Основы безопасности в Интернете

Пароли

Пароли являются основой любой политики безопасности, обычно пароль – это единственное, что отличает действительного пользователя от остальных. Он действует как паспорт и служит для того, чтобы пользователь доказал системе, что он действительно тот, за кого себя выдает. Если пароль выбран неудачно, злоумышленнику не обязательно владеть сложной техникой, чтобы **выдавать себя за настоящего пользователя** и попасть в систему.

Было опубликовано множество разных исследований на тему «Наиболее распространенные пароли», и большинство из них в десятке самых частых называет следующие:

- 123456
- password
- jesus
- love
- dragon
- qwerty
- monkey
- freedom
- iloveyou
- и др.

Эти пароли при автоматизированных атаках проверяют первыми, их в любом случае стоит избегать. Автоматизированная атака часто может вводить в систему тысячи паролей в минуту и способна испробовать множество слов, содержащихся в **словарях разных языков**. Базы данных слов и часто используемых паролей можно без проблем скачать из Интернета и автоматически их испробовать. Атакующие программы учитывают и различные комбинации слов, а также их **простые варианты** (слово, написанное задом наперед и т.д.), кроме того они проверяют и пароли, составленные из известных данных о пользователе (имя, фамилия, адрес электронной почты и т.д.).

При выборе пароля стоит придерживаться хотя бы основных правил качественного пароля, благодаря которым можно значительно снизить вероятность автоматизированного или целенаправленного раскрытия пароля:

1. Отсутствие какого бы то ни было пароля равняется открытому пути в нашу систему. Злоумышленники обычно в первую очередь нацеливаются на открытые счета.
2. Пароль, совпадающий с именем пользователя, также эффективен, как и отсутствие пароля. Словарный метод учитывает и этот вариант. Такие пароли **проверяются в первую очередь**. Также не рекомендуется использование в качестве пароля собственного адреса

электронной почты и других легкодоступных данных.
3. Тривиальные пароли, такие как aaa, abc, 12345, qwert и т.п., также абсолютно бесполезны. Их очень **просто угадать**, и при большом количестве пользователей очень легко найти кого-то, кто использует такой пароль.
4. Любое слово, содержащееся в словаре - это также очень неудачный пароль. А так как используемые словари очень обширны, нельзя полагаться даже на редко используемые слова.
5. Обычно для словарных атак используются словари в нескольких языковых версиях. Поэтому даже использование **иностранных слов** не является гарантией безопасности.

6. Не подходят для пароля и **легкодоступные сведения**, например, имя жены или шефа. При целенаправленной атаке их можно без труда получить и испробовать.
7. Объединение слов, их написание задом наперед или простые варианты слов для современной словарной программы не являются препятствием. Такие слова, как uoyevoli, mar1a, qwer123 не являются безопасными.
8. Имеет смысл сложить пароль из строчных и прописных букв и дополнить его **специальными знаками**, например, такими как: @#$%^*/-} и др.
9. Пароль, который вы где-то записали, не является безопасным. Никогда нельзя быть уверенным в том, что его никто не прочел. Например, известны случаи, когда люди писали PIN-код своей банковской карты прямо на карте, чтобы не забыть его. Это то же самое, что не иметь никакого пароля.
10. Каким бы удачным ни был пароль, он бесполезен, если его знает еще кто-нибудь, кроме пользователя, которому он принадлежит.

Для запоминания своего пароля можно использовать какую-нибудь игру слов, взять из каждого слова первую букву, а результат дополнить специальными знаками. Например:

I was father all my life
have no children have no wife.

IWFAML@hnchnw

Это удачный пароль, который никому не удастся угадать, и при этом вы его хорошо запомните. Но этот пароль ни в коем случае не используйте! Вы далеко не единственный, кто прочел этот документ.

Безопасный компьютер

Чтобы быть уверенным, что никто не получит доступа к вашим данным и паролю, необходимо обеспечить и безопасность своего компьютера. У злоумышленника есть несколько возможностей добраться до его содержания или до того, что вы пишете на клавиатуре. Существуют программные инструменты, которые следят за пользователем, и после введения пароля **отправляют его на специализированный сервер**. Речь может идти как о государственной шпионской программе, так и об обычных компьютерных вирусах.

Современные вирусы специализируются как раз на получении паролей не только от банковских счетов, но и от других систем, доступ к которым потом могут получить злоумышленники.

