Пароль как основа информационной безопасности

Пароль — это единственное, что защищает Вашу учетную запись от доступа к ней злоумышленника, а Ваша почта или аккаунты в социальных сетях принадлежат только Вам исключительно потому, что защищены надежным паролем.

Составляя пароль используйте комбинации букв, цифр, специальных символов, неочевидные ассоциации и сочетания различных элементов. Имя или номер телефона — не лучший выбор. Правильно оценивайте сложность пароля перед началом использования:

- совсем слабый пароль: общеизвестные аббревиатуры, названия, общеупотребительные фразы и слова (qwerty, admin, pass123, password, root; 4% пользователей используют пароли из первой десятки популярных, а три самых популярных пароля держат лидерство годами);
- плохой пароль, который кажется сложным: дата вашего рождения или рождения кого-то из близких, номер какого-то из ваших документов, кличка вашего домашнего питомца, инверсия в раскладке простого слова, особенно, вашего имени, замена пары букв цифрами в применимом к Вам слове;
- сложный пароль: имеет не очевидную и не сводимую к одному слову основу для запоминания с обязательным использованием цифр, букв (со сменой регистра клавиатуры) и специальных символов.

Запомнить сложные пароли порой затруднительно по этой причине их приходится записывать, однако делать это нужно соблюдая следующие рекомендации:

- записывайте пароль отдельно от логина или имени пользователя;
- записывайте его не полностью, а лишь частично или разделите пароль на части и поменяйте их местами;
- записывая пароль, зашифруйте его часть или добавьте заведомо для вас лишние символы.

Использовать один пароль для доступа к разным аккаунтам не рекомендуется так как каждый интернет-ресурс использует свои системы защиты и хранения паролей, которые не всегда могут быть реализованы на высоком уровне. Согласно статистике, около 14% пользователей используют один и тот же пароль для авторизации на всех аккаунтах и получив доступ к одному, злоумышленник непременно получит доступ и к другим.

Очень часто, злоумышленники даже не пытаются взломать пароль, а просто стараются его узнать под тем или иным предлогом. Они массово рассылают письма и сообщения с призывом поучаствовать в

беспроигрышной акции, проводимой крупной торговой сетью или финансовой организацией, при этом злоумышленники стараются оставить на раздумья как можно меньше времени, чтобы подтолкнуть пользователя на принятие решения немедленно, под влиянием эмоций. Зачастую, для участия в таких «акциях» требуется предоставить имя пользователя и/или пароль от какого-либо аккаунта или сведения о банковской платежной карте. Использование эффекта внезапности излюбленный прием злоумышленников: так, обнаруженное в электронном почтовом ящике письмо о якобы заблокированном аккаунте в социальной сети, очень часто толкает пользователей на переход по прикрепленной ссылке, которая в свою очередь ведет на поддельную страницу (очень похожую на настоящую), где для отмены блокировки необходимо вести свои данные. После ввода вся информация попадает в руки злоумышленников.

В качестве дополнительного способа защиты своей информации, рекомендуется также использовать двухфакторную систему идентификации, при которой специально сгенерированное SMS-подтверждение будет поступать на указанный пользователем абонентский номер телефона при каждой попытке входа в аккаунт с нового устройства. При использовании данной системы, злоумышленник не сможет осуществить доступ к аккаунту даже зная пароль.

Безопасное использование сети Интернет

Посещение сайтов стало настолько привычным, что мы не задумываемся об опасностях, которые может скрывать любая страница в Интернете. Сайт — это программа, неявным для вас образом взаимодействующая с вашим браузером и операционной системой и конечные цели такой программы могут быть совершенно разными.

Основная опасность бездумного серфинга в том, что вредоносное ПО может быть размещено на любом сайте и перейдя по непроверенной ссылке мы незаметно загрузим его на свой компьютер. Ссылка может быть замаскирована под заманчивое предложение скидки, интересный видеоролик, скандальные факты о знаменитостях и т.д. Сайт, который на первый взгляд кажется вам знакомым и проверенным, может быть взломан или подделан злоумышленниками.

Таким образом вас всегда должно насторожить если:

- при загрузке из Интернета музыку или видео, сайт предлагает установить проигрыватель;
- осуществляя покупки в интернет-магазине, сайт предлагает установить специальное приложение;

- попав на сайт вы заметили, что на странице неестественно много ярких кнопок и ссылок со словом «скачать», «загрузить» и «установить»;
- установленный антивирус информирует о том, что сайт является мошенническим.

