Общий обзор угроз

Финансовые махинации

Работая в Интернете, вы можете столкнуться с различными опасностями. Главная причина этого заключается в деятельности интернет-мошенников. Их основные цели заключаются в том, чтобы получить что-либо обманом от других пользователей или что-то украсть. Зная о том, как действуют мошенники, вы сможете свести к минимуму риск быть обманутым ими. Распространенное мошенническое действие – неправомерное получение денежных средств других пользователей. В частности, мошенники могут украсть деньги, хранящиеся на счетах в электронных платежных системах и на банковских картах. Для того чтобы это сделать, злоумышленнику нужно узнать ключевые данные для доступа к средствам. К таким данным относятся имена (логины) и пароли для входа в учетные записи платежных систем, данные банковских карт, необходимые для осуществления платежей.

Помимо кражи денежных средств мошенники нередко организуют фальшивые интернет-магазины либо интернет-магазины, которые продают некие цифровые товары, ценность которых явно завышена. Покупатель, который приобрел такой товар, обычно не получает то, на что рассчитывал.

В фальшивых интернет-магазинах и на мошеннических сайтах покупателю предлагают приобрести что-либо, произведя оплату с помощью отправки SMS-сообщения. Точно узнать сумму, которая будет списана со счета сотового телефона, можно либо из описания, сделанного добросовестным продавцом, либо после списания денег со счета.

В Интернете можно встретить множество предложений о получении высокого дохода без вложений либо с минимальными вложениями средств. Часто такие предложения касаются высокорисковых способов дохода, где вероятность потерять вложенные средства гораздо выше вероятности заработать. Иногда за подобными предложениями скрываются и откровенно мошеннические схемы.

Кража данных учетных записей

В Интернете ценность представляют не только деньги, но и учетные записи пользователей. В частности, особо ценны учетные записи электронной почты. Дело в том, что адрес электронной почты обычно используется для подтверждения регистрации на других веб-сайтах. Большинство веб-сайтов, предусматривающих регистрацию, поддерживают и функцию восстановления пароля.

Если пользователь забыл пароль к учетной записи и воспользовался возможностью его восстановления, на почтовый ящик, указанный при регистрации, может быть отправлено письмо с паролем или с данными для его восстановления.

Владея доступом к почтовому ящику, злоумышленник может завладеть и другими учетными записями. Основные цели здесь: кража денежных средств, если речь идет об учетных записях платежных систем, и недобросовестная реклама чего-либо. Например, если злоумышленник завладеет доступом к учетной записи в социальной сети, он сможет от имени пользователя рассылать рекламные сообщения. Обычно подобная деятельность через некоторое время пресекается администрацией социальной сети, во многом благодаря тому, что другие пользователи, заметив необычные действия, сообщают об этом.

Нередко мошенники используют для достижения своих целей вредоносные программы.

Вредоносные программы

В соответствии со ст. 273 УК РФ создание, использование и распространение вредоносных компьютерных программ уголовно наказуемо. Однако благодаря достаточно высокому уровню анонимности это не останавливает мошенников. Вредоносные программы используются для кражи информации и денежных средств. Их применяют для вымогательства денег, для скрытого управления компьютером, для нарушения работы компьютерных систем.

В Интернете существует несколько каналов распространения вредоносных программ.

Так, злоумышленники создают сайты, при переходе на которые на компьютер, не защищенный специальным программным обеспечением, может быть скопирована вредоносная программа. Ее действия зависят от логики, которую предусмотрел ее создатель. Например, она может просмотреть файлы пользователя и отправить злоумышленнику те из них, которые могут содержать сведения о паролях. Она способна уничтожить данные, сделав невозможной работу на компьютере. Она может передавать злоумышленнику все тексты, которые пользователь вводит с клавиатуры (в том числе и пароли). Такая программа способна заблокировать компьютер, сделав невозможной работу на нем, и выводить окно с предложением отправить платное SMS для разблокировки компьютера. Это – классический пример вымогательства.

Мошеннические веб-сайты нередко имеют адреса, которые очень сильно напоминают адреса известных сайтов – например, адреса поисковых систем. Внешний вид таких сайтов также может очень сильно напоминать те сайты, за которые они себя выдают. Ошибившись при вводе адреса сайта в адресную строку, вы рискуете попасть на такой сайт.

Работая в Интернете, вы будете видеть рекламные изображения или тексты, которые призывают вас щелкнуть по ним. Например, на таком изображении может быть сказано, что ваш компьютер заражен вирусами и вам срочно нужно от них избавиться, перейдя по ссылке. Относитесь к ним с осторожностью – они могут привести вас на сайт, который используется для распространения вредоносных программ.

Нередко вредоносные программы распространяются через электронную почту и программы для обмена сообщениями (такие как Skype или ICQ). Письмо или сообщение может либо содержать такую программу в виде вложения, либо содержать ссылку на сайт, при переходе на который компьютер может быть заражен.

В наши дни веб-сайты и системы обмена сообщениями – это основные пути распространения вредоносных программ. Однако нельзя забывать и о том, что многие вредоносные программы (компьютерные вирусы) распространяются другими способами – в частности, посредством заражения файлов на переносных носителях информации, например, на флэш-дисках.

Если компьютер "А" заражен и к нему был подключен флэш-диск, вирус может заразить файлы на этом диске. После того как диск будет подключен к неинфицированному компьютеру "В", этот компьютер также может быть заражен. Особенно опасны в этом плане компьютеры общего пользования.

Неосторожность пользователя

Определенную угрозу безопасности собственных данных и денежных средств создают пользователи, которые пренебрегают правилами безопасности или не знают о них. Нередко они полагают, что их данные не представляют интереса для кого-либо. В результате, не уделяя должного внимания безопасности, они сильно рискуют.