Еще одной возможностью являются программы-килоггеры (keylogger), представляющие собой небольшие устройства, подключаемые между клавиатурой и компьютером или прямо интегрированные в клавиатуру. Часто их обнаружение очень проблематично, а они постепенно записывают все, что пользователь набирает на компьютере, и высылают эту информацию своему первоначальному владельцу. К сожалению, эти устройства можно очень недорого купить в Интернете, а их подключение – вопрос нескольких секунд.

Еще одним устройством, часто становящимся инструментом злоупотребления, является веб-камера. С помощью программного обеспечения ее можно на расстоянии **включить и следить за пользователем**. Камеру сегодня имеет почти каждый ноутбук, она является частью многих настольных компьютеров дома и в интернет-кафе. В большинстве камер имеется светодиод, который показывает работу. Однако существуют способы включения камеры без зажигания этой лампочки. Поэтому камеру во время, когда она не используется, рекомендуется закрывать или отключать.

Основой охраны от подобных видов атак должна быть **актуализация** операционной системы и всех приложений (прежде всего браузера), актуализация **антивирусной программы** и включенный **межсетевой экран**. Актуализация системы и приложений исправляет пробелы в безопасности, через которые злоумышленники устанавливают свои коварные программы. Если речь идет об известном компьютерном вирусе, его поможет остановить антивирусное программное обеспечение. Против дистанционного злоупотребления сетевого подключения может помочь качественный межсетевой экран, который действует как фильтр и не пропускает коммуникацию, в которой пользователь не заинтересован и которая могла бы совершать различные виды атак на компьютер извне.

Из этой информации следует, что использовать чужой компьютер (например, в интернет-клубе) для совершения конфиденциальных действий всегда рискованно. Если есть хоть малейшая возможность, следует использовать свой компьютер, регулярно проверять его как программными инструментами, так и с технической стороны. При любой аномалии следует консультироваться с опытным техником.

Как безопасно работать на чужом компьютере

Существуют ситуации, когда у вас просто нет другой возможности, кроме как использовать чужой компьютер или компьютер в интернет-клубе. В таком случае никогда нельзя быть уверенным, что машина не заражена вирусом или что в ней нет другого программного обеспечения, которое следит за действиями пользователя. Речь может идти об умышленно установленном приложении или об обычном вирусе, который

попал в компьютер, потому что на нем работало слишком много пользователей (интернет-клуб), а обеспечение безопасности было недостаточным.

В такой ситуации помочь может только одно: запустить на этом компьютере собственную операционную систему, которая не имеет ничего общего с установленной на компьютере и не содержит ее коварные коды. Конечно же, такие действия возможны не везде, к тому же, они могут быть подозрительными сами по себе, но если есть хоть малейшая возможность, об этом следует подумать. Система, запущенная с вашего носителя, полностью находится под вашим контролем, вы можете совершить в ней необходимые операции, а потом вернуть все в изначальное состояние.

Существует целый ряд таких операционных систем, обычно они базируются на Linux. Конкретно можно порекомендовать испробовать дистрибутив Slax (www.slax.org), который можно записать на CD/DVD или установить на флеш-диск или внешний жесткий диск. После этого достаточно вставить/подключить носитель к компьютеру, перезагрузить его и на старте выбрать запуск системы с вашего носителя. Он запустит вам полноценную операционную систему, которая будет работать с вашего носителя и никак не будет связана с жестким диском компьютера. Кроме того, что эта система не может содержать никаких вирусов и вредоносного программного обеспечения, вы не оставите в изначальной операционной системе никаких следов своей работы. Как только вы завершите свои действия, следует выключить компьютер, отключить носитель и снова запустить компьютер в стандартном режиме.

Упомянутый Slax предлагает базовый набор приложений, таких как браузер, простой офисный пакет, мультимедийный проигрыватель, компрессионные утилиты, программы для скачивания и т.п. На домашней странице проекта можно скачать несколько сотен других приложений, которые можно или доустановить на время работы Slaxe или записать прямо на флеш-диск, где они будут сохранены.

Таким образом вы можете добавить на флеш-диск приложения, необходимые для шифрования с помощью ключа GPG, шифрования данных на жестком диске (TrueCrypt) или для подключения к сети TOR. Эти приложения будут описаны в этом документе ниже. Обратите внимание на то, что в систему Slax невозможно установить приложения, предназначенные для Windows. Программы можно найти на сайте www.slax.org.

