17 – Fevereiro de 2000

# Fraudes financeiras: nem sempre os hackers são os culpados.

As empresas do segmento bancário são certamente as mais adiantadas em relação à segurança eletrônica, contudo, esbarram em um problema curioso. Saber dosar o nível adequado de segurança que seja compatível com o negócio e inspire confiança, e ao mesmo tempo, evitar que as medidas selecionadas não impliquem na comodidade do cliente.

Cartão magnético que não acaba mais. Cartões multifunção de crédito e débito. Caixas eletrônicos de auto-atendimento espalhados por toda parte. Dinheiro eletrônico indo e vindo. São cenas que compõem o cenário financeiro e que estão formando a pauta dos noticiários jornalísticos. Uma verdadeira avalanche de casos de fraudes financeiras, transações e transferências indevidas que nos leva a questionar: quem são os culpados?!

Indiscutível a tendência das instituições financeiras em oferecer cada vez mais comodidade aos seus correntistas. Movimentação de altos valores, emissão de talão de cheques, realização de pagamentos, e ainda podendo fazer tudo isso de um caixa eletrônico ou de seu computador pessoal à qualquer hora do dia ou da noite, fazem parte da lista de operações permitidas aos clientes.

O que estamos vendo é o nascimento de um novo, interessante e vulnerável alvo para os golpistas. Afinal, porque se expor tanto e tentar uma fraude dentro do próprio banco - que certamente tem algum, senão forte, mecanismo de segurança – se o correntista - frágil, normalmente desinformado e agora com "poder" maior de movimentação de recursos - pode ser mais facilmente ludibriado?

Não pense somente na potencial escalabilidade de fraudes proporcionada pela Internet, Internet Banking e Home Banking, mas também no simples (para alguns) uso do próprio cartão magnético nos caixas eletrônicos. Todos os dias vemos novos "métodos" – se é que podemos chamar assim – de se trapacear. Pessoas nas salas de auto-atendimento que se mostram super prestativas e prontas a ajudar aquele senhor idoso que quer muito sacar sua aposentadoria, mas não consegue inserir o cartão no leitor, e tem seu cartão substituído e sua senha descoberta por descuido. Aquele caixa eletrônico providencial – no meio da noite – que resolve engolir seu cartão, mas que na verdade, foi vítima de uma "armadilha" feita pelo trapaceiro com o uso de uma película plástica. Ainda existem situações combinadas - como a que aconteceu ano passado - onde além de instalar uma "armadilha" que retinha o cartão, uma câmera da loja de conveniência fora direcionada intencionalmente para o caixa eletrônico do interior da loja e filmava toda a operação e consequentemente a senha.

Inúmeros golpes desse tipo surgem diariamente, o que sinaliza para a crescente ação dos oportunistas e não somente dos especialistas. A técnica de engenharia social, aliada à falta de conscientização e preparo dos correntistas, sem esquecer a parcela de culta por descuido, potencializam ainda mais este tipo de ação e nos faz criar uma separação clara entre os problemas associados aos hackers – que se utilizam principalmente da tecnologia - e os oportunistas que possivelmente nunca manusearam um computador.

A técnica de invasão por engenharia social é especialmente curiosa, pois não requer conhecimento técnico nem tão pouco computador. O importante é conhecer o comportamento humano e explorar seus pontos fracos de forma a atingir o objetivo de ganhar acesso à informações privilegiadas. Muitas vezes complementada pela técnica de vasculhar lixo (*trashing*) - onde se obtém as primeiras informações em papeis descartados de forma imprópria – a engenharia social se potencializa. Um único telefonema, se fazendo passar por um técnico ou demonstrando conhecer a empresa, os diretores, seus filhos ou algum processo importante, pode viabilizar o sucesso da tentativa.

Diante de todas essas vulnerabilidades, grande parte dos problemas estariam equacionados com a divulgação e conscientização pública de uma política de segurança específica, destacando-se o comportamento pessoal, criação, manutenção e uso de senhas de acesso. Pensando nisso, resolvi criar uma lista com algumas importantes dicas para minimizar os riscos e permitir o uso seguro dos serviços que se utilizam de uma senha:

- Selecione uma senha adequadamente complexa e compatível com o que está protegendo, levando-se em conta seu tamanho e formação;
- Opte por uma sequência sem sentido e formada por letras em caixa alta e baixa, além de números e – se quiser estar mais seguro – complete-a com caracteres especiais como #$*;
- Garanta sua confidencialidade acima de tudo. Nada de anotar em agendas de papel ou colocá-la em um bilhete sob o teclado, decore-a;
- Solicite sua substituição com alguma frequência ou quanto suspeitar de um vazamento;
- Exerça seu direito de substituição quando uma senha é gerada automaticamente pelo sistema;
- Agora um dica que torna sua tarefa de gerenciar senhas menos trabalhosa: escolha uma frase de fácil lembrança e crie sua senha com as iniciais das palavras que a compõe.

Vale lembrar que as vulnerabilidades e ameaças não se limitam ao que já foi falado. As próprias instituições financeiras são um grande e poderoso alvo e têm de estar preparadas para garantir o manuseio, transporte, armazenamento e descarte de informações. Não é à toa que 35% dos problemas de segurança eletrônica estão relacionados a funcionários ou ex-funcionários. Abra o olho.

***Marcos Sêmola*** *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Coordenador de Segmento de Mercado e Analista de Segurança da Módulo Security Solutions S.A.*
*msemola@modulo.com.br*