ЭЛЕКТРОННЫЕ ДЕНЬГИ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

С постепенным проникновением информационных технологий во все сферы жизнедеятельности человека появилось такие понятия как "on-line магазины", "электронные деньги", "web-транзакции" и т.п. Фактически все эти сервисы имею одну цель – создать комфортные условия для приобретения товара или заказа услуги с минимальными затратами. Пользуясь современными технологиями на работе, дома или в любой точке, где есть беспроводной доступ к сети интернет, вы кладёте виртуальные товары в виртуальные корзины и оформляете покупку, при этом деньги вы за них платите вполне реальные. Или эквивалентные реальным. Только кошелек ваш при этом лежит не в кармане, а в глобальной сети, что логичным образом подвергает его определенным рискам. Попробуем разобраться, чем может обернуться использование виртуальных денег и как избежать связанных с этим потенциальных неприятностей.

В ходе исследования, проведенного компанией R&T Research, по заказу BSA накануне нового 2008 года, были опрошены сотрудники компаний, постоянно использующие ресурсы Интернет в рабочих и, как все прекрасно понимают, личных целях. Выяснилось, что 27% предстоящих новогодних покупок офисные работники Москвы планировали делать через интернет (год назад эта цифра равнялась 20%). Такой способ приобретения новогодних подарков, заказа алкоголя, электроники и других товаров позволяет существенно экономить время, тем более, что 54% московских сотрудников, планировавших Интернет-покупки к новогодним праздникам, собирались делать это непосредственно из офиса.

Системы оплаты "виртуальными деньгами" пока не вышли на первое место по популярности для on-line заказов– их по-прежнему опережает оплата наличными курьеру при получении заказа, однако пластиковые карты они уже "обогнали".

На сегодняшний день В России на рынке сервисов, основанных на электронных деньгах, играют не один десяток крупных организаций, владеющих электронными-платежными системами, среди них - WebMoney, "Яндекс.Деньги", RUpay, MoneyMail и "Деньги@mail.ru". Популярность таких систем, скорее всего, будет только расти, особенно если учесть, что сейчас еще не все Интернет-магазины взяли на вооружение эту технологию. С ростом доверия к ней – рынок расширится. Однако здесь есть несколько "но".

Электронный кошелек, как и любой другой счёт, необходимо заранее пополнять. Вариантов виртуализации реальных денег занесением средств в электронные кошельки существенно больше, чем аналогичных вариантов для пополнения классических банковских счетов, но мало кто конвертирует в виртуальные деньги большие суммы. В основном, пользователи пополняют свой счёт ровно на ту сумму, которая будет потрачена в ближайшее время на заранее определенную покупку. Это связано, прежде всего, с невысоким уровнем доверия к электронным платежным системам. Точно такое же мнение сложилось и в отношении оплаты Интернет-покупок пластиковыми картами сразу через Web. Попробуем разобраться, насколько это мнение соответствует действительности. На самом ли деле использование сервисов, связанных с глобальной сетью с одной стороны и финансовыми операциями с другой – может повлечь негативные последствия?

При первичной регистрации в какой-либо системе расчётов создаётся личный электронный кошелёк каждого пользователя. Когда он пожелает провести определённую транзакцию – снять деньги, оплатить покупку или перечислить деньги на другой Web-кошелёк – то должен будет ввести корректный пароль, который, по идее, известен лишь ему одному. Для проведения любых операций со своим Web-кошельком пользователь устанавливает некое клиентское приложение на свой компьютер или просто запускает браузер, после чего идентифицирует себя, вводя логин и пароль, и в случае успешной аутентификации, получает доступ к своему виртуальному кошельку.

"Финансовая газета" №8, 2008

ПАРОЛЬ ПАРОЛЮ - РОЗНЬ

Широко известно, что качественным и стойким к перебору паролем является набор символов, цифр и букв (причем желательно в разном регистре), состоящий из 10-15 знаков. Естественно, мало кто соблюдает это правило, часто пароли записываются на стикеры, а использование одинакового пароля для доступа к публичной почте, компьютеру и различным Интернет-сервисам вообще является чуть ли не всеобщей практикой. А между тем небезопасность такого подхода очевидна.

Вот один из примеров: исследователи из университета Мэрилэнд провели эксперимент, оставив на 24 дня подключенными к Интернет четыре компьютера под управлением Linux, защищенные "слабыми" легкоподбираемыми паролями. Как показали результаты, на системы было совершено около 270 тыс. попыток атаки, примерно по одной на каждые 39 секунд. Большинство атак проводилось с помощью словарных сценариев, просто перебирающих в расчёте на совпадение списки наиболее распространенных паролей и имён. В 43% случаев атакующие пытались использовать одни и те же слова и в качестве имени и в качестве пароля. Всего успеха добились 825 атак.

