Классификация Интернет-угроз

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, 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.

Рассмотрим подробнее вышеперечисленные угрозы.

Вредоносное ПО

Что такое Malware (вредоносное ПО)?

Malware (от англ. „malicious software“: malicious — злонамеренный и software — программное обеспечение) - общепринятый термин, используемый для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу, или компьютерной сети. Вредоносные программы представляют собой широкую категорию программного обеспечения. Они устанавливаются без Вашего разрешения и влияют на работу Вашего компьютера.

Наиболее распространенными видами вредоносных программ являются трояны, черви и вирусы.

Троян - вредоносная программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях

Компьютерный вирус — разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликации). В дополнение к этому он может повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена заражённая программа.

Сетевой червь — разновидность самовоспроизводящейся компьютерной программы, распространяющейся в локальных и глобальных компьютерных сетях. В отличие от компьютерных вирусов червь является самостоятельной программой. Trackware - новая вариация вредоносной программы, которая отслеживает и регистрируют действия, производимые на компьютере.

Каким образом вредоносные программы проникают на компьютер пользователя?

Вредоносные программы, чаще всего, проникают на компьютер через Интернет или по электронной почте. Если Вы сделаете ошибку в URL-адресе или случайно нажмете на известную ссылку, то можете попасть на опасные сайты с «агрессивным» содержания или вредоносными программами. P2P (peer-to-peer) сети, в которых пользователи могут передавать файлы непосредственно с одного компьютера на другой, представляют существенный риск для заражения компьютера вредоносным и рекламным ПО.

Как вредоносные программы влияют на работу компьютера?

Симптомами заражения вредоносной программой являются всплывающие окна, снижение работоспособности системы или перенаправление запросов в браузере на нежелательные сайты. Вредоносные программы влияют на нормальное функционирование системы, что может привести к отказу в обслуживании, замене данных и понижению пропускной способности сети. Кроме того, компьютер будет невозможно выключить или перезагрузить.

Как защитить компьютер от вредоносных программ?

Вредоносные программы зачастую распространяются в приложении с другими файлами, так что не открывайте вложения электронной почты, отправленные с неизвестных Вам ресурсов. Никогда не принимайте файлы от незнакомых Вам пользователей, а также проявляйте осторожность, когда открываете файлы с расширением: AVI, EXE или JPG.

Если Вы подозреваете, что Ваш компьютер заражен вредоносной программой:

- Приостановите любую деятельность, которая связана с использованием логинов, паролей и другой конфиденциальной информации.

- Используйте антивирусное ПО для защиты Вашей системы от возможных онлайн-угроз.

- Убедитесь, что Ваша антивирусная программа обновлена, сканирует компьютер и удаляет все программы, которые определяются как вредоносные. Зачастую, в спешке можно невнимательно прочитать всплывающее сообщение, которое содержит неверную информацию об окончании проверки компьютера и обнаружении вредоносных программ. В подобном сообщении предлагается загрузить фальшивое программное обеспечение, которое широко используется для распространения вредоносных программ.

- После того, как Вы очистили свой компьютер от вредоносного ПО:

- Регулярно обновляйте Ваше антивирусное программное обеспечение.

- Во время пользования Интернетом, включайте брандмауэр.

- Прежде чем открывать скаченные файлы, проверяйте их с помощью антивирусной программы.

- Не открывайте вложения электронной почты, отправленные с неизвестных Вам ресурсов.

Рекламное ПО

Что такое Adware (рекламное ПО)?

Adware – (от англ. Advertisement — реклама и Software — программное обеспечение) - нежелательное программное обеспечение, содержащее рекламу. Adware поставляется в сочетании с программными продуктами, как правило, бесплатными или условно-бесплатными. В дальнейшем, при использовании программного продукта пользователю принудительно показывается реклама. Некоторые компоненты

Adware обычно скрыты, что усложняет процесс их удаления. Также, рекламные системы могут собирать конфиденциальную информацию о компьютере и пользователе:

- IP-адрес компьютера;

- версию установленной операционной системы и интернет-браузера;

- список часто посещаемых пользователем интернет-ресурсов;

- поисковые запросы;

- прочие данные, которые можно использовать при проведении последующих рекламных кампаний.