Неосторожность пользователей часто становится причиной поломки компьютеров. Основная опасность, которой подвержены настольные компьютеры и ноутбуки, – перегрев. Они перегреваются, когда вентиляционные отверстия, присутствующие на их корпусах, перекрываются или забиваются пылью.

Рекомендации по организации безопасной работы в Интернете

Вот общие рекомендации, следуя которым вы значительно повысите уровень безопасности и конфиденциальности при работе в Интернете.

1. **Пользуйтесь защитным программным обеспечением.** Если у вас не установлен антивирус и межсетевой экран (файрвол), работать в Интернете очень опасно.
2. **Пользуйтесь свежими версиями программного обеспечения.** Это касается всего программного обеспечения на вашем компьютере, особенно операционной системы, веб-браузера, защитного ПО. Обычно приложения настроены на автоматическое обновление. Не препятствуйте их обновлению, так как с их помощью компании-разработчики устраняют уязвимости к вредоносному ПО и повышают качество приложений. Защитное программное обеспечение обновляется чаще другого. Так оно способно наилучшим образом противостоять недавно появившимся вредоносным программам. Выключайте компьютер после работы, что позволит установить актуальные обновления при его включении.
3. **Никогда не передавайте конфиденциальные данные в ответ на письма или сообщения в социальных сетях.** Пароли к учетным записям нельзя передавать никому. Другие данные, такие как номер банковской карты, паспортные данные, можно передавать лишь при наличии предварительной договоренности и лишь тем людям, которых вы знаете. При этом категорически не рекомендуется пользоваться для передачи таких данных системами обмена сообщениями в социальных сетях и программами-мессенджерами. Обычно передача таких данных преследует определенную цель, которая вам известна и понятна. Получив запрос на предоставление подобной информации от неизвестного пользователя, не передавайте данные до тех пор, пока не выясните, кто этот пользователь и зачем они ему нужны.
4. **С осторожностью относитесь к неправдоподобно выгодным предложениям финансового характера.**
5. **Избегайте приобретать что-либо в Интернете, используя платные SMS-сообщения.** Если вы все же решитесь воспользоваться этим методом платежа, убедитесь в том, что вы точно знаете, какая сумма будет снята со счета. Если возникают малейшие сомнения в надежности сделки, SMS лучше не отправлять. В противном случае со счета телефона может быть снята сумма, во много раз превышающая заявленную.
6. **Используйте сложные пароли.** Такие пароли состоят из букв разных регистров, цифр, специальных символов. Не храните пароли на компьютере, либо используйте

специальные приложения для безопасного хранения паролей. Надежнее всего использовать для этого обычный бумажный блокнот.

7. **Не публикуйте в социальных сетях данные, попадание которых в свободный доступ недопустимо.** Даже если вы при публикации ограничите доступ к таким данным лишь пользователями-друзьями, кто-нибудь из друзей может опубликовать эти данные в общем доступе.
8. **Делайте копии важных данных и храните их отдельно от компьютера.** Это позволит вам сохранить такие данные, даже если с компьютером что-нибудь случится.

Потенциально опасные веб-сайты: снижение риска

Работая в Интернете, вы можете случайно попасть на потенциально опасные веб-сайты. Такие сайты создают мошенники. Эти сайты используются для распространения вредоносного программного обеспечения, для сбора адресов электронной почты, номеров сотовых телефонов, данных об учетных записях.

Распознать мошеннический сайт можно по следующим признакам:

- При переходе на сайт вы заметили необычное поведение. Например, вы щелкнули по какой-либо ссылке, была открыта страница, после чего, без вашего явного участия, в новом окне браузера была открыта еще одна страница. Такие страницы нужно как можно скорее закрыть.
- После перехода на сайт вам настойчиво предлагают загрузить и установить какое-то приложение. Например, вы можете увидеть сообщение о том, что ваш компьютер заражен компьютерным вирусом и вам срочно нужно скачать новый антивирус. Это может быть и сообщение о том, что ваш браузер устарел и вам срочно нужно скачать обновление. Не загружайте и не устанавливайте приложения, если вы не уверены в надежности веб-сайта, на котором они размещены. Подобные приложения могут стать источником серьезных проблем.
- Внешний вид сайта, который вам знаком, незначительно изменился. Возможно, ухудшилось качество изображений, иначе выглядят кнопки, поля ввода, в тексте содержатся ошибки. Адрес сайта в адресной строке выглядит иначе, чем обычно. Это может указывать на то, что вы находитесь не на том сайте, на который рассчитывали попасть. Например, если вы ввели в адресную строку браузера адрес сайта и ошиблись хотя бы в одном символе, вместо нужного веб-ресурса может быть открыт подставной сайт. Такой сайт может довольно точно копировать внешний вид и поведение другого сайта. Если вы сомневаетесь в подлинности сайта, надежнее всего закрыть вкладку браузера с его страницей и попытаться открыть нужный сайт снова. Причем нужно пользоваться тем способом, которым вы пользуетесь обычно. Например, воспользоваться закладкой на сайт, сохраненной в браузере, или, если вы точно знаете адрес сайта, внимательно ввести его в адресную строку. Если вы и после повторного открытия сайта, сомневаетесь в его подлинности, возможно, ваш компьютер заражен вирусом, подменивающим страницы.
- После перехода на сайт вам настойчиво предлагают ввести какие-либо данные о себе – например, адрес электронной почты. Обычно это делается под вполне благовидным предлогом. Введя на таком сайте адрес электронной почты, вы можете сделать свой

почтовый ящик мишенью для рассылки нежелательной рекламы или для других нежелательных или опасных действий.