Главной проблемой парольной системы доступа, с которой может столкнуться пользователь web-кошелька, заключается в том, что кто-то выдаст себя за него. Узнав номер кошелька и пароль, злоумышленник сможет провести любую транзакцию, не говоря о возможности узнать баланс, оценить финансовую историю, скопировать эти данные и переправить любому заинтересованному лицу. И если пропажу денег ещё можно обнаружить, то всё остальное – гораздо сложнее.

При этом нужно понимать, что в случае использования сети Интернет, пароль не обязательно "подсматривать", ведь далеко не всякий злоумышленник имеет возможность заглядывать через плечо своей жертвы. Метод подбора пароля, вопреки распространённому мнению, тоже не всегда действенен. Большинство систем не позволит долго подбирать пароль, а кошелёк, в отношении которого начались подозрительные действия, заблокируют до выяснения обстоятельств. Конечно, легальный пользователь потратит определённое время на возобновление работоспособности своего кошелька, но в случае с паролями это, к сожалению, чуть ли не единственный вариант.

Но самым распространённым видом атаки стоит признать всё же перехват паролей. Ведь последовательность символов, введённая пользователем с клавиатуры, и предназначенная для передачи серверу, во время пути своего следования может быть подсмотрена не один раз. Для решения этой проблемы используется протокол SSL, который позволяет установить защищённое соединение с сервером. При этом все данные, в том числе и пароль, передаваемые между пользователем и сервером надёжно шифруются.

В основе протокола SSL лежит использование цифровых сертификатов, удостоверяющих подлинность сервера. Этот протокол используется и для подтверждения того, что пользователь находится на доверенном с точки зрения безопасности сайте. Ведь, далеко не всегда клиенты банка точно знают, какой адрес страницы правильный:

- Правильно citibank.account.com или account.citibank.com ?
- В некоторых шрифтах заглавная i и строчная L выглядят одинаково (I = l)
- URL-адрес не обязательно набирается вручную (адрес для перехода из поисковика или по ссылке из электронного письма может выглядеть крайне запутанно)

Значок SSL (защёлкнутый замок) – верный признак того, что пользователь находится на аутентифицированном сайте.

Но всегда ли на него обращают внимание? К сожалению, достаточно редко пользователи хорошо представляют себе, что такое цифровые сертификаты и как правильно реагировать на вопросы браузера о

доверии тому или иному удостоверяющему центру, выдавшему сертификат для сайта. Таким образом, многие (если не все) не проверяют то, что сервер действительно верно аутентифицирован.

ВСЕГДА ЛИ РИСК – ДЕЛО БЛАГОРОДНОЕ?

Незнание элементарных вещей или отсутствие должного внимания неизбежно ведёт к тому, что риски совершения финансовых мошенничеств продолжают оставаться высокими, тормозя развитие самой сферы электронных платежей, т.е. фактически, целой отрасли.

- Самое забавное, что компании, оказывающие данный вид услуг вместо решения проблемы просто перекладывают всю ответственность на самих пользователей. Вот, например, выдержки из публичной оферты на использование одной из платёжных систем:
- Оператор не несет ответственность за убытки, понесенные Клиентом в результате пользования предоставляемыми услугами.
- Оператор не несёт ответственность за возможные нежелательные для Пользователя последствия, возникшие вследствие предоставления Пользователю телефонной консультации.
- Оператор не несет ответственность за обеспечение безопасности оборудования и программного обеспечения Пользователя, используемого для получения Услуг.
- Клиент самостоятельно несет ответственность за выполнение договора об использовании платежной системы, приложений, соглашения и положений к настоящему договору, размещенных на сайте.

Тем не менее, варианты решения проблемы безопасных платежей в сети Интернет всё же есть.

ДОКОЛЕ?

Ещё в 2005 году на свет появилась программа Verified by Visa (Проверено Visa), основанная на технологии 3D-Secure. Суть её состоит в том, что первоначально пользователь регистрируется в системе электронной торговли. Он заходит на Web-сайт банка-эмитента и по ключевому слову (называется при оформлении карты) получает отдельный пароль для совершения on-line покупок. Далее он идет в Интернет-магазин, выбирает товар и заявляет, что собирается расплатиться картой. Запрос поступает на сервер банка-эмитента, который и производит аутентификацию. В этот момент между персональным компьютером пользователя и банком организуется закрытое соединение (с использованием SSL). Человек вводит данные карты и пароль, банк их проверяет, после чего сообщает магазину результаты проверки - "да" или "нет". Дальше магазин обычным образом запрашивает авторизацию через банк-эквайер. Если банк-эмитент подтверждает наличие денег на счете - покупка совершается. При этом весь процесс занимает считанные секунды. Хакеры лишаются возможности воровать данные держателей карт из базы Интернет-магазина, потому что этих данных там больше нет.

