ESTUDO DA VULNERABILIDADE À COLETA DE INFORMAÇÕES POR MEIO DA TÉCNICA DE PHISHING SCAM NA FATEC BOTUCATU

[1]ALMEIDA, Igor N. S. de; [2]**ALMEIDA, Osvaldo Cesar Pinheiro de**; [3]**RALL**, **Ricardo**

[1]*Infomática para Negócios, Faculdade de Tecnologia, Botucatu, SP, Brasil. E-mail: irmão_dele@hotmail.com*
[2]*Faculdade de Tecnologia, Botucatu,SP, Brasil.* ***E-mail: c****esar.pinheiro@gmail.com*
[3]*Faculdade de Tecnologia, Botucatu,SP, Brasil.* ***E-mail:*** *rrall@fca.unesp.br*

Palavras-chave: Engenharia Social. Phishing. Vulnerabilidade.

INTRODUÇÃO

A informação é um item de suma importância para os negócios de uma organização e necessita ser adequadamente protegida. Com isso, surgiu o termo Segurança da Informação, que é a proteção da informação contra os mais variados tipos de ameaça (VICTÓRIA, 2007).

Mais comumente, as organizações focam a sua atenção na tecnologia e subestimam o elo mais fraco, que rege toda e qualquer empresa: o fator humano. Neste contexto, surge a Engenharia Social, que explora alguns fatores da psicologia humana como confiança e o poder de persuasão em extrair informações pessoais e confidenciais com intuito de usá-las indevidamente (PEIXOTO, 2006).

Umas das técnicas mais utilizadas de Engenharia Social é o *Phishing Scam*, onde sites falsos são criados e indivíduos inescrupulosos utilizam-se da tecnologia, utilizando da boa fé das pessoas para obter informações úteis que poderão ser utilizadas em golpes (MARCIANO; LIMA-MARQUES, 2006).

Este projeto teve como objetivo analisar a vulnerabilidade do fator humano em ceder informações por meio da Engenharia Social em conjunto da técnica de *Phishing Scam*, por meio da coleta de dados em site falso.

MATERIAIS E MÉTODOS

Na elaboração do projeto foi utilizado um computador – AMD Athlon○ tm 64 X2 Dual Core 4000+ 2.11 GHz, 2GB de RAM, Disco Rígido de 160 GB, Windows 7 Home Premium. Também foi utilizada a ferramenta Adobe Dreamweaver CS4, para a criação do site. Para a criação do banco de dados em MySQL, utilizou-se o software Navicat.

A metodologia empregada foi baseada em fontes científicas atualizadas disponíveis sobre o assunto de desenvolvimento e análise da tecnologia

Phishing Scam. A Figura 1 mostra o site elaborado.

Figura1 - Visualização do site criado.

RESULTADOS E DISCUSSÃO

O site foi utilizado por seis dias, e, como observado na Figura 2, constatou-se que 749 pessoas visualizaram o site, dentre as quais 465 (62%) realizaram cadastros

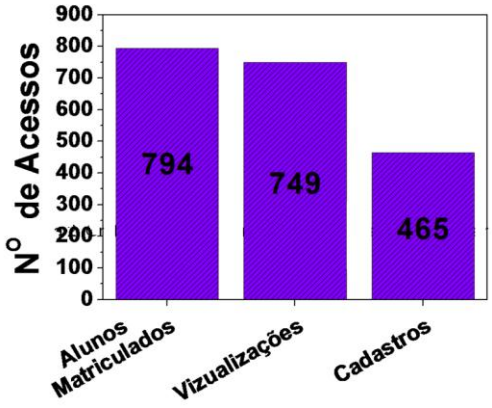

Figura 2 – Gráfico de análise comparativa Visualização x Cadastros

Dividindo os cadastros por sexo, temos a revelação de uma grande porção de homens, como demonstra a Figura 3.

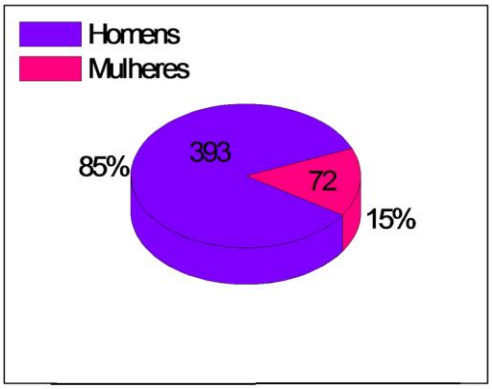

Figura 3 – Comparação de cadastro Homens X Mulheres.

Analisando os cadastros por faixa etária, como demonstrado na Figura 4, localizamos a porção mais atingida pela técnica de *Phishing*

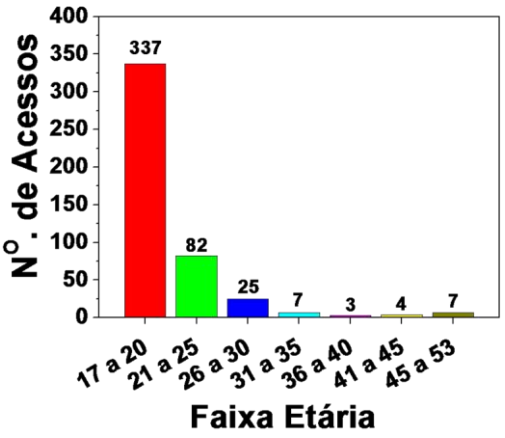

Figura 4. Análise por idade da amostra afetada.

.

CONCLUSÕES

A partir dos resultados obtidos, constatou-se que as pessoas podem ser

facilmente enganadas às ações de Engenharia Social. A técnica de *Phishing Scam*, associada a um ganho fácil, pode se tornar uma ótima ferramenta para o uso de *hackers*.

Diante do total de alunos da Fatec-BT que tiveram acesso ao site, 62% realizaram cadastro. Dentre eles, 85% eram homens e somente 15% mulheres. A faixa etária mais atingida foi de 17 a 20 anos. Sendo identificado o público alvo, deve ser realizado um trabalho de conscientização quanto aos perigos escondidos por trás destes sites mal intencionados.

REFERÊNCIAS

VICTÓRIA, E. M. **Gestão coorporativa**: Estudos, métodos e metodologias da engenharia social para a segurança da informação. Trabalho de conclusão de curso – Fatec, Botucatu, 2007.

PEIXOTO, M. C. P. P. **Engenharia social e segurança da informação**: na Gestão Corporativa. Rio de Janeiro: Brasport, 2006. 132p.

MARCIANO, J. L.; LIMA-MARQUES, M. O enfoque social da segurança da informação. **Ci. Inf.** Brasília, DF, v.35, n.3, p. 89-98, set/dez., 2006