- После перехода на сайт вы видите требование об отправке SMS-сообщения на некий номер для подтверждения учетной записи или для входа в учетную запись. Этим приемом часто пользуются мошенники для кражи денежных средств пользователей. При этом мошеннические страницы могут быть оформлены так же, как страницы популярных веб-сайтов, – например, страницы входа в учетные записи социальных сетей.

Если вы подозреваете, что оказались на мошенническом сайте, постарайтесь как можно быстрее закрыть вкладку браузера, на которой открыта его страница. Если у вас возникают малейшие подозрения в подлинности некоего известного вам сайта, работа с которым предусматривает ввод логина и пароля, не вводите на нем никаких данных.

Если вы, работая в Интернете, видите рекламные объявления, настойчиво призывающие вас щелкнуть по ним, не делайте этого. Такие объявления могут вести на мошеннические сайты.

Безопасный поиск

Поисковые системы, такие как http://www.yandex.ru/ и http://www.google.com, имеют механизмы, которые ограничивают попадание потенциально опасных веб-сайтов и сайтов с непристойным содержимым в результаты поиска.

Работая с поисковой системой Google, вы можете включить функцию фильтрации результатов поиска. Для этого нужно перейти по ссылке http://www.google.com/preferences. На открывшейся странице (рис. 1), нужно установить флаг **Не показывать непристойные результаты**.

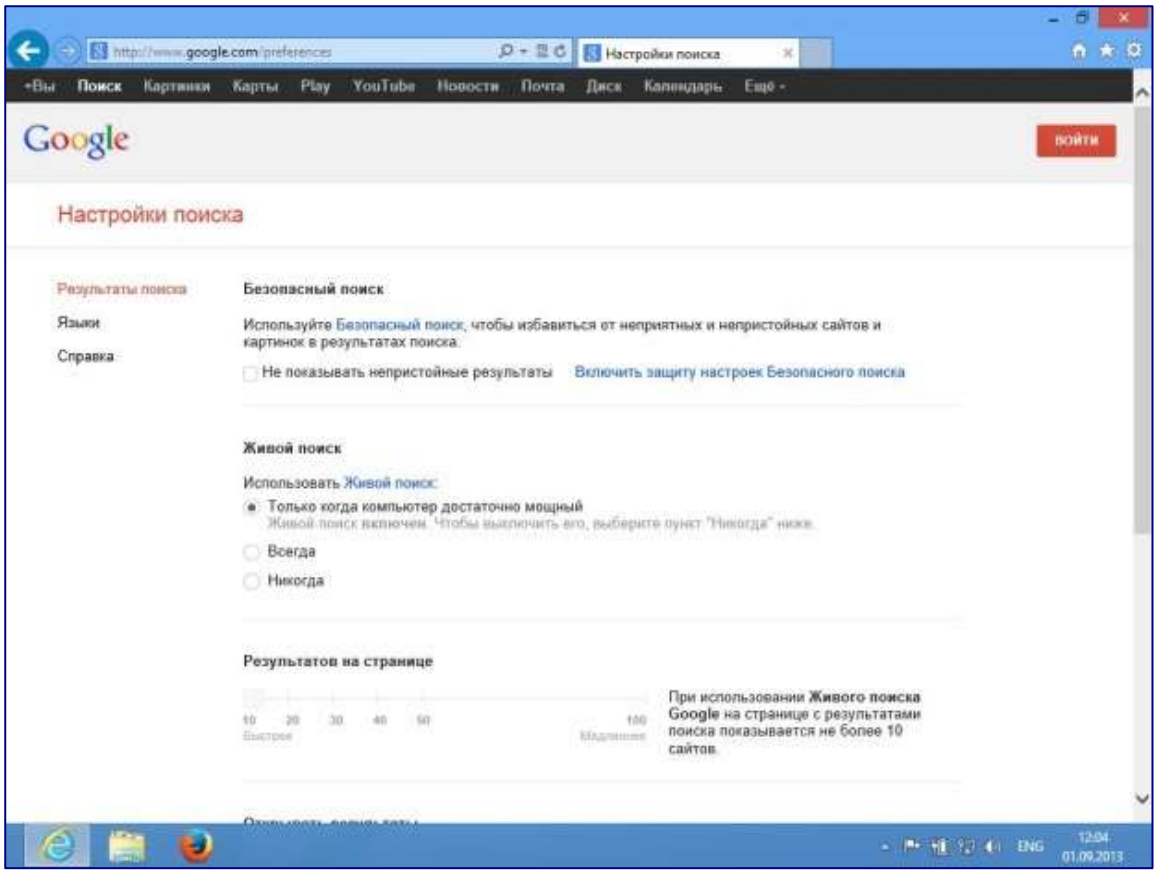

Рис. 1. Включение безопасного поиска в поисковой системе Google Обратите внимание на ссылку **Включить защиту настроек безопасного поиска**. Она позволяет защитить эти настройки паролем. Для того чтобы парольная защита работала, необходимо иметь учетную запись Google. При щелчке по ссылке будет показана страница для входа в учетную запись.