Чтобы не допустить ущерба вашей информации и компьютеру, необходимо соблюдать следующие правила:

- не нажимайте кнопки «Скачать» на любых сайтах, кроме сайтов производителей программного обеспечения или официальных поставщиков нужных вам материалов;
- не загружайте ничего с сайтов, вид которых вас настораживает обилием всплывающих окон или множеством рекламных объявлений;
- если вам необходимо установить какую-либо программу, загружайте ее только с сайта разработчика или в надежном интернет-магазине;
- проверяйте любой загруженный файл антивирусом;
- обращайте внимание на расширение загружаемых файлов и соответствие их стандартному для такого рода файлов;
- не запускайте и не открывайте подозрительные файлы, которые неожиданно загрузились на ваш компьютер
- доверяйте рекомендации антивируса, если он считает сайт подозрительным.

Еще одним важным аспектом на пути обеспечения личной информационной безопасности является регулярной обновление операционной системы. Вместе с тем обновлять ПО стоит исключительно на официальных сайтах, ведь установка вредоносных программ, замаскированная под обновление ПО — излюбленный трюк злоумышленников, поэтому очень часто на мошеннических сайтах предлагают обновить версию вашего браузера или Flash Player, а также обновить или установить бесплатную версию антивируса.

Для того, чтобы удостовериться, что предложение об обновлении прислано самой программой, полностью закройте интернет-браузер и если просьба об обновлении исходит от одной из программ, установленных в вашей системе, то всплывающее окно не исчезнет после закрытия сайта. Кроме этого можно посетить официальный сайт программы и проверить наличие свежих обновлений.

Загружая что-либо из Интернета, обращайте внимание на мелкие подписи к ссылкам для загрузки, на дополнительные предложения (от таких предложений можно отказаться без ущерба для устанавливаемой программе, просто «снимайте» все ненужные галочки). Если что-то начало устанавливаться и вызвало у Вас подозрение, смело отменяйте установку.

Даже если вы загружаете что-либо с известного вам сайта, всегда нужно проверять такой файл антивирусом перед его первым открытием или установкой.

Точно также, как и на персональном компьютере, при работе с мобильными устройствами стоит опасаться вредоносного программного обеспечения. Существует два основных класса такого вредоносного ПО, опасного для обычных пользователей:

- программы для перехвата информации, основная задача которых перехват паролей, данных для онлайн-банкинга, банковских SMS;
- программы-блокировщики экрана, которые выводят на экран свое сообщение, не позволяя пользоваться устройством и требуя перечисления денег за разблокировку.

Вредоносная программа может попасть на устройство разными способами:

- Вы получили SMS с подозрительной ссылкой, нажали на нее и перешли на сайт;
- Вы нажали на подозрительную ссылку в браузере — нечаянно или думая, что переходите в какое-то интересное вам место;
- Вы самостоятельно запустили установочный файл .apk на своем Android-устройстве, загрузив его на телефон с компьютера;
- Вы загрузили файл неизвестного производителя, полагая, что устанавливаете нужное приложение;
- Вы активировали анонимный QR-код.

Вас должны настораживать любые неожиданные предложения перейти по ссылке, если вы не полностью уверены в том, что увидите после перехода на сайт. Это может быть:

- ссылка на MMS в SMS;
- непрошеная реклама нового приложения;
- QR-код, кнопка загрузки, замаскированная под интересный текст или красивую картинку, или призыв посмотреть веселый видеоролик.

Принцип действия антивируса на мобильных устройствах совершенно такой же, как и на компьютерах: фильтрация входящих файлов. В этой связи важно обращать внимание на то, что загружается на устройство и всегда помнить, что программы, загруженные с любых сторонних сайтов, проверенных или нет, могут быть заражены вредоносным ПО.

С целью обеспечения личной информационной безопасности и повышения уровня защищенности своих данных помните, что:

- установка «пиратских» приложений может повлечь за собой самые неприятные последствия;

- следует устанавливать только приложения, приобретенные или бесплатно загруженные в официальных магазинах;
- если вы не хотите платить за приложение, воздержитесь от загрузки пиратской версии и найдите бесплатный аналог;
- даже при загрузке приложений из официальных магазинов предварительно их следует проверять антивирусом.

