IX SEGeT 2012
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
Tema: Gestão, Inovação e Tecnologia para a Sustentabilidade

Fraudes na Internet e Engenharia Social - uma Experiência na Semana Nacional de Ciência e Tecnologia no Ifsp – 2011

Eulicio Fonseca Júnior
euliciojunior@gmail.com
IFSP

Marco Antônio Monteiro Guimarães
marco-antonio-monteiro@hotmail.com
IFSP

Resumo: Este documento apresenta uma análise da experiência realizada durante a palestra sobre Fraudes na Internet na Semana Nacional de Ciência e Tecnologia no Instituto Federal de Educação Ciência e Tecnologia - Campus Caraguatatuba - 2011. Foram abordados os métodos mais comuns utilizados pelos fraudadores para convencer suas vítimas a fornecerem informações necessárias para aplicarem seus golpes. Após o evento um dos palestrantes usou um dos métodos de engenharia social para obter o numero do CPF dos ouvintes

Palavras Chave: Fraudes - Engenharia social - - -

INTRODUÇÃO

O conceito de engenharia social tem levado a diferentes opiniões sobre o que é, e como funciona. Se é o ato de se contar uma mentira para conseguir alguma vantagem ou um favor sexual; ou se são apenas as técnicas usadas por criminosos ou talvez uma ciência, cujas teorias podem ser subdivididas em partes e suas equações podem ser estudadas; ou ainda, uma arte mística há muito perdida dando aos praticantes a capacidade de usar truques com sua mente poderosa como um mágico ou ilusionista, o fato é que seus efeitos têm causado prejuízo à sociedade.

RESUMO

Este documento apresenta uma análise da experiência realizada durante a palestra sobre Fraudes na Internet na Semana Nacional de Ciência e Tecnologia no Instituto Federal de Educação Ciência e Tecnologia - Campus Caraguatatuba - 2011. Foram abordados os métodos mais comuns utilizados pelos fraudadores para convencer suas vítimas a fornecerem informações necessárias para aplicarem seus golpes. Após o evento um dos palestrantes usou um dos métodos de engenharia social para obter o numero do CPF dos ouvintes.

PALAVRAS-CHAVE: Fraudes, Engenharia Social.

ABSTRACT

This document presents an analysis of the experiment conducted during the lecture on Internet Fraud at the National Week of Science and Technology at the Federal Institute of Education, Science and Technology - Campus Caraguatatuba - 2011. In the lecture, we discussed the various methods that fraudsters use to convince their victims to provide information needed to apply his phishings. After the event, one of the speakers used a method of social engineering to get the listeners' CPF number (Registration of Individuals).

KEYWORDS: *Fraud, Social Engineering*

Em 2003, o Computer Security Institute juntamente com o FBI constataram que 77% das companhias entrevistadas alegaram que a principal brecha de segurança relacionava-se com seus funcionários . A empresa Symantec – que atua na área de segurança – disse que em 1 (um) em cada 500 (quinhentos) e-mails enviados contem dados confidenciais[1]. O site financialservices.house.gov[2] destaca em relatório que 62% dos incidentes reportados ao trabalho podem colocar em risco os dados do cliente permitindo roubo de identidade. Nesse mesmo relatório 46% dos funcionários dizem ser extremamente fácil remover dados sensíveis do banco de dados das corporações.

A engenharia social é usada por pessoas comuns em situações cotidianas, seja uma criança fazendo manha para conseguir algo dos pais, ou o empregado tentando conseguir um aumento. Isso é engenharia social. Ela acontece no governo, nas empresas, no mercado de ações e outros segmentos. É o ato de manipular uma pessoa apara atingir objetivos que podem ou não ser de seu melhor interesse, e pode incluir a obtenção de informações, acesso, caminho ou direção para atingir determinado alvo e pode ser usada para o bem ou mal. Muitas vezes a engenharia social é usada em fraudes,

em roubo de identidade, ou procedimentos mal intencionados. (HADNAGY, 2011).
Existem vários casos de uso de engenharia social, porém existem dois tipos comuns:

- Por confiança: Ganhar a confiança da vítima para que ela entregue a informação;
- Por extorsão ou chantagem: Ameaçar a vítima com algo que a possa comprometer, obrigando-a a entregar a informação.