Помимо пароля в 3D-Secure могут использоваться различные методы аутентификации, - рассказывает С.Елютин, менеджер по развитию новых технологий компании Visa Int.: "Можно, например, выдать чиповые карточки, можно каждый раз присылать клиенту SMS-сообщение на телефон, когда он что-то покупает в Интернете. SMS-сообщение будет содержать одну надпись: "Введите пароль". Вы вводите пароль на телефоне, отправляете его через SMS, после чего на компьютере возникает сообщение: "Вы аутентифицированы, продолжайте покупку". Чтобы программа действительно заработала, ее должны поддержать банки-эквайеры, сетевые магазины, банки-эмитенты, а каждый держатель карточки - получить пароль".

Программа Verified by Visa сейчас реализуется во всем мире. В Америке ее поддержало несколько тысяч банков и большая часть on-line магазинов. В России технология до сих пока не столь широко распространена, даже среди крупнейших банков есть непримкнувшие к этой программе, поэтому

пользователи и продолжают использовать электронные деньги, зачастую доверяя защиту своих финансов парольной аутентификации, хотя есть и на порядок более надёжные методы.

Тот же протокол SSL предлагает действенное решение проблемы – аутентификацию пользователя по цифровому сертификату. Ведь отказываться от простого и удобного использования web-сервиса доступного из любой точки мира из-за возможных рисков готовы далеко не все. Выход один – снизить эти риски. Большинством аналитиков и специалистов в области информационной безопасности безоговорочно признаётся, что лучшей практикой для защиты доступа к своему электронному счёту является использование аппаратного средства для строгой аутентификации – электронного ключа или токена. Здесь можно провести аналогию с системами типа "клиент-банк", где важнейшим вопросом, касающимся удалённых способов работы банка с пользователем – является обеспечение безопасности. Уровни обеспечения могут быть разными, но система безопасности в целом состоит из следующих составляющих:

- аутентификация и авторизация (подтверждение того, что пользователь системы действительно является тем, за кого себя выдает и проверка прав пользователя на совершение каких-либо операций);
- шифрование передаваемых данных (имеет опциональное использование);
- использование электронной цифровой подписи или иного аналога собственноручной подписи (подтверждение авторства транзакции и целостности ее данных, а также действий, совершенных конкретным пользователем);
- регистрация всех транзакций в специальных журналах и аудит.

Топ-менеджмент ряда прогрессивных банков понимает, что использование простейших способов аутентификации, типа "логин-пароль", не обеспечивает нужной степени защиты и это серьёзным образом подрывает доверие к дистанционным технологиям обслуживания клиентов, Интернет-банкингу и т.п., что не может не сказываться на репутации банка.

Конечно, в системах клиент-банк речь идёт о реальных денежных средствах, а не о неких эквивалентах денег, как в случае с WebMoney, Яндекс-деньги и др. Однако риски и в том и в другом случае одни и те же – вопрос лишь в масштабе бедствий. А между тем использование двухфакторной аутентификации представляет собой сферу взаимного интереса как компаний, представляющих сервисы на основе "электронных денег", так и, собственно, пользователей этих сервисов. С одной стороны, пользователь будет уверен в том, что при любых обстоятельствах никто не сможет получить доступ к его счёту, без наличия электронного ключа (USB-устройство или смарт-карта) и знания PIN-кода к нему. С другой стороны – риск дискредитации компании, предоставляющей услуги электронных платежей с использованием электронных же денег, при применении клиентами токенов – фактически сводится к нулю.

Электронные ключи для аутентификации могут использоваться для подтверждения подлинности пользователя фактически в любой среде – при доступе к операционной системе, ПК, информационным ресурсам и порталам. Это многофункциональное устройство хранит в себе сертификаты, лицензии, пароли и другую секретную информацию и может быть тесно интегрировано с инфраструктурой открытых ключей (PKI).

На данный момент, основными преградами по применению аппаратных средств аутентификации в системах электронных расчетов в Интернете является незрелость сегментов e-banking и e-conmmerce, высокий уровень сокрытия инцидентов, связанных с нарушениями безопасности в этой области и не самая низкая стоимость самих аппаратных средств. Однако, появление таких бюджетных токенов, как например, eToken PASS, ориентированного для использования в подобного рода сервисах, вполне возможно исправит данную ситуацию в будущем. Более того, стоит отметить, что некоторые ЭПС, например, WebMoney по запросу клиента может предложить использование аппаратного токена для проведения аутентификации перед какой-либо операцией с электронными деньгами. Развитие такой тенденции может привести к существенному росту доверия к электронным системам платежей, а значит – развитию этого рынка.