Официальные магазины приложений — вполне безопасное место для поиска и установки необходимого ПО. В официальных магазинах всегда можно посмотреть рейтинг приложения, количество загрузок, а также почитать отзывы, чтобы получить представление о том, что вы собираетесь загрузить и не мошенническое ли это приложение.

Безопасное использование социальных сетей и мессенджеров

Социальные сети занимают в нашей жизни все больше места. Мошенники охотно и умело пользуются социальными сетями. Они используют любую лазейку, чтобы добраться до чужих денег и данных, которые тоже стоят денег.

Злоумышленники часто используют социальные сети:

- для выманивания денег через взломанные аккаунты людей из вашего списка контактов;
- для рассылки спама;
- для получения доступа к другим ресурсам, связанным с социальной сетью;
- для получения доступа к данным, которые могут пригодиться для шантажа.

При наличии полного доступа к вашей странице кто угодно может действовать от вашего имени: рассылать вашим друзьям фишинговые ссылки и сомнительные рекламные сообщения или просить денег взаймы.

На все просьбы сообщить пароль — друзьям, знакомым, самым близким людям — вы должны ответить отказом. В этой связи игнорируйте письма и сообщения, в которых запрашивают ваш пароль так как это всегда письма от мошенников.

Никогда не публикуйте в Интернете, не храните в почте или в социальных сетях копии ваших документов, в том числе фотографии паспорта и банковской карты. Если какой-то сайт требует для регистрации копию вашего паспорта, постарайтесь оценить возможные риски.

Если Вы подозреваете, что кто-то получил доступ к вашему аккаунту в социальной сети, немедленно смените пароль, при этом убедившись, что аккаунт все еще «привязан» к Вашему абонентскому номеру телефона и

электронной почте. При «взломе» важно обезопасить ценные личные данные и список контактов, к которым теперь есть доступ не только у вас, поэтому чем скорее вы восстановите доступ к аккаунту и защитите его надежным паролем, тем меньше ущерба успеют причинить злоумышленники. Если вы использовали пароль от этого аккаунта где-то еще, эти страницы/ресурсы/аккаунты тоже окажутся под угрозой в случае наличия хоть какого-либо упоминания о них в скомпрометированном аккаунте.

Злоумышленники могут действовать хитро и долгое время не выдавать себя — не делать массовых рассылок и ничего не удалять. Вас должны настораживать самые малейшие признаки чужого присутствия. Если вы подозреваете, что кто-то завладел вашим аккаунтом в популярной сети «ВКонтакте», первым делом откройте меню настройки безопасности и перейдите на вкладку «Последняя активность», где отображаются сведения о последних успешных входах в Ваш аккаунт.

Используя браузер для входа в социальные сети всегда стоит соблюдать простейшие правила:

- вводите пароль от социальной сети только на сайте или в официальном клиентском приложении самой социальной сети;
- благонадежные сайты никогда не попросят вас ввести имя пользователя и пароль от социальной сети, с помощью которой вы авторизуетесь на этих сайтах.

Вас всегда должны настораживать:

- предложения ввести имя пользователя и пароль от социальной сети на сайте, который Вы посещаете впервые и функциональные особенности которого по своей сути никак не должны быть связаны с персональными данными пользователей социальной сети;
- предложения обновить данные аккаунта в социальной сети, которые присылают вам по электронной почте, особенно если они содержат форму ввода имени пользователя и пароля;
- всплывающие окна, похожие на форму ввода имени пользователя и пароля от социальной сети.

Если вас автоматически перенаправили на сайт авторизации в социальной сети, проверьте, действительно ли он настоящий. Посмотрите на адресную строку: там должен быть настоящий адрес социальной сети.

Звонок от «представителя» банка с просьбой срочно предоставить необходимую информацию

Преступники сообщают, что необходимо осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. Только за последние две недели в правоохранительных органах области зарегистрировано более 70 подобных фактов. Следует отметить, что преступники используют современные возможности сети Интернет и в частности возможность «подмены номера», как следствие у потерпевшего на экране мобильного телефона может отображаться совершенно любой абонентский номер телефона, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным.

Следует обращать внимание на то, что сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен.

