O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing

Gliner Dias Alencar[1], Marcelo Ferreira de Lima[2], André C. A. Firmo[2]

[1] Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Av. Jornalista Anibal Fernandes, s/n – 50.740-560 – Recife – PE – Brazil

[2]Secretaria de Tecnologia da Informação e Comunicação – Tribunal de Justiça de Pernambuco (TJPE)
Av. Martins de Barros, 593 – 50010-230 – Recife – PE – Brazil

{gliner.alencar, marcelo.lima.br, caetanofirmo}@gmail.com

Abstract. *This paper, based on theoretical and applied research in companies in Greater Recife, Pernambuco State, Brazil, aims to measure the efficiency achieved through the ongoing process of awareness and training of employees of private companies in areas outside of the IT on the subject of Social Engineering and Phishing. Research shows that social engineering and phishing continue to be an efficient way to get data from employees in the corporate environment. Thus, we demonstrated a strategy, without the cost of acquiring tools, so users often categorized as a weak link in the chain, are transformed into a more efficient enterprise-class protection layer.*

Resumo. *O presente trabalho, baseado em estudos teóricos e pesquisa aplicada em empresas do Grande Recife, Estado de Pernambuco, Brasil, tem como objetivo mensurar a eficiência obtida através do processo contínuo de conscientização e treinamento de funcionários de empresas privadas de áreas externas à TI, sobre o tema Engenharia Social e Phishing. A pesquisa demonstra que a engenharia social e o phishing continuam sendo um meio eficiente para se conseguir dados de funcionários em meio corporativo. Desta forma, demonstra-se uma estratégia, sem custos de aquisição de ferramentas, para que os usuários, muitas vezes categorizados como elo fraco da corrente, sejam transformados em mais uma camada eficiente da proteção corporativa.*

1. Introdução

Para um efetivo tratamento da segurança da informação nos dias atuais são necessárias ações gerenciais para tratar e melhorar os processos, tecnologias e pessoas, como cita Gualberto *et al*. (2012). A presente pesquisa, com foco principal no elemento pessoa da tríade mencionada, consiste em interpretar a influência de uma política de conscientização continuada sobre a segurança da informação (SI) para funcionários, aplicada em empresas do Grande Recife, na tentativa de verificar se tais medidas realmente conseguem aumentar o nível de segurança da informação das empresas através da diminuição, principalmente, de casos de engenharia social ou *phishing* sofridos pelos usuários.

Segundo Mitnick e Simon (2006) e Soni, Firake e Meshram (2011), engenharia social pode ser entendida como uma arte para manipular pessoas fazendo-as tomar

ações que normalmente não fariam para um estranho, normalmente cedendo algum tipo de informação. Do ponto de vista corporativo, ações deste tipo podem ser usadas para atacar relações de confiança e processos de uma organização, com o objetivo de garantir acessos não autorizados. Em ataques de *phishing*, segundo Jagatic *et al.* (2007), que podem ser combinados com engenharia social, as vítimas também são levadas a fornecerem informações restritas ou sigilosas, como senhas e outras que darão acesso a dados sensíveis ou de algum valor. No caso do *phishing*, segundo Moore, Clayton e Anderson (2009) e Soni, Firake e Meshram (2011), as pessoas são estimuladas a fornecer dados por meio de mensagens eletrônicas cujo remetente personifica entidades ou organizações que devem inspirar confiança ou receio ao atacado.

Atualmente diversos casos de *phishing* e engenharia social são relatados pela imprensa, como citam Moore, Clayton e Anderson (2009) e Sullivan (2010). As tentativas de fraude tentam obter acesso a contas de *email*, dados pessoais, credenciais de acesso a contas bancárias, informações estratégicas das corporações e tudo o mais que se traduza em valor para o atacante, que em suas investidas pode personificar uma empresa que o atacado se relacione comumente ou até mesmo um órgão governamental com o qual o atacado tenha obrigações legais. Casos novos surgem com freqüência assustadora e uma solução de combate ao problema parece estar distante.

Segundo pesquisa de Alencar (2011), que também aborda empresas do Grande Recife, em 65% das empresas não existe a divulgação institucional e frequente sobre a SI na corporação e 85% da amostra citaram que não existem treinamentos periódicos ou processos de conscientização sobre o tema SI para os funcionários. Na mesma pesquisa, Alencar (2011) ainda afirma que as principais dificuldades para se implantar as ferramentas de SI na empresa são: restrições orçamentárias (47%), falta de priorização (41%), falta de conscientização dos funcionários (38%) e escassez de recursos humanos especializados (32%).

Baseado nessas informações, este trabalho visa demonstrar que é possível se criar uma camada a mais na Segurança da Informação, abordando um aspecto geralmente desprezado, o fator humano e como esta visão pode diminuir dispêndio de recursos financeiros em segurança da informação, colaborando com a principal dificuldade apresentada pelas empresas analisadas por Alencar (2011).

2. Metodologia

O estudo consistiu em aplicar um treinamento sobre engenharia social e *phishing*, durante 2 dias consecutivos, com 2 horas de treinamento por dia, focando em casos práticos para exemplificar e melhor transmitir a teoria sobre os referidos assuntos.