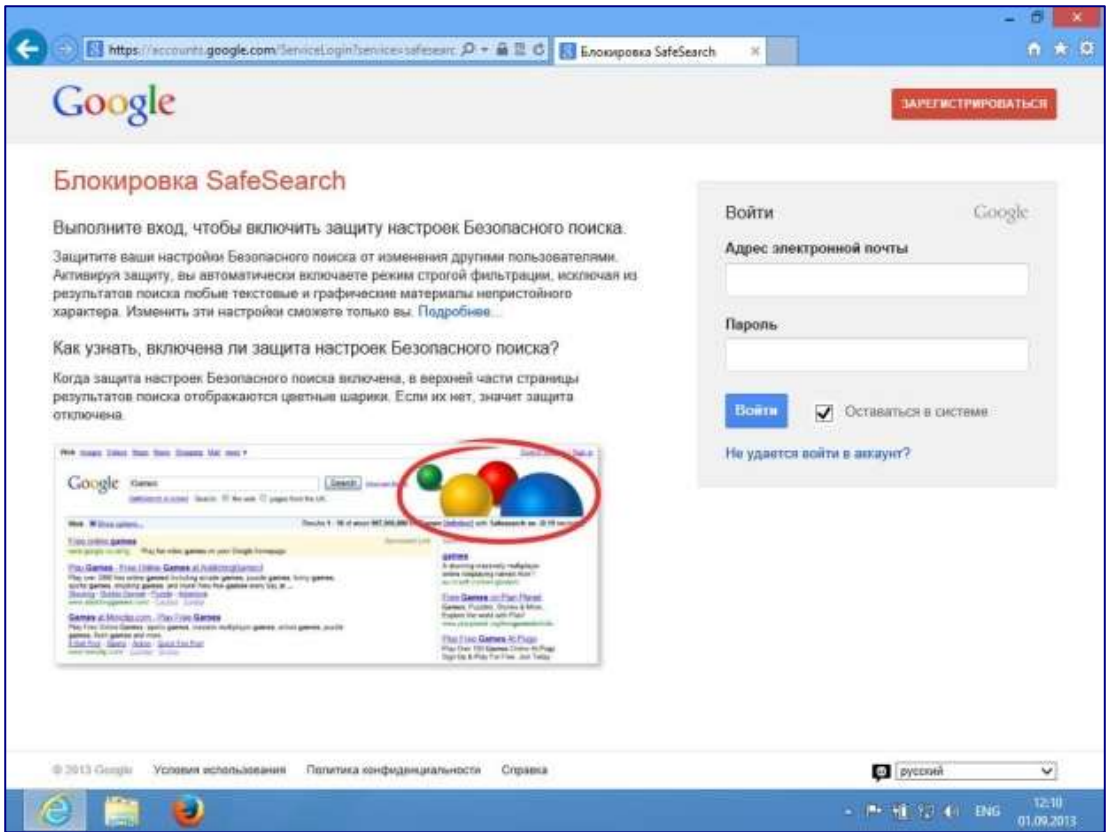

Рис. 2. Страница входа в учетную запись Google Если у вас уже есть учетная запись Google, введите здесь адрес электронной почты и пароль, если нет – вы можете зарегистрировать ее, щелкнув по кнопке **зарегистрироваться**. После входа в учетную запись вы увидите страницу (рис. 3), на которой нужно нажать на кнопку **Включить защиту настроек безопасного поиска.**