Если Вам поступил такой звонок, то:

- ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме. В случае если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и Банк это заметит, то его сотрудники сперва инициативно заблокируют Вашу банковскую платежную карту, после чего сообщат Вам причину принятого решения (ничего не уточняя) и пригласят в свое учреждения с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;
- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы. Скорее всего собеседник сообщит, что Вам вообще не звонил. Современные технологии позволяют подменить номер на экране Вашего телефона на совершенно любой, в том числе заменить его для примера названием учреждения банка;
- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то

оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения. Даже в этом случае не сообщайте никакой информации собеседнику;

- сами перезвоните в свой банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся. Скорее всего специалист сообщит Вам, что никаких несанкционированных операций зафиксировано не было, а сотрудник Банка Вам не звонил.

Если же Вы сообщили кому-либо информацию о своей банковской платежной карте, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта. Помните, что если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства.

Звонок или переписка в мессенджере по поводу приобретения продаваемого Вами в сети Интернет товара

При этом преступник предлагает перевести предоплату на Вашу карту, реквизиты которой просит ему предоставить. Важно помнить, что для совершения перевода нужны данные лишь лицевой стороны, а если поступают просьбы предоставить еще и код, нанесенный с оборотной стороны или содержание смс-сообщений, которые как раз начинают поступать из банка – то это наверняка злоумышленник, пытающийся похитить деньги. Наиболее оптимальным способом обезопасить себя будет открытие дополнительной банковской карты, которая будет предназначена лишь для совершения оплат в сети Интернет и на которой не будут хранится денежные средства. В настоящее время многие банки предоставляют возможность оформления даже виртуальных карт совершенно бесплатно.

Нередко злоумышленники для получения информации о банковской платежной карте жертвы, предлагает якобы получить денежный перевод для чего присылает ссылку на некий интернет-ресурс. Стоит быть очень внимательным, так как содержательная часть такой ссылки может частично состоять из названия банковского учреждения, но отличие даже в один незаметный символ приведет Вас по совершенно иному адресу в сети Интернет. Если Вы заметили, что в представленной ссылке помимо

названия финансового учреждения присутствуют и иные названия (пусть даже знакомые), символы или знаки, не переходите по ней ни под каким предлогом. Если у Вас в мобильном устройстве или на персональном компьютере сохранены какие-либо конфиденциальные данные (в том числе логин и пароль для доступа к интернет-банкингу), при переходе по такой ссылке, злоумышленник может иметь возможность заполучить их из памяти устройства. Если Вы все же перешли по подобной ссылке и видите уведомление о том, что в системе имеется денежный перевод и для его получения необходимо ввести данные банковской платежной карты, ни при каких обстоятельствах не вводите запрашиваемые сведения, так как это прямой путь к утрате собственных средств. Внешний вид открывшегося интернет-сайта может быть очень похож на официальный раздел сайта банковского учреждения, но в адресной строке будет указан совершенно иной, отличный от настоящего, адрес (он может быть похож и иметь лишь незначительные отличия). Кроме этого, стоит попытаться перейти в какие-либо иные разделы, ссылки на которые отображены на открывшейся странице. Зачастую злоумышленники создают простые сайты, которые состоят лишь из одной страницы и все иные разделы (новости, курсы валют, контакты и т.д.) являются недоступными для пользователей. Если хоть что-либо насторожило Вас, немедленно покиньте такой интернет-ресурс и не поддавайтесь на уговоры или угрозы злоумышленника.

Угрозы, связанные с использованием социальных сетей

В настоящее время злоумышленники активно используют возможности виртуального общения для совершения преступлений. Одной из наиболее распространенных проблем, позволяющей злоумышленникам совершать противоправные действия, является несанкционированный доступ к персональным аккаунтам пользователей в сети Интернет. После совершения несанкционированного доступа к персональным аккаунтам зачастую развиваются следующие сценарии:

- злоумышленник, рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты, при этом, хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу» очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше,

чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон). Анализ показывает, что не более 20% людей, получивших такие сообщения, связываются с владельцем страницы, что в этой ситуации крайне важно. Чтобы обезопасить себя от этого вида преступлений, не стоит сообщать никому реквизиты доступной банковской платежной карты или номер мобильного телефона и содержание смс-сообщений, поступающих для подтверждения совершения операции.

- злоумышленник изучает содержание переписок потерпевшего и использует их содержание в качестве инструмента для вымогательства денежных средств. Таким образом, инструментом вымогательства становятся личные диалоги на откровенные темы, фотографии, содержащиеся на странице и в диалогах и иные очень личные данные. Обычно, перед тем как связаться с потерпевшим, преступник делает скриншот списка всех его друзей и близких. Избежать подобного возможно лишь путем регулярной чистки своих диалогов и удаления из сети всей информации компрометирующего характера.