2 A SEMANA NACIONAL DE CIÊNCIA E TECNOLOGIA.

A Semana Nacional de Ciência e Tecnologia - 2011 teve como tema "Mudanças Climáticas, desastres naturais e prevenção de riscos" , promoveu palestras, minicursos, exposições, workshops e o 1º Seminário de Iniciação Científica do Litoral Norte – 2011. Dentre as palestras promovidas, Fraudes na internet destacou a necessidade de se prevenir contra **hackers** que usam a engenharia social como meio para conseguir informações sobre senhas bancárias, números de cartão de crédito de suas vítimas. Algumas das fraudes são listadas a seguir.

2.1 AS FRAUDES MAIS COMUNS

A engenharia social é muito mais antiga do que se imagina, algumas fraudes remontam ao século XVIII e mesmo antes na idade média - a venda de indulgencias é um exemplo clássico de Engenharia Social, cujo objetivo era arrecadar dinheiro daqueles que acreditavam que seus pecados podiam ser perdoados, ou que podiam conseguir uma boa posição no céu - mais recentemente no século XX, surgiram algumas fraudes notórias.

2.1.1 ESQUEMA DE PONZI

Este tipo de fraude consiste em convencer um grande número de pessoas a depositar quantidades em dinheiro em um suposto investimento rentável a curto prazo. O grande golpe está na entrada de valores de novos investidores, os quais têm o seu dinheiro usado para pagar investidores mais antigos. Num esquema de Ponzi existe apenas uma pessoa que é o centro do golpe e este é o responsável por atrair novos investidores para o esquema. Já no esquema de pirâmide, cada novo investidor que entra deve recrutar outros para manter os ganhos daqueles que já pertencem ao grupo.

2.1.2 CARTA DA NIGÉRIA -

Este golpe tem origens antigas, existem relatos de uma carta de Jerusalém datada do século XVIII (VIDOCQ, 1834) que utilizava os mesmos meios de persuasão utilizados atualmente.
A vítima recebe o golpe principalmente por e-mail, podendo também ser aliciada por cartas escritas à mão ou outro meio de comunicação. A história contada basicamente é a mesma, independente do meio em que ela chegue ao seu destinatário. O fraudador sempre se passa por um funcionário de banco ou do governo e conhece um milionário que faleceu recentemente deixando toda a sua fortuna no banco ou na forma de jóias. Ele precisa da ajuda da vítima para que ela se passe por um parente distante do falecido a fim de receber esta herança para que ambos a dividam. Contudo, antes de receber a sua devida parte, a vítima é persuadida a pagar altos valores em dinheiro ou fazer transações bancárias a fim de arcar com as despesas provenientes da transferência da "fortuna" para a sua conta. Este golpe também é conhecido como o Golpe do

Pagamento Adiantado. (Advanced Fee Fraude, em inglês).

2.1.3 Golpe das pessoas desaparecidas -

Este golpe é muito antigo e consiste em entidades falsas que tratam de pessoas desaparecidas, enviam **spams** pedindo informações de pessoas, doações e que seja repassado o email para todos os seus contatos. O interessante para tais entidades que criaram esses **spams** é a lista de e-mails verdadeiros, que são vendidos a outras entidades que realizam um trabalho similar.

2.1.4 Golpe do envelope vazio –

Este golpe, realizado geralmente em fins de semana e feriados, é um golpe que explora a fraqueza dos bancos, que realizam recesso bancário naqueles dias. Consiste em usar a engenharia social em negociações, oportunidade na qual os golpistas efetuam o pagamento com um envelope vazio em alguma instituição bancária, retirando o comprovante do caixa eletrônico. Com este em mãos, o golpista realiza a negociação, na qual a vítima só descobre que fora enganada após fim do recesso.

2.1.5 - BOATOS (*HOAXES*)

Utilizam a engenharia social e apelam para que o usuário (destinatário) os envie "para todos os seus conhecidos" ou "para todas as pessoas especiais de sua vida".

A diferença entre correntes e boatos está no conteúdo, pois, os boatos geralmente contam histórias alarmantes e falsas, sensibilizando o usuário (destinatário) a continuar a propagação. Os boatos mais comuns são:

- DIFAMATÓRIOS: denigrem empresas ou produtos, prometendo brindes ou falam dos riscos que determinado componente da fórmula do produto causa à saúde.

- FILANTRÓPICOS: contam histórias de crianças doentes, usando as tragédias e as catástrofes naturais como argumentos para pedir ajuda em dinheiro, que não será repassada às reais vítimas[3].