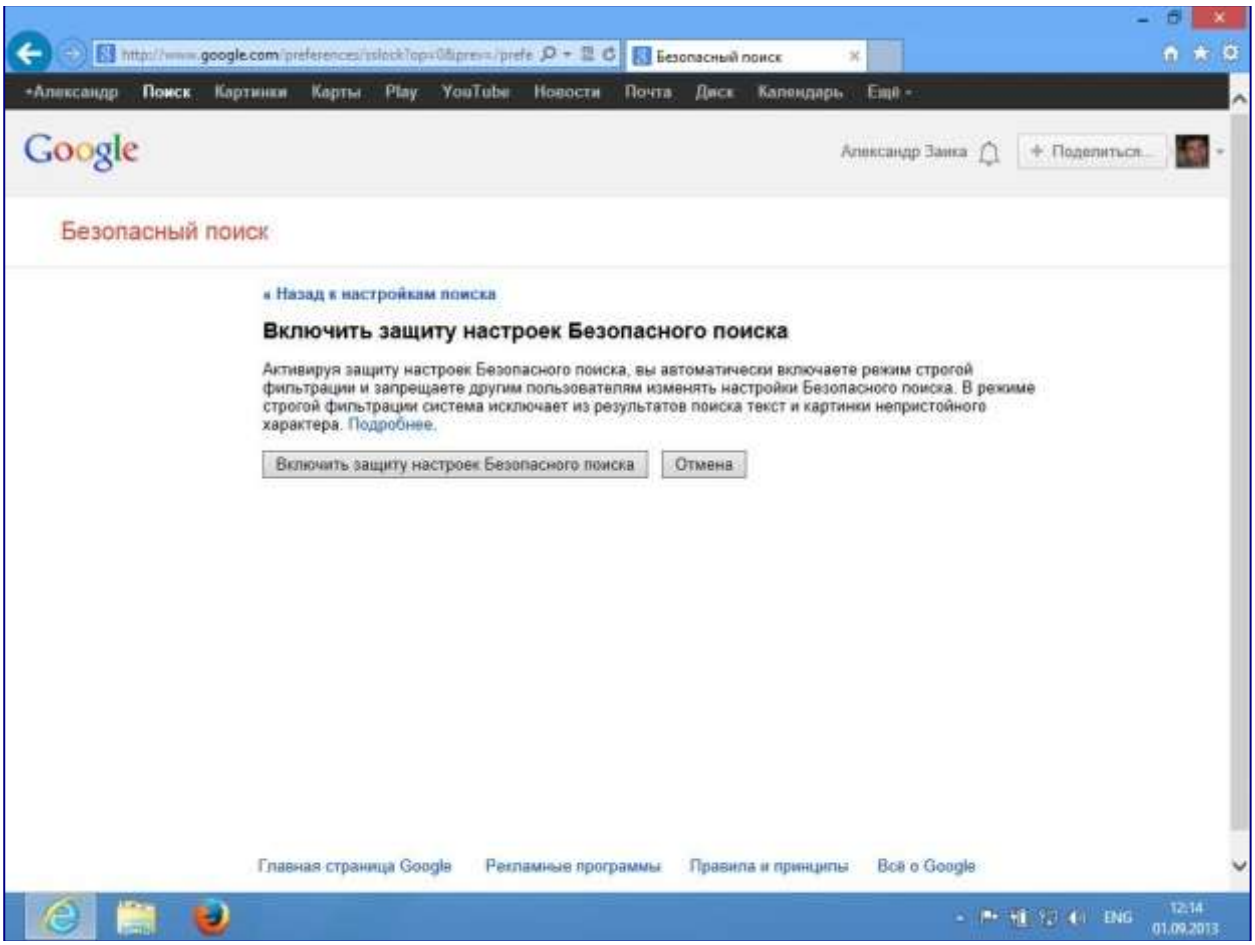

Рис. 3. Включение защиты настроек безопасного поиска. После успешного выполнения операции вы увидите страницу с сообщением о включении защиты настроек (рис.4)

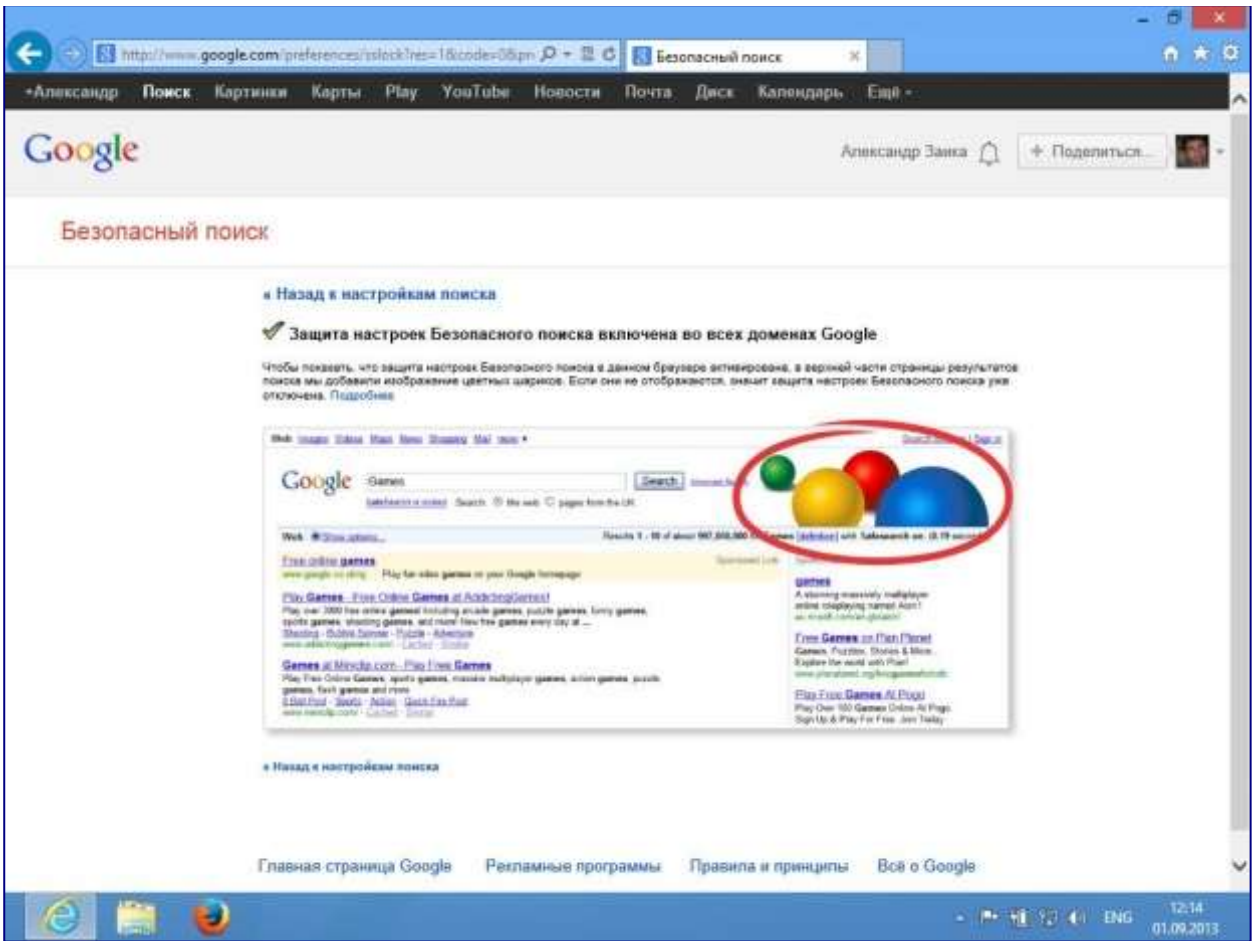

Рис. 4. Успешная защита настроек Теперь для того, чтобы отключить настройки безопасного поиска, нужно будет знать данные для входа в учетную запись Google. Для включения фильтрации результатов поиска в системе Яндекс нужно щелкнуть по ссылке **Настройка**, которая расположена правее строки поиска на странице результатов поиска (рис. 5).