- злоумышленник начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям, ссылки на поддельные ресурсы банковских учреждений, а также вредоносное программное обеспечение, что также может привести к серьезным последствиям.

В случае обнаружения «взлома» аккаунта, прежде всего, следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого следует оповестить друзей и знакомых об инциденте, используя при этом иные социальные сети и мессенджеры. Кроме этого, чтобы в какой-то мере обезопасить себя от взлома, специалисты по безопасности рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты, при этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который будет выслан на указанный при регистрации страницы номер.

Очень часто злоумышленники не пытаются получить доступ к чужому аккаунту, а просто копируют содержащиеся в нем фотографии и вставляют их в новый, заранее созданный. При этом в таком фальшивом аккаунте злоумышленник меняют сведения об имени и фамилии на те, которые указаны у пользователя, копию страницы которого он создает. После

создания такого дубликата, злоумышленник начинает рассылать всем знакомым пользователя сообщения с предложением поучаствовать в какой-нибудь беспроигрышной акции или получить какие-либо материальные вознаграждения, однако для всего этого необходимы сведения о банковской платежной карте. Для того, чтобы не стать жертвой злоумышленника в данном случае, при получении подобного сообщения стоит:

- обратить внимание имеется ли с этим пользователем более ранние диалоги. Если это сообщение действительно поступило со страницы знакомого, который ранее поздравлял Вас с праздниками или что-либо обсуждал в переписке, то эти сообщения тоже должны быть видны;
- перейти на страницу пользователя, который прислал Вам это сообщение и изучить содержащуюся в ней информацию. Зачастую злоумышленники не наполняют такие страницы какой-либо информацией, а просто копируют несколько фотографий или добавляют пару свежих новостных ссылок;
- в любом случае необходимо связаться с пользователем от имени которого поступило подобное сообщение, не используя при этом страницы в социальных сетях (лучше всего по телефону). Зачастую, в ходе такого разговора пользователь сообщает, что никакого сообщения он не присылал, а от его имени действовал кто-то другой.

Блокировщики операционной системы

Очень часто, осуществляя поиск актуальной информации в сети Интернет пользователи попадают в неприятную ситуацию, когда на экране их устройства появляется информация о наложении правоохранительными органами штрафа якобы за просмотр или распространение порнографических материалов и т.п. в результате чего устройство принудительно заблокировано. При этом указанная информация полностью заполняет экран и привычным способом пользователь не может ее закрыть. За «разблокировку» устройства необходимо уплатить какую-либо сумму денежных средств, перечисли их на абонентский номер телефона или положив на электронный кошелек. Расчет злоумышленников в том, что человек растеряется и перечислит денежные средства, так как эмблемы и названия правоохранительных органов, ссылки на какие-то статьи, указанные временные ограничения и обвинение в некорректном поведении зачастую приводят пользователя в стрессовое состояние. Стоит запомнить, что правоохранительные органы не «собирают» штрафы на электронные кошельки и номера телефонов. В подавляющем большинстве таких случаев, пользователь сталкивается или с вредоносным программным обеспечением,

которое было установлено на его устройство или перешел по интернет-ссылке, имеющей специфические настройки, не позволяющие закрыть ее привычным образом. Для того, чтобы попытаться восстановить работоспособность своего устройства, следует прежде всего полностью ненадолго отключить его от электросети. При повторном включении, в случае если информационное сообщение вновь отобразилось на экране, следует одновременно нажать комбинацию трех клавиш «Ctrl+Alt+Delete» и открыть «Диспетчер задач». В открывшемся окне следует выбрать интернет-браузер, который в настоящее время запущен и используется Вами, после чего необходимо нажать на клавишу «Снять задачу». После проведения указанных действий работоспособность устройства зачастую восстанавливается, но при повторном подключении к сети Интернет, интернет-браузер может сообщить, что предыдущая сессия была завершена некорректно и предложит ее восстановить. С этим предложением соглашаться не стоит так как восстановление прошлой сессии работы приведет к открытию в том числе блокирующей интернет-ссылки.