3 - FRAUDES BANCÁRIAS

O último relatório do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br)[4] em 2011 conforme apresentado na Figura 1, revela que o número total de notificações de incidentes no terceiro trimestre de 2011 foi um pouco superior a 100 mil, o que corresponde a uma queda de 21% em relação ao trimestre anterior, mas a um aumento de 152% em relação ao mesmo trimestre de 2010. A queda das notificações está relacionada a uma diminuição das notificações da categoria Outros.conforme a Figura 1. Entretanto é preocupante os incidentes relacionados a páginas falsas conforme exemplo na Figura 2.

A expectativa da Federação Brasileira de Bancos (FEBRABAN) no ano de 2011 é de que a opção por pagar as contas do próprio computador esteja aumentando cerca de 20% ao ano. Mas o número atual de 35 milhões de correntistas que acessam os serviços conhecidos como internet banking certamente cresce quando há dificuldades em fazer transações nos espaços físicos, ou quando ocorrem greves e as agências bancárias

sofrem paralisação. Por isso, a recomenda-se prevenir para evitar que falhas eletrônicas se tornem problemas financeiros.

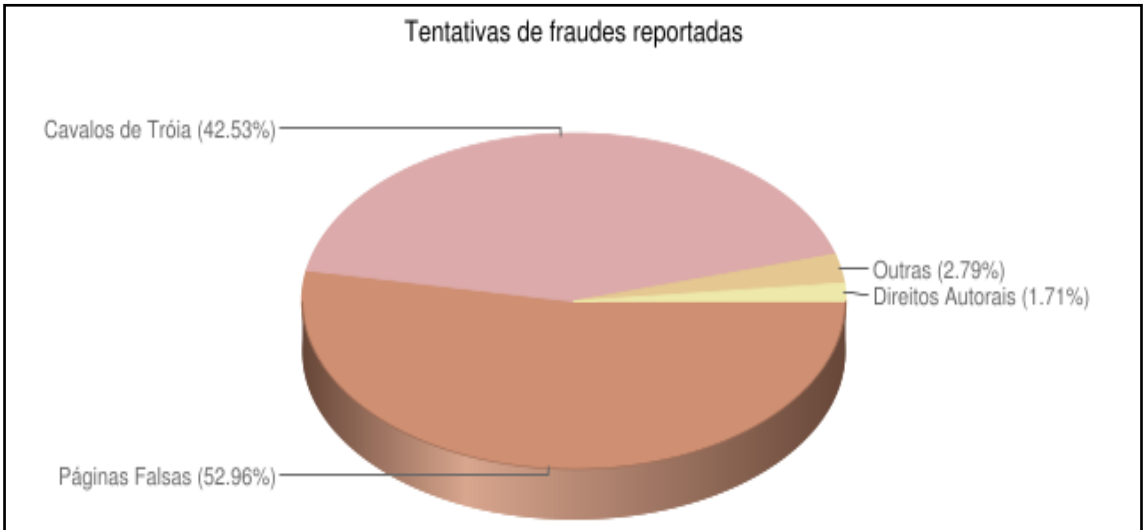
4. COMO EVITAR OS RISCOS DA ENGENHARIA SOCIAL EM CASA OU NO TRABALHO

Segundo James Della Valle, em artigo editado para revista Veja em 12/12/11[5], para evitar os riscos da engenharia social recomenda-se:

1. Cuidado com senhas pessoais, nomes de usuários e números de acesso. Qualquer sucesso na conquista desses itens pode motivar criminosos a continuar no seu encalço à procura de mais informações;

2. Evitar discutir projetos do trabalho em ambientes informais. Nunca se sabe quem pode estar ouvindo ou mesmo se colegas de trabalho são capazes de manter segredo.

3. Cuidados ao telefone. O hacker Kevin Mitnick ficou famoso nos anos 80 por aplicar golpes via telefone. Fraudadores se fazem passar por um profissional de suporte de uma empresa para pegar informações com funcionários. Muitos chegam a pedir senhas via telefone alegando os mais diversos motivos.



- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- **Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Direitos Autorais**: Notificações de eventuais violações de direitos autorais.
- Outras: Outras tentativas de fraude.

[*]Figura 1:Incidentes reportados ao CERT.br -- Julho a Setembro de 2011

Embora e-mails com tentativas de roubo de senha sejam facilmente descartados, algumas ameaças podem passar despercebidas. Tomar cuidado ao abrir apresentações e relatórios. Conferir sempre a procedência e-mail observando certos detalhes:

1. Algumas vezes, o nome da suposta pessoa que enviou pode estar correto, mas o endereço, não.

2. Cuidado com anotações contendo senhas na mesa de trabalho. Usuários incautos chegam ao ponto de colar o código de acesso do próprio computador no monitor.