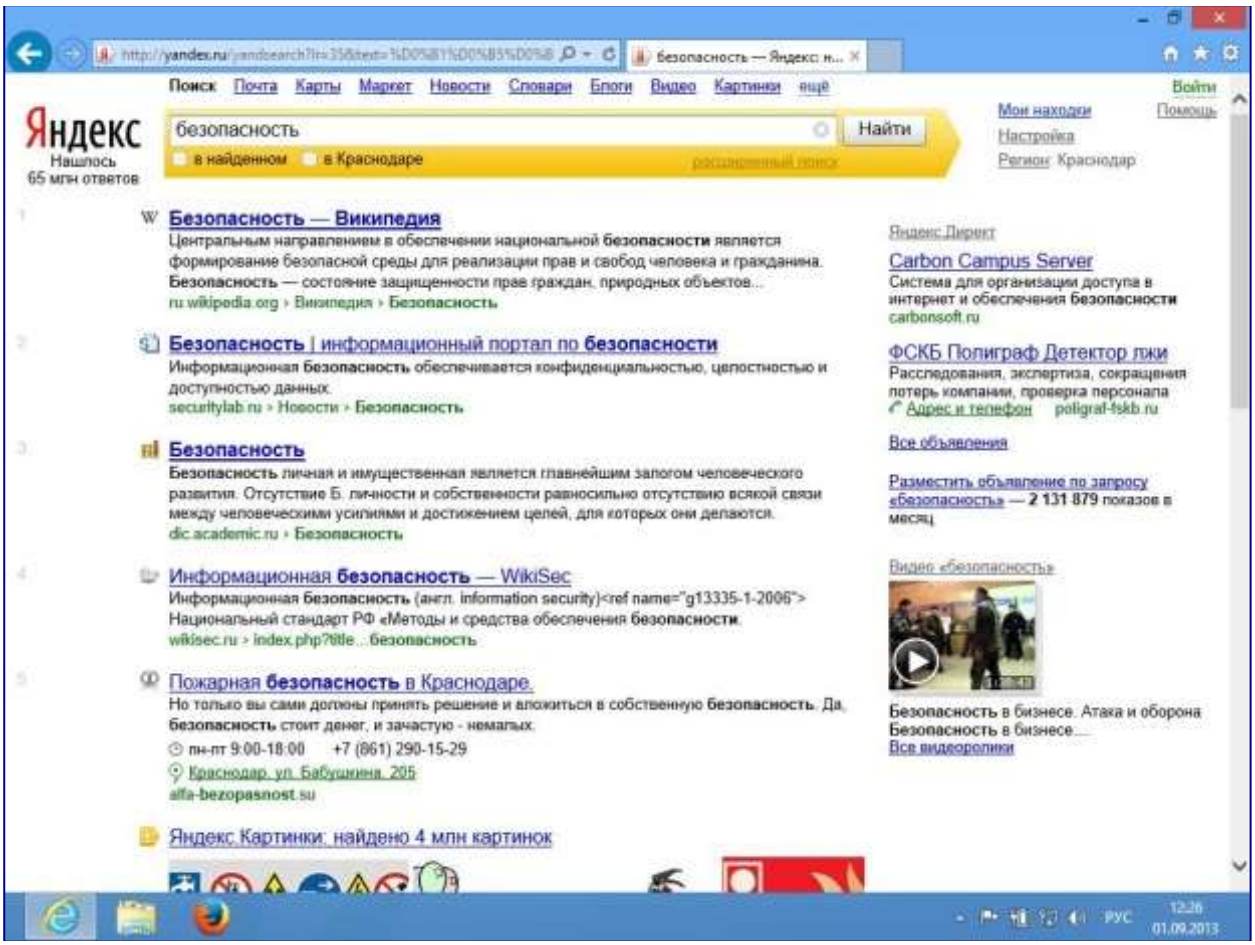

Рис. 5. Ссылка для перехода к настройкам поиска На открывшейся странице (рис. 2.6) нужно найти группу параметров **Область поиска** и установить параметр **Фильтрация страниц** в значение **Семейный поиск**.