Установка «фальшивых» приложений и приложений с пробным периодом использования

Устанавливая любое приложение очень важно обращать внимание на разрешения — действия, которые приложение сможет выполнять после установки. Всегда стоит задуматься об установке приложения если Вы даете ему разрешение на отправку смс-сообщений или осуществление звонков, а также на доступ к персональной и финансовой информации, а права администратора обычным приложениям вообще не нужны. Если вы загружаете приложение из официального магазина, про все разрешения можно прочитать подробнее, нажав на галочку около каждого пункта. Кроме этого, устанавливая якобы бесплатное приложение всегда обращайте внимание на наличие платной подписки. Очень часто пользователь бесплатно устанавливает приложение, которое на самом деле является бесплатным лишь в течении пробного периода его использования и в том случае если пользователь не отменит подписку, она ежемесячно будет автоматически продлеваться, при этом со счета банковской платёжной карты, привязанной к аккаунту, будут списываться денежные средства. Для того, чтобы избежать подобных неприятностей, необходимо внимательно изучать свойства устанавливаемого приложения, а в случае наличия желания прекратить его использование, стоит не просто его удалить, но и осуществить отмену подписки на соответствующем ресурсе.

Безопасное использование электронной почты

Ежедневно мы получаем значительное число электронной корреспонденции: это могут быть информационные сообщения, различного рода уведомления и предложения, а также личная почта. Мы не задумываясь переходим по прикрепленным ссылкам в письмах, загружаем файлы и фотографии, пересылаем необходимые данные. В ежедневном потоке сообщений злоумышленникам не составляет никакого труда спрятать письма, реальная цель которых не сообщить значимую информацию, а добыть ее у пользователя или вынудить совершить какие-либо действия.

Первым шагом на пути повышения уровня безопасности при работе со своей электронной почтой является использование надежного пароля, известного только вам. Вводить логин и пароль от электронной почты в достаточной мере безопасно лишь на официальном сайте почтового сервиса или в почтовой программе. Обращайте внимание непосредственно на адрес страницы, где предлагается ввести реквизиты для доступа, так как внешний вид ресурса можно подделать и единственным способом в этом удостоверится, является правильность написания адреса почтового сервиса. Если данные будут введены на небезопасном сайте, то с высокой долей вероятности ими воспользуются злоумышленники.

Используя электронную почту всегда должны настораживать:

- любые требования и просьбы сообщить пароль или иные персональные данные, поступившем даже от знакомого лица или якобы от представителя службы безопасности;
- любые письма с требованиями ввести или отправить свой пароль от онлайн-банка или реквизиты банковской платежной карты. Этими сведениями должен владеть только держатель карты и даже сотруднику банка их сообщать не стоит;
- всплывающие окна в том числе с предложениями поучаствовать в беспроигрышных акциях, а также письма с неоправданными пометками «Срочно!» и невнятно сформулированной темой письма. Помните: чем соблазнительнее предложение, тем выше вероятность того, что оно мошенническое.

Немаловажное значение в обеспечении безопасного использования электронной почты является внимательное отношение к содержимому входящей корреспонденции. Прикрепленные файлы обычно воспринимаются как рабочий инструмент и подозрения не вызывают. Вследствие чего на расширение файла внимание обращается в последнюю

очередь (расширение объясняет системе, какие действия необходимо выполнить с этим файлом):
*.doc - документ Word;
*.bat - пакетный файл, содержащий последовательность исполняемых команд;
*.exe - исполняемый файл, запускающий определенную программу;
*.vbs - сценарий, написанный на языке Visual Basic, также используется для выполнения команд и программ в Windows;
*.js - JavaScript; открывая такой файл, запускается определенная последовательность действий;
*.scr - файлы с этим расширением используются в системе Windows как заставка экрана.

Файл, открытый (запущенный) или загруженный из ненадежного источника может запустить на компьютере определенные действия, направленные на получения конфиденциальной пользовательской информации, использования ресурсов компьютера для совершения противоправной деятельности, а также на причинение вреда самому пользователю, в том числе путем шифрования данных на его компьютере. Стоит запомнить, что открытие любых исполняемых (запускающих выполнение определенных процессов) файлов, полученных по электронной почте – это всегда риск и перед его открытием стоит как минимум проверить его расширение. Файлы с расширениями .exe, .js, .vbs, .scr и т. д., а также с двойными расширениями .txt.exe, .pdf.scr, .doc.js, mp3.vbs, .jpg.exe потенциально угрожают вашей информационной безопасности. Любые файлы с неизвестными и непонятными расширениями должны вызывать опасение и их необходимо проверять антивирусом, предварительно сохранив файл на диск, не открывая его.