Шифрование передаваемой информации

В обычных условиях большая часть данных перемещается по Интернету без какого-либо шифрования и проходит через множество различных узлов по всему миру. Во всех этих пунктах можно отслеживать данные и сохранять интересную или конфиденциальную информацию. Таким образом можно получить доступ не только к различным именам пользователей и паролям, но также и к передаваемой информации целиком, например, к электронным сообщениям, различным файлам, информации, передаваемой через программы мгновенного обмена сообщениями, такие как Live Messenger, ICQ и т.п.

Таким образом, следует заранее проверить, шифруется ли передача информации. Обычно это можно выяснить в справке к конкретным сетевым приложениям, эту информацию также можно найти в Интернете. В случае просмотра веб-сайтов ситуация довольно проста: на некоторых сайтах есть возможность включить шифрование. Включено ли шифрование, можно определить по адресу сайта. Если он начинается http://, шифрование не включено. Если изменить начало адреса на https:// ("s" в значении «secure»), шифрование активируется. Это можно узнать по иконке маленького замка рядом с адресом.

Однако не каждая служба предлагает шифрованную версию. Например, службы Google предоставляют возможность включить шифрование, таким образом, вы можете читать почту или пользоваться браузером с включенным шифрованием. В этом случае передаваемые данные сможете читать только вы и Google. Некоторые службы (например, банки и др.) шифрование даже требуют и без него невозможно получить доступ ни к какой информации.

Если шифрование уже включено, имеет смысл также проверить того, кто выдал «сертификат». Речь идет об организации, проверяющей, действительно ли просматриваемые сайты принадлежат тем, кому должны принадлежать. Если проверка не была произведена, за владельца сайта может выдавать себя кто угодно. Если у вас включено шифрование, кликните на иконку замка и посмотрите, кто выдал конкретный сертификат. К самым известным и надежным сервисам сертификатов относятся, например, Thawte и VeriSign. Если сайт предоставит вам их сертификат, вы можете быть уверены, что вводите свой пароль на действительном сайте, а не на фальшивой имитации, которая таким образом могла бы завладеть вашим паролем.

Шифрование данных на диске

В наше время большое количество пользователей использует ноутбуки или внешние жесткие диски с ценными данными. В случае кражи такого устройства существует риск кражи конфиденциальной информации, которая часто бывает более ценной, чем само устройство. Единственной охраной является шифрование данных на диске. Существуют инструменты, интегрированные прямо в операционные системы (Windows, Mac OS X и Linux), а также внешние инструменты. Преимуществом инструментов третьей стороны является то, что они универсальны и вы можете установить их одновременно в разных средах и операционных системах.

Из числа таких инструментов можно порекомендовать проверенный инструмент TrueCrypt. Он предлагается в бесплатном доступе, его можно скачать на сайте www.truecrypt.org. Когда вы установите этот инструмент в свою операционную систему, он предложит вам создать новый шифрованный диск. Можно зашифровать весь диск (включая операционную систему) или создать на внешнем носителе небольшую шифрованную зону. Чтобы получить доступ к своим данным, вам нужно будет вводить

пароль. Безопасность такого решения зависит только от силы выбранного пароля.

В случае более серьезных проблем TrueCrypt позволяет создавать так называемые скрытые зоны. Это шифрованные диски внутри шифрованных дисков. Таким образом, к одному хранилищу существует несколько паролей. Если вы будете вынуждены выдать пароль, вы можете сообщить только один из них. Злоумышленник в этом случае получит доступ только к фальшивой информации, которая должна быть настолько правдоподобной, чтобы он был удовлетворен и перестал требовать от вас другие пароли. Внутри зоны существует еще один скрытый диск, к которому вы получите доступ только после введения второго пароля. Если этот пароль вам неизвестен, нет никакой возможности получить эти данные и даже узнать о том, что они существуют.

Безопасность TrueCrypt была проверена многими экспертами и тестами, на это программное обеспечение можно на 100 процентов положиться и доверить ему свои данные. Однако следует обратить внимание на выбор качественного пароля.

Безопасная электронная почта

Электронная почта является службой, которая очень часто становится объектом атак спама или целенаправленных обманных электронных сообщений. Это одна из старейших служб в Интернете, и поэтому она не содержит никаких механизмов безопасности. Таким образом, очень просто сфальсифицировать адрес отправителя, изменить любое сообщение, которое передвигается по Интернету, и т.д. По причине цифрового характера принципа электронной почты такое изменение практически невозможно выявить, и поэтому злоумышленник может очень легко манипулировать своей жертвой.