Каким образом Adware проникает на компьютер пользователя?

Чаще всего, рекламные компоненты Adware интегрированы в бесплатные приложения. MyWay Searchbar, имеющий утилиты SmileyCentral и Zwinky, и WeatherBug (рекламный модуль, который может быть отключен только после оплаты обновления) – примеры приложений, сообщавших о содержащихся рекламных компонентах. Также, Adware и Spyware (шпионские программы) программы могут быть установлены через «дыры» в безопасности браузера или операционной системы.

Как Adware-программы влияют на работу компьютера?

Всплывающие рекламные объявления появляются во время просмотра веб-страниц и общего использования ПК. Это раздражает и, в некоторых случаях, снижает производительность системы.

Как защитить себя от Adware?

Прежде, чем Вы сможете защитить свой компьютер от Adware-программ, убедитесь, что Вы удалили все рекламные компоненты, которые уже были на Вашем ПК.

- Запустите обновления anti-spyware и anti-adware программ.

- Включите опцию иммунизации в anti-spyware и anti-adware ПО.

- Убедитесь, что ваша операционная система, браузер и программа электронной почты - обновлены, с целью исключить появление в них уязвимостей.

- При пользовании Интернетом включите брандмауэр.

Шпионское ПО

Что такое Spyware (шпионское ПО)?

Spyware (от англ. Spy — шпион и Software — программное обеспечение) – это несанкционированно установленный программный продукт, целью которого является скрытое отслеживание поведения пользователя в сети. Также, подобные программы используются для сбора различных типов личной информации:

- привычка пользования Интернетом и посещаемые сайты (Tracking Software)

- контроль нажатий клавиш на клавиатуре компьютера (Keyloggers)

- контроль скриншотов экрана монитора компьютера (Screen Scraper)

- несанкционированный удалённый контроль и управление компьютерами (Remote Control Software)

- несанкционированный анализ состояния систем безопасности (Security Analysis Software)

Spyware могут даже менять установки в компьютере для несанкционированного внесения изменений в операционную систему, результатом чего являются снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ.

Каким образом программы-шпионы проникают на компьютер пользователя?

Часто Spyware распространяются в комплекте с другим программным обеспечением, бесплатными пробными (trial) версиями программ и с некоторыми скачиваемыми продуктами. Также, программы-шпионы попадают в систему посредством обмана пользователя или через уязвимости системы.

Как Spyware влияет на работу компьютера?

Большинство пользователей считают, что программы-шпионы нарушают неприкосновенность их частной жизни, так как могут устанавливаться без их согласия. Некоторые типы Spyware отключают брандмауэр и антивирусные программы и/или понижают установки безопасности браузера, таким образом, делая систему неприкрытой для дальнейшего вредоносного ПО. При удалении какого-либо компонента Spyware, программа автоматически его восстанавливает. В дополнении к разрушению системы Вашего компьютера, программы-шпионы могут запускать всплывающие рекламные окна, влиять на производительность процессора и эффективность работы других программ. Чрезмерное количество spyware-программ на Вашем компьютере может привести к частым сбоям и снижению скорости работы системы

Как защитить компьютер от spyware?

Самый лучший способ защитить себя и свой компьютер в Сети - проявлять осторожность.

- Ознакомьтесь с правилами безопасного серфинга и информацией о новых угрозах.
- Запустите антишпионские и антивирусные программы для очистки компьютера.
- Убедитесь, что на Ваш браузер и операционную систему установлены последние обновления.
- Включите автоматическое обновление программного обеспечения.
- Установите в браузере высокий уровень безопасности и конфиденциальности информации.
- Игнорируйте всплывающие рекламные окна.

Браузерный эксплойт

Что такое браузерный эксплойт?

Браузерный эксплойт (иначе «атака браузера» или «незапрашиваемая загрузка») - это форма вредоносного кода, которая использует уязвимость в браузере или компоненте системы, с целью изменить настройки без Вашего ведома.

Каким образом осуществляется браузерный эксплойт?