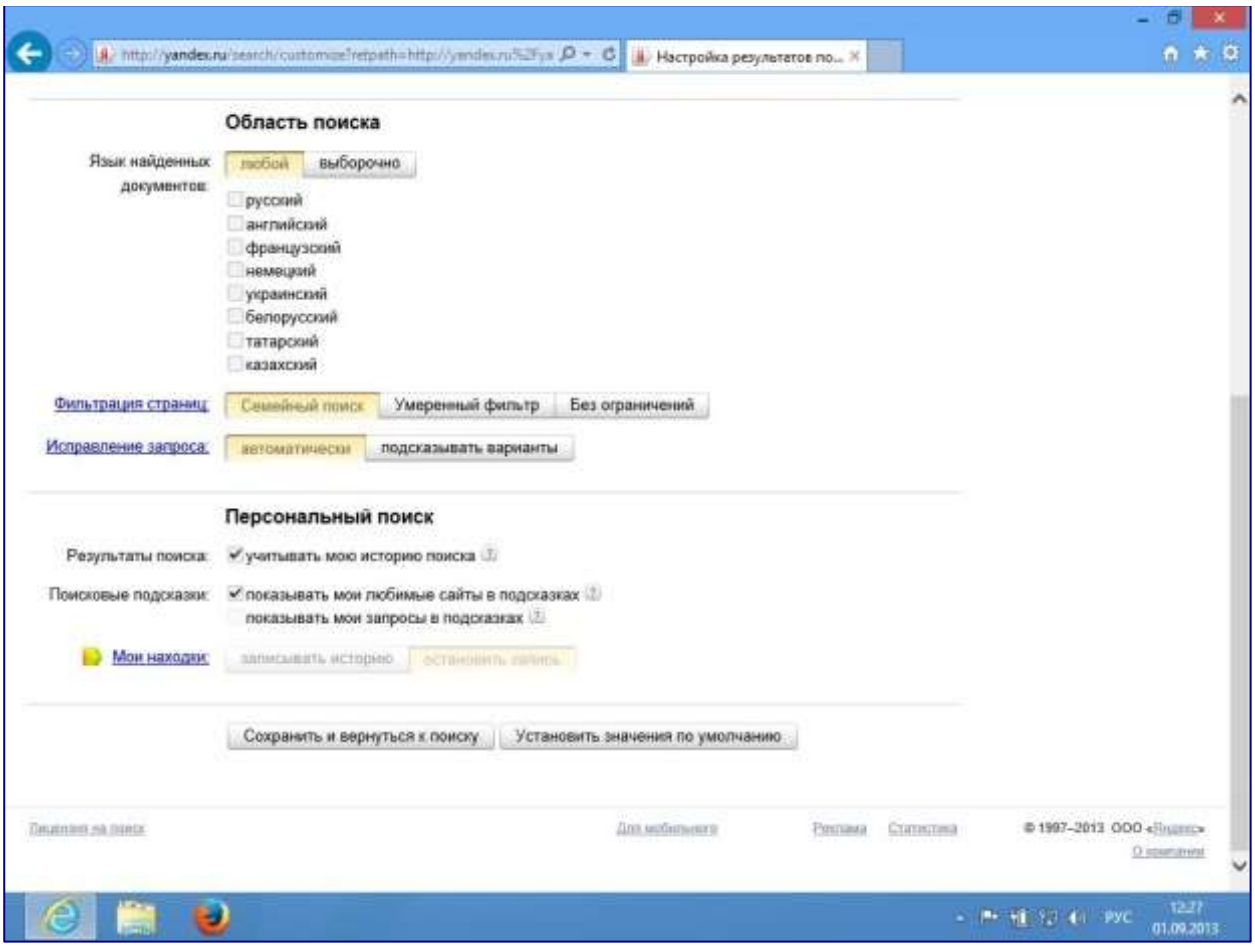

Рис. 6. Включение семейного поиска в системе Яндекс После этого нужно нажать на кнопку **Сохранить и вернуться к поиску** Функция безопасного поиска особенно важна, если за компьютером работают дети. Однако защита детей при работе в Интернете подразумевает дополнительные средства обеспечения безопасности, этим средствам посвящен наш специальный курс.

Безопасность при работе с электронной почтой и с системами обмена сообщениями

Электронная почта и системы обмена сообщениями часто являются каналами распространения вредоносных программ. Кроме того, ими пользуются мошенники для того, чтобы обманом получать какие-либо секретные сведения.

В потенциально опасных сообщениях обычно содержатся ссылки и предложение перейти по ним. Предлоги могут быть самые разные. Например, в сообщении может говориться о том, что по ссылке расположена какая-то интересная страница.

Нередко в подобных сообщениях говорится о том, что ваша учетная запись на каком-либо сайте взломана, и для того, чтобы восстановить доступ к ней, вам нужно перейти по ссылке и выполнить какие-либо действия. Потенциально опасное сообщение может быть замаскировано под сообщение от администрации некоего сайта, с которым вы работаете. Переход по ссылке приведет вас либо на мошеннический сайт, либо на страницу, которая используется для распространения вредоносных программ. При этом сообщение может быть отправлено и с незнакомого адреса, и с адреса человека, с которым вы уже переписывались. Текст таких сообщений часто изобилует ошибками и выглядит неестественно. Это –

результат автоматического составления текста письма вредоносной программой. Даже если текст письма не содержит ошибок, его стиль может отличаться от стиля того человека, от имени которого написано письмо. Это – признаки потенциально опасного письма. Надежнее всего – связаться с этим человеком альтернативным способом (например, позвонив по телефону) и спросить у него, отправлял ли он вам письмо, которое показалось вам подозрительным. Иногда в потенциально опасных сообщениях можно увидеть поля для ввода логина и пароля на каком-либо сайте. В тексте может быть указано, что, введя здесь логин и пароль, вы можете восстановить доступ к взломанной учетной записи.

Основное правило при получении подобных сообщений заключается в том, что нельзя переходить по ссылкам, которые в них присутствуют. Если вы зарегистрировались на каком-либо сайте и получили письмо с просьбой щелкнуть по ссылке для подтверждения адреса почтового ящика, по этой ссылке можно щелкнуть, не опасаясь мошенничества. Если же письмо со ссылкой пришло неожиданно – не переходите по ссылкам, которые в нем есть.

Иногда потенциально опасные сообщения содержат, в виде вложений, различные файлы. В них может присутствовать предложение скачать эти файлы. Не скачивайте такие файлы и не пытайтесь с ними работать. В них могут находиться замаскированные вредоносные программы.

Если вы, работая с электронной почтой, используете веб-интерфейс почтовой системы, ознакомьтесь с настройками безопасности этой системы. Обычно к настройкам имеются пояснения. Изучите эти материалы и выполните те настройки, которые позволят повысить безопасность работы.

Периодически меняйте пароль к электронному почтовому ящику. Если некто пытается подобрать пароль, это серьезно усложнит ему задачу. Эта рекомендация касается и паролей к другим учетным записям.

Безопасная работа с банковскими картами и платежными системами

Для расчетов в Интернете используются пластиковые банковские карты и системы электронных денег.

Злоумышленников интересуют следующие данные банковских карт:

- Номер карты.
- CVV2-код (у карт системы Visa).
- CVC2-код (у карт системы MasterCard).
- Срок действия карты.
- Имя и фамилия владельца карты.

Кража этих данных (или хотя бы номера карты и CVV2/CVC2-кодов), сравнима с кражей карты и кода для снятия денежных средств с нее в банкомате.