Единственной охраной и здесь является шифрование, а также электронная подпись. Она дает получателю возможность убедиться, что сообщение действительно выслал данный отправитель и что сообщение не было изменено. Подпись прочно связана с содержанием сообщения и ее невозможно перенести в другое сообщение или изменить хоть одну букву в данном сообщении так, чтобы это не определило программное обеспечение получателя.

Существует несколько разных решений электронной подписи и шифрования электронных сообщений, чаще всего пользователи выбирают GPG или GnuPG. Речь идет о решении, совместимом с PGP, которое позволяет просто создать собственный сертификат подписи, получать и администрировать сертификаты остальных пользователей и контактировать с приложениями.

Процесс установки в Windows прост. Скачайте и установите GPG4Win (http://www.gpg4win.org/), речь идет о наборе приложений, необходимых для работы с GPG. С помощью программы GPA вы можете создать собственный сертификат и получить сертификат второй стороны. Чтобы кто-то другой мог получить ваш сертификат,

произведите его экспорт на сервер с ключами. Тогда любой пользователь сможет убедиться, что ваши сообщения подписаны правильной подписью, которая принадлежит вам. Данные, которые попадают на сервер и к остальным пользователям, совершенно невозможно использовать для поддельной подписи от вашего имени.

Если вы установили и подготовили ядро GPG указанным образом, используйте почтовый клиент Thunderbird, в который установите расширение Enigmail. Оно автоматически соединится с вашим GPG – и вы готовы шифровать или подписываться. Для подписи вам необходим только собственный ключ, который вы генерировали, для шифрования вам понадобятся и ключи вторых сторон, с которыми вы хотите контактировать. Если и остальные пользователи используют GPG, они могут принимать от вас шифрованные и/или подписанные сообщения. Вы можете передавать и строго засекреченные данные, доступ к которым получит только определенный вами пользователь.

Анонимный просмотр Интернета

Иногда необходимо просматривать веб-страницы так, чтобы их владелец не знал, кто их посещает. Каждый администратор сайта может видеть различную информацию о посетителях, например IP-адрес пользователя, приблизительное местонахождение пользователя (иногда на удивление точно), установленное программное обеспечение, версия операционной системы и другие данные. Также можно определить, какие сайты пользователь посетил ранее и т.д. Это информация, которую мы иногда хотим скрыть.

Одним из способов является использование так называемых анонимайзеров. Это веб-страницы, которые входят на нужный веб-сайт «за нас» и становятся нашими посредниками. Владелец сайта в таком случае видит информацию о данном анонимайзере, а не о нас. В Интернете существуют сотни анонимайзеров, испробовать можно, например, Anonymouse.org или ввести в Google ключевое слово "anonymizer" и найти другие. Потом на странице анонимайзера достаточно ввести адрес нужного компьютера в верную колонку и просматривать сайты, как обычно. Адрес в браузере при анонимном просмотре всегда должен начинаться с адреса анонимайзера.

Вторым и гораздо более изощренным способом является использование сети TOR. Речь идет о сети сотен серверов по всему миру, через которые вы можете осуществлять все свое общение с внешним миром. Передача данных несколько раз шифруется, и поэтому даже сами эти серверы не знают, кто с кем на самом деле контактирует. Таким образом, скрыто абсолютно все.

Для пользования сетью TOR нужно использовать браузер Firefox и необходимо установить единственное приложение Vidalia. Его можно найти по адресу https://www.torproject.org/projects/vidalia. После установки программы в вашей системе рядом с часами появится иконка луковицы. Когда вы на нее кликнете, появится простой интерфейс управления. В нем активируйте соединение с сетью TOR. Потом запустите Firefox, в котором также появится новая кнопка. С ее помощью вы можете легко включать

и отключать использование сети TOR.

Проверить ее работу очень просто: посетите страницу www.whatismyip.com и посмотрите, какой IP-адрес у вашего компьютера. Потом включите TOR и зайдите на страницу еще раз. Ваш IP-адрес должен измениться. Если вы через какое-то время снова зайдете на страницу, ваш IP-адрес снова будет другим. Это происходит потому, что TOR использует много различных серверов по всему миру и постоянно (каждые несколько минут) изменяет путь, по которому передается ваша информация. Поэтому отображается информация, что ваш компьютер находится то в Нидерландах, то во Франции, то в Канаде. Реальное местонахождение при включенном TOR никто не определит.