5 – A EXPERIÊNCIA DE ENGENHARIA SOCIAL

No decorrer da palestra criou-se um clima de interação e confiança com a platéia seja nas respostas às perguntas ou na orientação de como se proteger contra as fraudes, enfatizando que nunca se deve fornecer informações pessoais sobre senhas de contas bancarias, senhas de cartões de débito ou crédito ou numero do CPF a quem quer que seja, a menos que seja muito necessário. Houve até uma simulação de cadastro em uma página falsa do banco Santander. Cada palestrante deixou a forte impressão de que estava ali para ajudar. No final da palestra, a platéia foi convidada a assinar o livro de presença e fornecer o numero do seu CPF.
A Tabela 1 mostra o resultado desta experiência:

Tabela 1: Perfil da platéia

Platéia	Área de atividade				**Assinantes**	**Forneceram CPF**
	Mat.	C civil	Web	PDS		
Alunos	3	5	15	12	**35**	**33**
Outros	1				**1**	**1**
Total geral					**36**	**34**
Percentagem dos que assinaram e forneceram o número do CPF					**94,4%**	

Embora os palestrantes tenham dado forte ênfase em tomar cuidado quanto a fornecer informações sobre senhas e principalmente sobre seu CPF, 94,4% foram induzidos a fornecer esta informação por causa do carisma criado pelos palestrantes.

CONSIDERAÇÕES FINAIS

Grandes empresas chegam a gastar mais de 30 milhões de dólares por ano com segurança só nos Estados Unidos para que lhes garanta proteção total às informações consideradas relevantes, desconsiderando de que a falha nem sempre está atrelada ao uso errado ou subutilização dessa mesma tecnologia, uma vez que é o ser humano quem está por trás dela. A vulnerabilidade do fator humano é mais decisiva do que a estrutura tecnológica envolvida nos equipamentos computacionais – que se bem configurados – bloqueiam com bastante eficiência as tentativas frequentes de pessoas maliciosas.

O atual paradigma nas grandes empresas e governo de que estão protegidos quando se investe apenas em equipamentos tecnológicos, está ultrapassado. Se essas entidades não incluírem treinamentos aos funcionários com relação aos ataques frequentes dos engenheiros sociais de nada vão valer os altos investimentos em equipamentos de segurança.

No curso ministrado no IFSP – Campus de Caraguatatuba – na Semana Nacional de Ciência e Tecnologia - 2011, percebeu-se - ao final da explanação sobre os tipos de fraudes mais comuns na internet e formas de como evitá-las - que mais de 94% dos participantes do curso, ao serem solicitados ao preenchimento de um formulário simples contendo seu nome e número do CPF, não questionaram o procedimento. Isso

demonstra que a engenharia social funciona bem quando se estabelece um laço de confiança entre os envolvidos.

As corporações e os governos – as maiores vítimas de fraudes – devem estar sempre atentos a esse fato e possibilitar formas constantes e eficientes de treinamentos de seus colaboradores. A tecnologia empregada na área de segurança, para ser eficiente, deve trabalhar paralelamente ao corpo funcional muito bem informado e cuidadoso.

AGRADECIMENTOS

Deixamos expressos nossos sinceros agradecimentos aos seguintes professores, sem os quais o presente trabalho teria sido impossível:
Prof. Msc. Eduardo Noboru Sasaki, Prof. Esp. Juliana L. A. M. G. do Nascimento e Prof. Msc. Nelson Alves Pinto

REFERENCIAS

[1]. http://go.symantec.com/vontu/ acessado em 12/12/2011
[2].http://financialservices.house.gov/media/pdf/062403ja.pdf acessado em 12/12/2011
[3].http://www.antispam.br/tipos/boatos/ em 12/12/2012

[4].http://www.cert.br/stats/incidentes/2011-jul-sep/fraude.html acessado em 12/12/2011

[5].http://veja.abril.com.br/blog/tech/seguranca/nao-caia-nos-golpes-da-engenharia-social/ acessado em 12/12/2011

HADNAGY, CRISTOPHER Social Engineering: The Art of the Human Hacking Indianapolis, IN,EUA Wiley Publishing Inc., 2011

VIDOCQ, EUGÈNE FRAÇOIS MEMOIRS OF VIDOCQ, PRINCIPAL AGENT OF THE FRENCH POLICE Philadelphia, IN EUA Carey & Hart, 1834

TABELAS:

[*]http://www.cert.br/stats/incidentes/2011-jul-sep/fraude.html acessado em 12/12/2011