Не стоит забывать, что в настоящее время вредоносное ПО может быть прикреплено к какому-либо файлу, который не вызывает каких-либо подозрений. Так, имеющиеся уязвимость MS Office приводит к тому, что источником вредоносного программного обеспечения может стать на вид совершенно невинный файл Word или Excel. Механика Office использует внутренние действующие механизмы — макросы. Самый обычный файл документа может нести в себе набор макросов, не регистрируемых защитой как самостоятельные исполняемые файлы — и этой лазейкой пользуются некоторые разработчики вредоносного ПО. Файл с макросом может сам по себе не наносить никакого вреда, но создавать в системе внутреннюю «отмычку», открывая доступ извне для злоумышленника. Опасность использования макросов была выявлена более десяти лет назад, и в

большинстве версий Windows их запуск по умолчанию заблокирован. В этом случае задача злоумышленника — уговорить вас разблокировать возможность запуска макросов.

Чем ценнее данные на вашем устройстве, тем внимательнее вы должны относиться к тому, что на него загружаете.

Для того, чтобы обезопасить себя и свою электронную почту рекомендуется:

- использовать сложные пароли, состоящие из букв, цифр и специальных символов, никому и ни под каким предлогом его не сообщая;
- обращать внимание на адрес ресурса на котором находитесь. Перейдя по подозрительной ссылке рекомендуется не вводить свою конфиденциальную информацию и не загружать какие-либо файлы;
- не хранить в электронной переписке сведения о банковской платежной карте;
- не открывать и не запускать подозрительные файлы с неизвестными расширениями, а также исполняемые файлы с расширениями .exe, .vbs, .js, .scr и т.д;
- использовать двухфакторную систему идентификации, привязав электронную почту к абонентскому номеру телефона. При ее использовании, авторизация с использованием нового устройства будет невозможна без введения кода, поступающего в смс-сообщении.

Кроме этого, в период повсеместного использования электронной почты для ведения деловой переписки стали активно использоваться такие схемы мошеннического завладения средствами предприятий как подмена адреса отправителя электронного письма. Современные почтовые сервисы при отправке электронной корреспонденции позволяют изменить адрес отправителя на совершенно любой. Таким образом получатель письма видит поступление корреспонденции с известного ему адреса электронной почты, хотя на самом деле письмо отправлено совершенно иным отправителем.

На примере это выглядит следующим образом: компания «А» активно сотрудничает с компанией «Б» и регулярно обменивается с ней электронной корреспонденцией. Для этих целей у компании «А» есть электронная почта «А@gmail.com», а у компании «Б» - «Б@gmail.com». Злоумышленники, зная о наличии коммерческих отношений между компаниями, в почтовой программе составил электронное письмо о том, что у компании «Б» якобы изменились реквизиты для оплаты и прикрепил к письму информацию о новом расчетном счете. Данное письмо злоумышленник направил в адрес компании «А», но при отправке осуществил подмену своего реального

адреса отправителя с «В@gmail.com» на «Б@gmail.com». Таким образом бухгалтер компании «А», получив указанное письмо, посчитал, что расчетный счет компании действительно изменился и не перепроверив данную информацию очередной платеж произвел в адрес счета, указанного злоумышленником.

Стоит отметить, что в ряде случаев злоумышленники ведут длительную переписку с потенциальными жертвами, пользуясь тем, что получатели таких писем (писем с подменным адресом отправителя) нажимают в поступившем письме на кнопку «ответить», а не формируют новое письмо, вводя адрес получателя письма вручную. При нажатии на кнопку «ответить» ответное письмо направляется именно на тот адрес электронной почты, с которого оно направлялось в действительности, т.е. на электронную почту злоумышленника, хотя в графе «получатель» будет стоять совершенно другой адрес.

Для того, чтобы избежать негативных финансовых последствий, необходимо очень внимательно относится к письмам о внезапной смене реквизитов для оплаты. Такую информацию в обязательном порядке необходимо дополнительно перепроверять путем непосредственного общения со знакомыми представителями компании, от имени которой поступило подобное письмо. При этом использовать электронную почту для уточнения данных обстоятельств нежелательно.

