



## **iTAN: оружие против мошенников**

### Новый способ защиты счета при Интернет-банкинге

В последнее время пресса в Германии неоднократно сообщала об уловке компьютерных мошенников под названием Phishing. Так окрестили хитроумный способ выяснения хакерами секретных кодов, которые есть у любого вкладчика, совершающего банковские операции в Интернете. После нескольких всплесков криминальной активности летом и осенью 2005 года мошенники, казалось бы, наконец, успокоились – но, как выяснилось, ненадолго. В электронных почтовых ящиках многих из нас вновь и вновь появляются послания с эмблемами разных немецких банков и с требованием перерегистрироваться, указав при этом секретные коды доступа к нашим счетам. На самом деле авторами этих э-мэйлов являются вовсе не финансовые институты, а мошенники, и следовать их требованиям «перерегистрации» означает предоставить им доступ к лежащим на вашем личном счету деньгам.

Однако и финансовые институты не теряли времени даром. Ими была разработана и частично введена новая, более надежная технология совершения банковских операций в Интернете. В ее основе – использование секретного кода iTAN. О чем идет речь? И действительно ли столь популярный среди жителей Германии и столь удобный онлайн-банкинг стал теперь полностью безопасным?

До сих пор подавляющее большинство банков и сберкасс, предлагающих услуги Homebanking (или Online-Banking), использовали так называемый PIN/TAN-Verfahren. Это коды, которые банк сообщал клиенту и с которыми тот должен был - в собственных интересах - обращаться строго конфиденциально. PIN (persönliche Identifikationsnummer), т.е. личный идентификационный код, предназначен, как говорит его название, для идентификации вкладчика банковским компьютером. Процедура эта крайне проста: выйдя на Интернет-страницу финансового института, нужно впечатать в двух соответствующих «окошках» номер счета (иногда снабженный дополнительными цифрами или буквами) и PIN-код. Если данные верны, то вкладчик оказывается в специальном, закрытом от посторонних глаз разделе сайта, где видит свой счет (или счета), лежащие на нем деньги, движения сумм на счету и т.д. – а главное, получает возможность совершить нужную ему банковскую операцию. При этом не

имеет значения, о какой, собственно, операции идет речь: об оплате коммунальных услуг и переводе денег по счету врача (т.е. собственно, классическом Online-Banking) или же об инвестициях в ценные бумаги (что обычно называют Online-Brokerage). И то, и другое становится доступно клиенту лишь после указания правильного PIN-кода.

Однако, PIN-код – это только первый уровень защиты: с его помощью можно лишь войти в закрытые разделы сайта вашего банка и подготовить совершение нужной вам банковской операции, например, заполнив электронный формуляр денежного перевода. Но перед тем, как начать исполнять ваши указания, компьютер запросит еще один специальный код – TAN (Transaktionsnummer), своеобразный код-разрешение на каждую конкретную операцию (т.н. транзакцию). Без него система ничего предпринять не может. Соответственно, если PIN-код у каждого владельца счета один (совместное ведение счета супругами сейчас оставим в стороне), то TAN-кодов – великое множество, а точнее, ровно столько, сколько операций требуется совершить вкладчику. Никакого «дефицита» TAN-кодов, конечно, не существует – банки регулярно присылают клиентам новые списки TAN-кодов по мере окончания прежних.

Таким образом, создается второй уровень защиты банковских счетов в Интернете: даже если злоумышленник сумеет выяснить ваш PIN-код, то «увести» с него деньги он всё равно не сможет – ведь для этого нужен TAN-код, которого у него нет! Ну, а если ему удастся «подсмотреть» используемый вами в Интернете TAN? И тогда бояться нечего: каждый TAN-код используется лишь единожды, и второй раз банковский компьютер его не примет.

И всё-таки – если система такая надежная, то как же мошенникам удавалось красть деньги со счетов? Увы, хакеры правильно определили слабое звено в цепи, сосредоточившись не на бесперспективных попытках «взломать» сайты банков, а на доверчивости клиентов. Рассылая поддельные электронные сообщения, они всеми правдами и неправдами выманивали у вкладчиков не только PIN, но и несколько еще **неиспользованных** TAN-кодов. Остальное (т.е. собственно кража) было делом нескольких минут - при наличии всех кодов система Online-Banking работает отлично.

Мириться с таким положением дел финансовые институты, естественно, были не намерены. Вначале они провели массовую акцию по информированию клиентов, а сейчас начали предлагать и технические решения проблемы. Наиболее распространенное – iTAN. Его уже ввели Postbank, ставший первой жертвой мошенников, Deutsche Bank, множество сберкасс на территории Германии (в том числе и в землях Гессен и Северный Рейн – Вестфалия) и другие финансовые институты. В целом, нововведение основывается на всё том же принципе PIN/TAN - за одним важным исключением. При совершении операции компьютер банка

требует не какого угодно из оставшихся неиспользованными TAN-кодов, а строго определенного, стоящего в присылаемом клиенту списке под определенным порядковым номером. Отсюда и название – iTAN, indizierte TAN.

Это небольшое, на первый взгляд, изменение перечеркивает все усилия мошенников, пытающихся выяснить у вкладчика пару неиспользованных TAN-кодов: ведь никогда не известно, какой код банковский компьютер запросит в следующий раз! Конечно, в жизни возможны всякие совпадения, но в данном случае их шанс настолько мал, что можно уверенно говорить о повышении уровня надежности системы.

Переход на iTAN и Postbank, и Deutsche Bank, и сберкассы осуществляют постепенно. Их новые клиенты имеют пронумерованные списки iTAN-кодов уже с первого дня, а прежние вкладчики могут в Интернете поменять систему защиты в любой момент. Впрочем, все финансовые институты подчеркивают, что никакой спешки или тем более обязанности делать это нет. И вовсе не потому, что iTAN работает еще не со всеми финансовыми компьютерными программами, которые некоторые клиенты ради удобства дополнительно устанавливают на своих домашних компьютерах. Главное – в том, что и прежняя система PIN/TAN обеспечивала высокий уровень надежности. Поэтому мы, в целом положительно относясь к нововведению, не считаем необходимым всем немедленно осваивать новую технологию онлайн-банкинга – и уж точно ради нее не отказываться от своего финансового института и переходить в другой. Тем более, что iTAN – явно не последнее изобретение в деле борьбы с мошенниками. И вообще: хотим напомнить, что никакая техника не заменит естественной осторожности, которая требуется в обращении с деньгами и в виртуальном, и в реальном мире.

Агентство экономической информации «ИнфоКапитал»

2006 г.

Запись на платные телефонные консультации у экспертов агентства «ИнфоКапитал» и фирмы «КУРС Консалтинг» - по тел. в Кельне 0221/340 61 80