Если появляется подозрение, что кто-то узнал конфиденциальные данные карты, ее нужно немедленно заблокировать. Банки при открытии карты сообщают клиентам номера телефонов, позвонив по которым можно заблокировать карту. Блокировка карты в подобной ситуации – самый быстрый и надежный способ обезопасить себя от кражи денежных средств с карты.

Повысить безопасность расчетов по карте помогает система одноразовых паролей для подтверждения факта списания средств. Обычно такой пароль приходит в виде SMS-сообщения на сотовый телефон владельца карты.

Для того чтобы снизить вероятность серьезных потерь при краже данных карты, на карте, которой вы пользуетесь для покупок в Интернете, не следует хранить крупные суммы денег. Еще значительнее повысить безопасность расчетов можно, используя так называемые виртуальные предоплаченные карты. Обычно выпуск таких карт производится в интернет-службах банков, в которых открыты карты. Оплачивая покупки в Интернете с помощью виртуальной предоплаченной карты, вы рискуете лишь суммой остатка на ней. Доступ к системам электронных денег напоминает доступ к обычному электронному почтовому ящику. Обычно в таких системах можно использовать дополнительные средства защиты. Среди них следующие:

- Использование платежного пароля для подтверждения операций по списанию средств.
- Использование одноразовых паролей, высылаемых по SMS на телефон владельца счета в системе.
- Повышенные требования к основному паролю для входа в систему.
- Использование дополнительных ключевых данных для доступа к электронному кошельку.

Работая с некоей платежной системой, выясните, какие средства обеспечения безопасности в ней предусмотрены, и пользуйтесь ими.

Если вы подозреваете, что кто-то узнал пароль к вашему электронному кошельку, – немедленно поменяйте его. Если сделать этого не удастся (то есть злоумышленник поменял пароль) – нужно связаться с администрацией системы и сообщить о проблеме. Данные для связи обычно указаны на веб-сайтах платежных систем. Кража денежных средств в Интернете – это не только кража данных банковских карт или информации для доступа к платежным системам, это и непосредственная кража денежных средств, которые поступают недобросовестным продавцам от покупателей. Речь идет о мошеннических интернет-магазинах.

Оценивая надежность интернет-магазина, обратите внимание на наличие среди контактной информации адреса и телефона. Позвоните по указанному телефону, уточните информацию о тех товарах, которые собираетесь заказать. Мошенники обычно не любят приводить такие данные или размещают на страницах контактной информации поддельные адреса и телефоны.

Для того чтобы убедиться в надежности некоего нового интернет-магазина, поищите отзывы о нем на независимых ресурсах. Учитывайте, что положительные отзывы могут быть оставлены создателями магазина, а отрицательные – его конкурентами. Если анализ отзывов показывает, что магазин создан не мошенниками, и вам очень нужно то, что в нем продается, используйте для первого заказа метод оплаты, который не предусматривает электронное совершение платежа. Это – оплата при доставке товара курьером, оплата почтовым или банковским переводом, оплата наложенным платежом при получении на почте. Если, получив первый заказ, вы убедились в том, что магазин действительно существует, и довольны качеством товара – продолжать работу с ним можно, используя и электронные средства платежей.

Списки надежных интернет-магазинов обычно можно найти на веб-сайтах электронных платежных систем.

Защитное ПО: основные сведения

Система программной защиты компьютера от информационных угроз включает в себя антивирус и межсетевой экран (файрволл, брандмауэр).

Антивирус – это программа, которая умеет бороться с компьютерными вирусами, например с теми, которые могут попасть на компьютер с зараженного флэш-диска или из Интернета.

Межсетевой экран – это программа, которая помогает предотвратить незаконный доступ к компьютеру при работе в Интернете.

Если на вашем компьютере установлена операционная система Windows , это означает, что у вас уже есть и антивирус, и межсетевой экран. То есть на базовом уровне ваш компьютер уже защищен. Для повышения уровня защиты и для получения возможности использовать дополнительные защитные механизмы вы можете воспользоваться дополнительным программным обеспечением.

Компании, производящие такое программное обеспечение, предлагают его в различных вариантах. Весьма популярны универсальные решения, объединяющие в себе антивирус, межсетевой экран и иногда дополнительные средства защиты системы. В частности, это следующие комплексные защитные продукты:

- Kaspersky Internet Security.
- ESET NOD32 Smart Security.
- Dr.Web Security Space.

Подобные программы работают на компьютере постоянно, обеспечивая его непрерывную защиту. В некоторых случаях нужно проводить дополнительную проверку системы с помощью специальных программ, таких как Microsoft Security Scanner, Kaspresky Virus Removal Tool и других подобных.

Кроме того, существует программное обеспечение, которое предназначено для использования в экстренных ситуациях. Например, тогда, когда компьютер, атакованный вредоносным ПО, перестает загружаться. Это, например, Kaspersky Rescue Disk и DrWeb LiveCD. Использование такого ПО позволяет как минимум спасти данные, которые хранятся на компьютере.

Для хранения и передачи особенно важных данных можно применять шифрование. Существует простой и доступный метод шифрования, отличающийся высокой стойкостью к взлому. Он заключается в создании RAR-архивов, закрытых паролем. Для создания таких архивов можно воспользоваться программой-архиватором.

Об этих и о некоторых других защитных программах вы узнаете на следующих занятиях.

Нужно учитывать, что использование дополнительного защитного программного обеспечения повышает уровень защищенности компьютера, но не отменяет других правил безопасности. Только совместные действия пользователя и защитного ПО позволяют говорить о достижении высокого уровня безопасности при работе в Интернете.