

# EDUCAÇÃO E SEGURANÇA NA INTERNET

## ENGENHARIA SOCIAL

MUNDO DIGITAL: Engenharia Social

Frank Ned Santa Cruz, especialista em segurança da informação

Tecnologias podemos comprar com dinheiro, entretanto cultura só se adquire com informação e educação. Desde que o mundo é mundo e o homem organizou-se em sociedade, diversas são as formas e artifícios para que uns se beneficiem em relação a outros. Assim sendo, uma das técnicas mais antiga e extremamente efetiva hodiernamente trata-se da ENGENHARIA SOCIAL.

Se buscarmos exemplos na natureza iremos perceber vários tipos de relações onde um predador usando de camuflagem, ou seja, mostrando-se ser quem não é, com isso conquista a confiança da vítima atraindo a mesma para a mão glacial da morte.

O mesmo verificação na literatura e contos diversos, desde os infantis, onde a bruxa má com uma maçã adormece a princesa a clássicos de Shakespeare.

Não seria diferente no dia-a-dia, onde criminosos passando-se por representante de instituições legítimas envolvem pessoas menos avisadas em conversas a fim de obter informações com o objetivo de perpetuar golpes diversos entre eles fraudes eletrônicas ao sistema financeiro, que é uma das maiores fontes de perdas monetária no mercado bancário. No Brasil 85% das transações são realizadas com cartões de crédito, ponto para os avanços tecnológicos. O lado negativo é que ocupamos o 5º lugar, no mundo, em fraudes com cartão de crédito. As perdas com fraudes bancárias realizadas por meio eletrônico somaram R\$ 685 milhões no primeiro semestre de 2011, o que representa um aumento de 36% em relação ao mesmo período do ano anterior, que foi de R\$ 504 milhões. Os dados são os mais recentes, disponibilizados pela da Federação Brasileira dos Bancos – FEBRABAN.

O mundo mudo, mudou muito e rapidamente logo todas estas inovações tecnológicas trás riscos não aparentes ao cotidiano dos usuários comuns, que durante anos foram educados para se resguardarem de ameaças físicas, como o batedor de carteiras, furtos e roubos de veículos, etc.

Nesse sentido os usuários precisam criar uma cultura de segurança para desfrutarem de uma experiência positiva no meio virtual. Devem estar atentos à abordagem, seja por telefone e principalmente por e-mail que peçam para instalar programas, clicar em determinados links ou solicitam informações cadastrais ou dados privados como agência, conta e senha de acesso a portais ou Internet Bank.

Mas, infelizmente, não são somente riscos financeiros. Existem indivíduos que criam perfis falsos em mídias sociais e com isso “aproximam-se” de crianças e jovens com os mais diversos tipos de propostas e segundas intenções. Assim, os pais devem estar atentos aos relacionamentos estabelecidos pelos seus filhos no mundo virtual, definindo em algumas situações limites de uso e mesmo criando um perfil para interagir e estar presente no

# EDUCAÇÃO E SEGURANÇA NA INTERNET

ciberespaço junto com os filhos. Fortalecer os laços familiares de convívio e confiança é, como sabido por todos, uma ferramenta poderosa para proteger e orientar as crianças e jovens.

Instituições legítimas também podem ter seu nome manchado ao serem, falsamente, associadas a campanhas, venda de produtos e ofertas de oportunidades diversas.

Para se protegerem dessa tão antiga forma de ataque que é a ENGENHARIA SOCIAL, não basta ao usuário final comprar programas de segurança para instalar em seus dispositivos computacionais, sejam eles computadores, tablets ou smartphones. Devem estar informados e preparados para reconhecer alguns dos riscos existentes.

## Alguns pontos de atenção

- **Ao acessar o site da sua instituição bancária, por exemplo, evite buscar o mesmo em ferramentas de busca, como o Google, pois criminosos realizam anúncios falsos em nome das instituições apontando para o sítio do fraudador. A recomendação é, você, digitar diretamente na barra de endereços o site da instituição, que provavelmente está impresso em algum extrato;**
- **Ao receber e-mails que dizem que seu nome está sujo no SERASA, que você está sendo investigado pelo Ministério Público, que existe uma ação de cobrança e correlatos, desconfie. Geralmente trata-se de “phishing”, uma forma tecnológica de engenharia social, que tenta direcioná-lo para algum sítio falso com o objetivo de furtar sua senha;**
- **Na mesma linha, ao receber e-mail com anexos ou joguinhos de pessoas desconhecidas ou mesmo de pessoas conhecidas, que geralmente não enviam e-mail desta natureza, desconfiem, podem ter sido enviados por criminosos com o objetivo de instalar em seu computador, tablete ou smartphone algum tipo de artefato malicioso, para capturar tudo que você digitar, inclusive suas senhas.**

A lista de formas de ataque é grande. Neste contexto, as instituições de ensino, do fundamental ao superior, possuem relevante papel na orientação e formação dos cidadãos do amanhã. Formando alunos conscientes e preparados para uma interação positiva com as novas tecnologias, mas também envolvendo os professores e pais no processo de esclarecimento e cuidados a fim de evitar exposições que podem gerar consequências negativas.

# EDUCAÇÃO E SEGURANÇA NA INTERNET

## NOVAS VERSÕES DESTE MATERIAL

Novas versões deste material podem ser encontradas em:

- <http://www.santacruzadv.com/artigos.html>