Если в Вашем браузере есть «слабые места», хакер может их использовать. Например, скрипты ActiveX могут загружаться самостоятельно и использоваться для изменения общих настроек или отдельных компонентов, что усложняет процесс их удаления. Браузерный эксплойт может быть в виде сообщения, отображаемого во время работы браузера. Сайты злоумышленников могут предоставлять инструкции по установке дополнительного программного модуля для корректного просмотра сайта и других сервисов, уверяя пользователя, что они получают расширение браузера или обновлении системы.

Как браузерный эксплойт влияет на работу компьютера?

Обычно атака браузера не вредит данным, хранящимся на компьютере, или их передаче через электронную почту. Признаки браузерного эксплойта:

- Ваша домашняя страница, страница поиска или избранное были изменены.

- Настройки интернета были изменены.

- Блокируется доступ к некоторым функциям браузера.

- Переадресация при неверном вводе URL-адреса (например, при вводе неверного адреса Вы попадаете на другой сайт).

Как защитить компьютер от браузерного эксплойта?

- Установите брандмауэр для защиты ПК.

- Регулярно обновляйте операционную систему, браузер и другое программное обеспечение с сайта поставщика.

- Никогда не принимайте файлы от незнакомых Вам пользователей.

- Не открывайте вложения, отправленные с неизвестных Вам ресурсов.

- Проявляйте осторожность при скачивании файлов.

- Проверяйте перед установкой скаченное программное обеспечение.

- Отключайте ActiveX, Java and JavaScript в настройках браузера (если возможно).

Спам

Спам (англ. spam)– это массовая незапрашиваемая рассылка электронных сообщений, рекламирующих услуги или продукты.

Каким образом распространяется спам?

Большинство спамеров используют массовую рассылку для распространения рекламы, продукции или различных вирусов. В первую очередь, термин «спам» относится к электронным письмам. Незапрашиваемая рассылка в программах обмена мгновенными сообщениями называется SPIM (от англ. Spam over IM). Также, известен термин SPIT (от англ. Spam over IT) - спам, распространяемый через IP-телефонию (например, через форумы пользователей Skype).

Как спам влияет на работу компьютера?

Несмотря на то, что спам может и не содержать вирусы или другие вредоносные программы, это вызывает неудобство и приводит к снижению производительности, так как Вы ежедневно вынуждены отслеживать и удалять нежелательные сообщения. В крупных организациях большое количество спама может вызвать перегрузку почтового сервера, что влияет на эффективность работы. В крайних случаях спамеры используют известные уязвимости в программном обеспечении или компьютерные вирусы для того, чтобы захватить управление над большим количеством компьютеров, подключенных к Интернету, и уже их использовать для рассылки сообщений другим пользователям.

Как защитить себя от спама?

Спам – это массовый побочный эффект электронной почты. Несмотря на то, что Вы вряд ли сможете полностью избавиться от спама, есть способы уменьшить его количество. Один из способов заключается в фильтрации спама через списки отправителей. Например, Вы можете установить правило для получения сообщений только от пользователей из Вашего списка контактов, а остальная корреспонденция будет автоматически отправляться в отдельную папку. Также, большинство почтовых программ имеют опцию «фильтр». Помните, что время от времени папку со спамом следует проверять.Советы по уменьшению количества спама:

- Перед тем, как размещать где-либо адрес своей электронной почты, ознакомьтесь с политикой конфиденциальности ресурса. Каждый порядочный сайт должен предоставить ссылку на раздел, посвященный политике конфиденциальности, где объясняется, каким образом будут использованы предоставленные данные.

- В процессе регистрации аккаунта, убедитесь, что все настройки, установленные по умолчанию (например, подписка на рассылку), отключены.

- Отвечая на спам-письма или открывая ссылки, присланные в них, Вы подтверждаете, что Ваш электронный адрес является действующим. В дальнейшем, Вы будете получать еще большее количество нежелательной корреспонденции. Будет правильнее полностью игнорировать подобные сообщения и удалять их.

- Для защиты Вашей электронной почты от большого количества спама, зарегистрируйте еще один email и используйте его исключительно для покупок через интернет, чатов и других онлайн-сервисов.

Кибермошенничество

Что такое интернет-мошенничество?

Интернет-мошенничество – 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 Вашу личную информацию, что предполагает мошенничество или обман.

Виды интернет-мошенничества:

- Нигерийские письма

- Фишинг

- Вишинг

- Фарминг

Каким образом осуществляется интернет-мошенничество?