Это решение очень безопасно, существуют теоретические возможности атаки на сеть TOR, но ни одна из них на практике не была успешно испробована. Недостатком этого решения является то, что работа через сеть TOR значительно более медленная, чем без нее. В любом случае через TOR не рекомендуется, например, скачивать большие объемы данных. Речь идет о решении, предназначенном для просмотра веб-сайтов. Однако стоит обратить внимание на то, что вы можете выдать себя тем, что введете на каком-либо веб-сайте свои личные данные. При входе в Facebook будет отображаться, что ваш компьютер находится в Египте, но Facebook благодаря вашему входу будет знать, что это именно вы.

Рискованные приложения

Использование некоторых приложений несет с собой больше риска, чем обычно. Причиной может быть то, что они не уделяют должного внимания безопасности или содержат известные ошибки в безопасности. Таких приложений лучше избегать, потому что они ставят вас в опасное положение. Несколько таких приложений будут представлены ниже.

Internet Explorer на протяжении долгого времени относится к очень проблематичным приложениями, потому что содержит много серьезных ошибок в безопасности, которые к тому же на протяжении месяцев остаются незалатанными. Большое количество злоумышленников направляет свое внимание именно на эти проблемы, и в случае умелого использования пробелов в безопасности часто достаточно только посетить зараженный веб-сайт.
Решение: используйте другой браузер, например, Firefox или Chrome.

Flash Player является частью большинства компьютеров, потому что пользователи используют его для интернет-игр и просмотра видео с YouTube и других серверов. К сожалению, и Flash Player известен своей «дырявостью», однако альтернативы ему не существует.
Решение: проверяйте актуальность своего Flash Player (http://tiny.cc/tn0u4) и используйте расширение FlashBlock, которое позволяет запуск Flash только на избранных веб-сайтах.

Skype – это очень распространенная коммуникационная программа для передачи видео и голоса через Интернет. Его создатели утверждают, что приложение использует шифрование, это подтверждают и эксперты по безопасности. Однако некоторые страны уже подтвердили, что заключили с владельцем сети Skype соглашение о предоставлении доступа к избранным разговорам. Среди этих стран Китай, США и Австрия. Однако не исключено (и даже очень вероятно), что их намного больше.
Решение: не передавайте по Skype конфиденциальную информацию, используйте альтернативу, например, GTalk.

Adobe Reader – это популярная программа для чтения файлов PDF. Она, к сожалению, также является причиной многих проблем с безопасностью, прежде всего потому, что способна интегрировать в браузер, и таким образом опасные PDF, злоупотребляющие пробелами в безопасности, могут стать частью веб-страницы.
Решение: установить альтернативу, например, Evince, Foxit Reader или PDF-XChange Viever

В любом случае должно действовать правило, что следует устанавливать только проверенные приложения и регулярно их актуализировать.

Форматы, используемые для обмена данными

Очень часто пользователям нужно передавать по Интернету конфиденциальные документы, действительный создатель которых должен быть скрыт. В этом случае ключевым является выбор формата, потому что некоторые форматы переносят и скрытую информацию, такую как имя создателя, установки его компьютера и т.п. Если вы хотите скрыть эти данные, следует выбрать формат, который их не передает. Очень неудачным выбором в таких случаях являются **форматы .doc, .xls и т.п.**, которые, к сожалению, очень широко распространены. Они сохраняют много деталей о пользователе. К тому же, в файлах часто появляются и **фрагменты совершенно других документов**, над которыми пользователь работал ранее! Причина этого в том, что Word, пытаясь ускорить свою работу, сохраняет в документ часть своей рабочей памяти в том состоянии, в котором она на данный момент находится. К сожалению, в этой памяти обычно находятся и большие отрезки уже закрытых документов.

Если вы хотите быть уверены, что эти данные не попадут в сохраняемый файл, всегда отправляйте конфиденциальную информацию в **файлах PDF**. Самым простым путем к их созданию является установка так называемого виртуального принтера, который предлагается, например, программой doPDF. После установки в вашей системе появится новый принтер. Если вы «распечатаете» на нем какой-либо документ, вместо действительной печати откроется указанная программа и спросит вас, как и где вы хотите создать PDF. При этом способе коммуникации (из приложения, которое выводит на печать) действительно передаются только изображения – то есть то, что появится на бумаге. Никакие другие данные в PDF не передаются.