Правила обеспечения информационной безопасности

По причине некорректного обращения с поступающей электронной корреспонденцией на территории страны широкое распространение получил такой способ хищения денежных средств со счетов предприятий всех форм собственности, при котором по каналам электронной почты, под видом уведомлений о просрочке платежей или иных документов, распространялось вредоносное программное обеспечение. Указанное программное обеспечение под видом обновления операционной системы осуществляло сбор необходимой конфиденциальной информации (логины и пароль для доступа к системе дистанционного банковского обслуживания, информация об электронной цифровой подписи предприятия и т.д.), с целью дальнейшего генерирования платежного поручения и перевода денежных средств со счетов предприятия.

Совершение преступлений стало возможным по причине допущенных нарушений в обеспечении информационной безопасности предприятий и пренебрежительного отношения со стороны сотрудников к соблюдению следующих правил безопасного использования сети Интернет:

- персональный компьютер с использованием которого осуществляется работа с системой клиент-банк предприятия, не следует подключать к локальной сети предприятия, а также использовать для обработки входящей корреспонденции по каналам электронной почты;
- USB-ключ с электронной цифровой подписью следует подключать к персональному компьютеру только непосредственно при проведении необходимых финансовых операций;
- при обработке входящей корреспонденции, поступающей по каналам электронной почты следует обращать внимание на прикрепленные к письмам файлы и не допускать их открытия (запуска) непосредственно из почтовой программы. Целесообразно сохранить вложение (не запуская его) и проверить его на наличие вредоносного программного обеспечения. Наличие у поступивших вложений двойного расширения или автоматическое его скрытие может свидетельствовать о прикреплении к файлу вредоносного программного обеспечения;
- на персональный компьютер, используемый для работы с системой клиент-банк, а также на компьютеры, подключенные к нему по локальной сети, следует установить лицензионное антивирусное программное обеспечение и произвести его верные настройки. Компьютер, на котором осуществляется обработка входящей электронной корреспонденции следует дополнительно оснастить антивирусным программным обеспечением, отвечающим за защиту почтовых сервисов и анализирующих поток данных, проходящий через них.

Открытие письма, содержащего вредоносное программное обеспечение или осуществление постоянного, неконтролируемого доступа персонального компьютера на котором осуществляется работа с данными системы «1С:Бухгалетрия» к сети Интернет очень часто приводит к тому, что злоумышленники получают возможность зашифровать данные указанной системы. Соблюдение указанных выше рекомендаций во много обезопасит предприятие от подобных инцидентов, а в качестве дополнительной защиты целесообразно как можно чаще делать резервные копии данных с целью их использования для восстановления системы в случае шифрования. Хранить такие резервные копии целесообразно на съемном носителе или устройстве, не подключенном к сети Интернет и сети предприятия, так как вирусы-шифоровальщики, в случае попадания во внутреннюю сеть предприятия, имеют возможность зашифровать данные на всех устройствах, подключенных к сети.

Угрозы, основанные на методах социальной инженерии

В настоящее время также имеют место инциденты, когда злоумышленники осуществляют телефонные звонки в региональные филиалы и небольшие отделения финансовых организаций и представляясь сотрудниками головного офиса соответствующего учреждения (сотрудниками технической поддержки или службы безопасности) сообщали о необходимости проведения каких-либо технических работ. Для осуществления указанных работ, звонящий склонял сотрудника учреждения к проведению якобы тестовых операций перевода денежных средств в адрес различных юридических или физических лиц, в том числе путем пополнения балансов абонентских номеров мобильных телефонов. Для введения сотрудника в заблуждение, злоумышленники предлагали ему нажать некую комбинацию клавиш на клавиатуре, после чего система якобы должна перейти в «тестовый» режим, однако фактически этого не происходило и все дальнейшие операции производились не виртуально, а реально.

Наиболее действенным способом борьбы с подобного рода преступными проявлениями является повышение профессионального уровня сотрудников в части знания ими правил обеспечения информационной безопасности в подобной ситуации. При поступлении подобного звонка необходимо:

- уточнить все данные собеседника в том числе его фамилию, имя и отчество, должность, номер телефона для последующей связи, данные его непосредственного руководителя;
- выяснить в связи с чем необходимо проведение каких-либо операций в системе и по какой причине сотрудник не может осуществить их удаленно, со своего рабочего места;
- сообщить звонящему о том, что ему перезвонят по указанному ранее номеру телефона, после чего необходимо положить трубку и сообщить о звонке непосредственному руководителю;
- личные данные, предоставленные звонящим необходимо проверить путем звонка в отдел, где якобы работает указанный сотрудник или его руководителю;
- проведение каких-либо операций возможно лишь после проверки всех сведений, предоставленных собеседником.