Многие интернет-аферы – это варианты мошеннических схем, существовавших еще до появления Сети, число которых увеличилось вместе с популярностью онлайн-шоппинга и других типов электронной коммерции. Для обмана пользователей интернет-мошенники используют электронную почту, чаты, форумы и фальшивые веб-сайты.

Как защитить себя от интернет-мошенничества?

Интернет-мошенничество и кража личных данных может произойти, если Вы отвечаете на спам-сообщения или на Ваш компьютер была запущена какая-либо вредоносная программа, позволившая

хакеру получить к нему доступ. Лучшая защита от интернет-мошенничества – здравый смысл. Если предложение слишком хорошо, чтобы быть правдой, то это, скорее всего, обман!

- Не доверяйте любым нежелательным сообщениям, содержащим просьбу предоставить личную информацию.

- Игнорируйте спам.

- Никогда не предоставляйте Ваши персональные данные людям, в личности которых Вы недостаточно уверены.

- Запомните Ваши пароли и PIN-коды.

- Будьте очень осторожны при совершении онлайн-покупок, так как существует угроза фишинга, при которой мошенник может узнать номер Вашей кредитной карты. Используйте веб-сайты, которые обеспечивают безопасность сделок. Также, ознакомьтесь с политикой конфиденциальности сайта.

- Безопасность должна быть многоуровневой. Установите и регулярно обновляйте программные продукты, обеспечивающие безопасность Вашего компьютера (antivirus, antispyware и antimalware).

Фишинг

Что такое фишинг?
Фишинг (от англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) – это вид интернет-мошенничества, основанный на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным - логинам и паролям. **Фишинг-атаки проводятся через электронную почту, всплывающие сообщения и ссылки на фишинговые веб-сайты, с целью обманным путем выявить у получателя личную информацию, часто финансового характера.**

Каким образом осуществляются фишинг-атаки?

Фишинг распространяется через интернет-мошенников посредством электронных писем или всплывающих сообщений, часто от имени представителя известного финансового учреждения. Большинство методов фишинга (известного также как бренд-спуфинг или кардинг) – сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций, с которыми Вы сотрудничаете (отделы кредитования, банки, государственные учреждения, платежные онлайн-системы).
Учтивые мошенники обращаются с просьбой сообщить обновленные данные, проверить или подтвердить информацию Вашего аккаунта, обычно мотивируя имеющимися проблемами. В письме часто содержится ссылка на фальшивый сайт, где пользователю предлагают ввести свои данные, которые сохраняются и используются в незаконных целях. Целью фишеров, как правило, являются представители различных компаний и клиенты банков, но в большей степени атакам подвергаются студенты и пенсионеры.

Как фишинг влияет на работу компьютера?

Кроме рисков получения большого количества спама, атаки фишеров не вредят работе компьютера. Однако, при краже личных данных этот вид мошенничества может привести к значительному ущербу. Заполучив единожды чью-либо личную информацию, мошенник сможет воспользоваться кредитом или совершить преступление от этого имени.

Как защитить себя от фишинга?

Возьмите себе за правила –

- Игнорируйте ссылки, получаемые со спамом, мгновенными сообщениями или в чате.
- Не открывайте вложения, отправленные с неизвестных Вам ресурсов.
- Не сообщайте свои пароли неизвестным людям.
- Не передавайте конфиденциальную информацию кому-либо по телефону, лично или посредством электронной почты, пока Вы не удостоверитесь, что это именно те люди, которые должны иметь доступ к данным.
- Проверяйте уровень конфиденциальности данных, установленный на сайте, перед тем, как отправлять на него свою личную информацию. Проверяйте URL сайта. В большинстве случаев фишинга адрес ресурса выглядит легальным, но URL или домен могут быть неправильными (.com вместо .gov, например).

- Установите и регулярно обновляйте фильтры электронной почты для уменьшения количества спама, антивирусные программы и брандмауэр. Регулярно обновляйте браузер и используйте патчи безопасности (security patches).

- Если Вы уверены, что подверглись фишинг-атаке, и Ваши конфиденциальные данные используются незаконно, свяжитесь с соответствующими организациями (банком, отделом кредитования или другим соответствующим органом) и предупредите о возможном мошенничестве.