manchete

Público

13-05-2014

Periodicidade: Diário
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 51453
Temática: Tecnologia
Dimensão: 339
Imagem: S/Cor
Página (s): 9

Fraudes na banca são quase sempre feitas com a colaboração "involuntária" dos cliente

Rosa Soares

O maior volume de fraudes na banca acontece com a chamada clonagem de cartões de crédito e nos pagamentos ou transferências realizadas através da Internet. Ainda assim, são as operações conhecidas por *phishing* (pesca), que consistem no envio de *emails* a pedir dados pessoais aos clientes que depois são utilizados de forma fraudulenta, as mais mediatizadas.

Os sistemas de segurança dos bancos, que são supervisionados pelo Banco de Portugal, não travam muitas das acções de pirataria informática e a colaboração directa ou indirecta dos clientes no fornecimento de dados ou em comportamentos menos seguros faz toda a diferença na hora de determinar quem vai suportar as perdas.

No caso dos cartões e transferências *online*, os clientes estão um pouco mais protegidos pela directiva comunitária de pagamentos, mas a legislação não é ainda muito clara. Em algumas situações, as perdas dos clientes estão limitadas a 150 euros, suportando o banco o restante. Mas, noutras situações, o cliente pode ter de suportar integralmente as perdas, ou repartir esse custo com o banco.

Uma transferência para uma entidade credível ou para uma desconhecida, ou a utilização do cartão num local que o cliente deveria ter considerado suspeito, pode fazer toda a diferença no momento de avaliação da segurança das operações e no apuramento da responsabilidade dos diferentes intervenientes.

No *phishing*, os bancos apostam tudo na informação preventiva aos clientes, através dos serviços *online* e de outros dispositivos, mas não assumem responsabilidades nas perdas sofridas, que correm por conta do titular de conta. No acesso aos serviços de banca *online* e através de outras comunicações, os bancos alertam os clientes para o facto de nunca pedirem dados pessoais por *email*, pelo que qualquer pedido do género deve ser associado a uma tentativa de fraude. Também alertam os clientes para rejeitarem *emails* suspeitos, uma vez que a simples abertura dessa correspondência electrónica pode permitir a instalação, nos computadores visados, de programas informáticos "maliciosos", capazes de obter códigos de acesso a contas bancárias e a outros dados financeiros.

Os bancos recomendam, ainda, aos clientes para não acederem aos serviços de *homebanking* através de computadores públicos ou partilhados, e insistem na instalação de programas de protecção nos computadores pessoais. À mínima dúvida ou suspeita, o banco deve ser imediatamente contactado.

O problema é que, na prática, muitos desses avisos ou não chegam a todos os clientes ou são neutralizados pela criatividade dos piratas informáticos, que chegam a conseguir imitar, com grande perfeição, as páginas principais dos *sites* dos bancos ou os seus logótipos. O número de fraudes detectadas não é divulgado pela banca e também nada se sabe sobre a capacidade de recuperação do dinheiro desviado.

Para garantirem sistemas de segurança eficazes, os bancos investem uma fatia significativa dos seus custos operacionais. Por causa deste encargo, alguns bancos, especialmente os mais recentes ou de menor dimensão, têm optado pela criação de cauções para pagar eventuais falhas de segurança, em alternativa a investimentos mais elevados em sistemas informáticas e equipas de controlo.

A segurança dos sistemas informáticos é uma área supervisionada pelo Banco de Portugal (BdP) através de vários tipos de controlo. Em resposta a um pedido de esclarecimento do PÚBLICO, o BdP refere que "os riscos relevantes das instituições supervisionadas são reavaliados anualmente" e que, "no conjunto diversificado e complexo de riscos a que as instituições estão sujeitas, o risco dos sistemas de informação assume relevância no âmbito do denominado 'risco operacional', que é avaliado a par de outros riscos considerados relevantes (por exemplo, risco de crédito, de mercado, de taxa de juro)".

O supervisor adianta que, "nas inspecções realizadas pelo Banco de Portugal, o risco dos sistemas de informação é avaliado no contexto das áreas funcionais analisadas". E que "as equipas de inspecção que o BdP mantém junto das instituições monitorizam os processos de controlo e revisão desenvolvidos pelas funções de controlo no contexto dos sistemas de informação, em que se incluem os trabalhos de auditoria interna".

Refere ainda o banco central que, anualmente, são reportadas à instituição todas as insuficiências relevantes detectadas pelas funções de controlo (relatório do sistema de controlo interno), em que se incluem as insuficiências associadas aos sistemas de informação. Em todos estes processos de supervisão, o BdP exige às instituições planos de acção para solucionar as insuficiências detectadas e a sua implementação é acompanhada pelos seus técnicos.

NELSON GARRIDO

Banco de Portugal supervisiona risco dos sistemas de informação