуальными банковскими услугами, компьютер, на который они загружают файл, может принадлежать их родителям, которые регулярно проверяют свой счет через интернет. Таким образом мошенники получают возможность убить сразу двух (или нескольких) зайцев.

Шансы попадания вредоносного ПО на компьютер из одноранговой сети довольно высоки. Поэтому, если, копируя нелегально игры или фильмы, Вы можете сэкономить, то загрузка троянской программы, предназначенной для кражи ваших банковских данных, может обойтись Вам в сотни евро, что мгновенно сводит всю выгоду к нулю. Несомненно, быть честным оказывается выгодно.

**Заключение**

Киберпреступники очень изобретательны и по мере возникновения новых интернет-технологий и приложений начинают применять их в своих мошеннических целях.  
То есть уже известные схемы приспосабливаются ими к новым возможностям. Лучший пример — классическое спам-сообщение со ссылкой на вредоносный веб-сайт. Теперь уже многие знают, что ни в коем случае нельзя нажимать на ссылки в электронных сообщениях от неизвестных отправителей. Однако когда это подход был приспособлен для использования в социальных сетях, количество людей, проходящих по ссылкам в нежелательных сообщениях, оказалось весьма большим. Еще несколько лет назад по внешнему виду сайта можно было определить подделка это или нет: ошибки в правописании, невзрачный внешний вид, и т.п. Однако сейчас киберпреступники стали намного более изощренными. Если Вы подозреваете, что имеете дело с мошенниками, поищите больше информации в интернете; если это действительно их рук дело, скорее всего, другие жертвы уже сообщили об этом. Найдите на подозрительных сайтах контактную информацию и сравните ее с другими источниками. И наконец, следуйте здравому смыслу.  
… Если что-то напоминает вам бесплатный сыр, то неплохо вспомнить и о мышеловке…