

93 – Novembro 2007

Inteligência da Fraude

Em Direito Penal, fraude é o crime ou ofensa de deliberadamente enganar outros com o propósito de prejudicá-los, usualmente para obter propriedade ou serviços injustamente. A fraude pode ainda ser praticada com o auxílio de objetos falsificados, através de diferentes meios e orientada a alvos distintos, permitindo ser classificada como fraude científica; artística; arqueológica; financeira; intelectual; eleitoral; contábil; jornalística entre outras.

De acordo com uma fonte especializada em fraudes, pesquisas recentes descobriram, por exemplo, que antigos egípcios, por volta de 500 A.C., fraudavam ricos e nobres vendendo falsos gatos e outros animais sagrados embalsamados para suas cerimônias fúnebres. Nas mitologias Grega e Romana, por sua vez, Hermes, considerado o deus dos ladrões e fraudadores, aplicava vários golpes nos demais deuses e por isso tinha freqüentes problemas com Zeus.

Estes e outros fatos históricos provam que o problema das fraudes é bem antigo. Obviamente com o progresso tecnológico, estes sistemas também evoluíram. Os fraudadores são comumente criativos, bem informados, flexíveis e adaptáveis a novas situações, por isso novas fraudes aparecem continuamente, se ajustando e desfrutando cada nova oportunidade.

No universo das fraudes eletrônicas, o que se tem visto é o aumento considerável da profissionalização dos golpes, assim como o aumento da extensão dos danos causados por esta modalidade. Isso se dá especialmente pelo crescimento da interatividade entre os ambientes Real e Virtual e ainda, pelo poder de alcance dos golpes. O mundo se globalizou e os golpistas também, o que nos faz ler notícias de um mesmo golpe praticado nas Américas, sendo aplicado em outro continente depois de alterações sutis.

Qualquer que seja o tipo de golpe, somos sempre uma vítima em potencial. Desta forma, a melhor forma de evitar as armadilhas e reduzir a probabilidade de queda em um golpe, é estar bem informado. Identificar as intenções do fraudador antecipadamente faz toda a diferença e estudar a inteligência da fraude o tornará mais preparado, e em teoria, um alvo menos interessante.

Em geral, as fraudes existem pela coexistência de três fatores básicos:

- A existência de golpistas motivados.
- A disponibilidade de vítimas adequadas e vulneráveis.
- A ausência de controles de fraude eficazes.

Explicar a motivação dos golpistas é relativamente fácil. Ela pode se dar pela falência do sistema prisional, a ineficácia das leis, a falta de regulamentação, a carência de fiscalização, o volume de vítimas vulneráveis, a facilidade de aplicação dos golpes, a redução dos custos da fraude, a impunidade, entre outras.

A existência de vítimas frágeis e vulneráveis se dá, por sua vez, por um conjunto de fatores ligados ao comportamento humano, mesmo que algumas diferenças possam ser percebidas pela cultura dos povos. Entretanto, em geral, os indivíduos se tornam vítimas vulneráveis pela falta de informação, pela ingenuidade, o despreparo para lidar com um ambiente eletrônico novo, o hábito do desrespeito às leis, a ganância, credulidade, ignorância, entre outros.

A ausência de controles eficazes representa o terceiro fator de existência das fraudes e se dá principalmente pelo despreparo das autoridades, da legislação, dos poderes que deveriam agir de forma integrada para aprender a inteligência do fraudador e fomentar o conhecimento da contra-inteligência para agir preventivamente.

Se tomarmos como exemplo as fraudes eletrônicas praticadas por email, veremos que os fraudadores iniciaram explorando fundamentalmente a carência de conhecimento técnico do usuário, fazendo-o executar, comandar e cometer erros operacionais que os beneficiassem ou que ao menos abrisse caminho para os próximos passos do golpe. Entretanto, à medida que a cultura da informática foi se popularizando, os índices de eficácia das fraudes puramente tecnológicas foram reduzidos, o que os obrigou a acrescentar mais inteligência aos golpes. Este movimento de transição pode ser claramente percebido pelos novos métodos baseados em informações pessoais ou informações de empresas e pessoas próximas ao ciclo de relacionamento da vítima, procurando tornar o golpe mais realista e verossímil possível.

É fato que a eficácia de uma fraude está diretamente relacionada à decisão da vítima em ir adiante, aceitar o convite, acreditar no discurso e assim, agir como espera o fraudador. É também factível que existam golpes tão bem desenhados que seria difícil não se tornar uma vítima, mas estes são a minoria. Infelizmente o ser humano é vulnerável por natureza e tem sua exposição ainda mais realçada quando se agregam outros fatores de alavancagem da fraude, muito bem explorados pelos golpistas. O principal deles é o desejo ganancioso de obter muito dinheiro ou outras vantagens sem os correspondentes esforços e riscos.

Se você não se encaixa nesse perfil e também não quer se tornar a próxima vítima, siga os dez conselhos básicos que compartilho caso esteja diante de uma abordagem duvidosa:

1. Não acredite em tudo que ouve, vê ou lê;
2. Tudo tem seu preço. Sempre desconfie de facilidades evidentes;
3. Resista ao que parece ser irresistível, até que tenha feito uma avaliação detalhada;
4. Antes de ir adiante, avalie os impactos potenciais e sua tolerância ao pior caso;
5. Colete o máximo de informações complementares para apoiar seu julgamento;
6. Use e abuse da Internet para procurar informações de fontes diferentes;
7. Não perca tempo com golpes básicos aprendendo um pouco mais sobre tecnologia;
8. Não se deixe tomar pelo impulso ou pela pressão da abordagem;
9. Se já for tarde demais, aja imediatamente e focado na contenção da fraude; e
10. Adquira um comportamento preventivo estudando a anatomia das fraudes.

O tema é interessante e extenso, por isso, deixarei a análise das técnicas e fatores psicológicos para a época do Natal, quando os golpistas passam a usar barba branca e as vítimas se enchem de bondade no coração, o que parece ser perfeito para os golpes natalinos.

Fonte: www.fraudes.org

Marcos Sêmola é Diretor de Operações de Information Risk da Atos Origin em Londres, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br