O treinamento foi realizado para 30 pessoas, em sala na própria empresa dos funcionários, em formato de palestra, utilizando vídeos e apresentação de *slides*, apresentando casos, debatendo e retirando dúvidas dos funcionários sobre os temas. Como pré-requisito para as pessoas que fariam parte da amostra, foi solicitado que todos fossem funcionários da empresa, que fossem de equipes ou setores diversos, que realizassem suas atividades laborais em computador corporativo, que não fossem da área de Tecnologia da Informação (TI), que não tivesse formação acadêmica na área de TI e que frequentassem o curso por completo.

Após o treinamento, metade dos funcionários treinados, recebeu boletins de segurança, três vezes por semana, durante 4 semanas, alertando sobre as ameaças

relativas à engenharia social e *phishing*, assim como informações de procedimento em tais casos (afirmando que bancos não enviam solicitações de recadastramento ou solicitam senha; o que são *links* suspeitos, entre outros avisos).

Durante 21 dias, iniciando quinze dias após o treinamento, era enviado um *email* por dia com algum tipo de *phishing* para a conta de *email* corporativo de 45 usuários, 15 funcionários que realizaram o treinamento e receberam o reforço via *email* posteriormente (grupo 1), 15 funcionários que realizaram o treinamento e não receberam reforços via *email* posteriores (grupo 2) e mais 15 usuários que atendiam a todos os pré-requisitos dos demais, porém não participaram do treinamento não receberam boletins por *email* (grupo 3). Todos os *emails* consistiam em imitar a aparência de instituições bancárias (Banco do Brasil – BB, Bradesco e Itaú), de *webmails* públicos (Hotmail e Gmail), de solicitações internas para troca de senha de rede ou do *email* institucional. No total de 7 tipos de *phishing* diferentes, sendo enviado, cada um, três vezes durante o período.

Todas as empresas utilizavam o correio eletrônico como ferramenta de comunicação corporativa e nenhuma das pesquisadas enviavam solicitações de trocas de senhas de sistemas, rede ou do próprio correio eletrônico via *email*.

Ao clicar no *link* do *email* era contabilizado o clique e aparecia uma página de erro, onde era solicitada que o mesmo tentasse em outro momento, não sendo contabilizado mais de um clique no mesmo *link* de um mesmo *email.*

3. A Amostra

A pesquisa foi realizada em quatro empresas do Recife, estado de Pernambuco, todas da iniciativa privada, do setor terciário da economia e que não tinham atividade fim relacionada à TI, na Tabela 1 são detalhadas a abrangência das empresas analisadas:

Tabela 1. Abrangência das Empresas Analisadas

	Abrangência	**Funcionários**	**Computadores**
Empresa A	Estadual	1300	2300
Empresa B	Nacional	500	400
Empresa C	Multinacional	5000	5000
Empresa D	Nacional	200	100

Em relação à existência e divulgação de uma Política de Segurança da Informação (PSI) pelas empresas analisadas, podemos observar os detalhes da amostra na Tabela 2, que aponta, na teoria, a empresa A em um nível de maturidade mais avançado (por possuir uma PSI implantada e ter divulgação contínua e frequente da própria PSI e sobre segurança da informação); as empresas B e C em um nível intermediário (com uma PSI, mas sem divulgação formal alguma) e a empresa D em um nível mais baixo de maturidade em SI (sem PSI nem divulgação na área de SI).

Tabela 2. Existência e Divulgação de PSI nas Empresas Analisadas

	PSI	**Plano de Divulgação de Segurança**	**Plano de Divulgação da PSI**
Empresa A	Formal implantada, sendo obrigatório o seu conhecimento.	Sim, Frequente e contínuo.	Sim. Frequente e contínuo.
Empresa B	Formal implantada	Não há um plano.	Não há um plano.
Empresa C	Formal implantada	Não há um plano.	Não há um plano.
Empresa D	Sem uma PSI implantada	Não há divulgação.	Não há divulgação.

Desta forma, foram criados três grupos de 15 funcionários em cada empresa, conforme metodologia, totalizando 12 grupos representados por A1, A2, A3, B1, B2, B3, C1, C2, C3, D1, D2, D3, onde a letra representa a empresa que o grupo pertence e a numeração o nível de informação e conscientização sobre o assunto, onde o número 1 representa o grupo com treinamento e reforço por *email*, o 2 apenas o treinamento e o 3 o grupo que não recebeu treinamento.

4. Resultados

Pela metodologia utilizada, em cada célula é possível observar a quantidade de cliques executados pelo usuário, podendo haver no máximo 45 cliques por célula da Tabela 3 (excetuando a coluna total), o que representa as três vezes em que cada *email* foi enviado para os 15 componentes de cada grupo. A Tabela 3 apresenta os resultados obtidos, mostrando que os usuários com capacitação e reforço (grupo 1), ou somente a capacitação (grupo 2), em engenharia social e *phishing*, diminuem gradativamente a quantidade de cliques se comparado aos grupos do tipo 3, visto que em todas as quatro empresas pesquisadas a quantidade de usuários que clicaram na armadilha enviada foi menor no grupo 1 do que no grupo 2 que, por sua vez, foi menor que no grupo 3. Tais resultados, também visualizados no Gráfico 1, ressaltam a importância do capacitação sobre SI, assim como de ações continuadas sobre o assunto no ambiente corporativo.

Tabela 3. Quantidade de cliques realizados

	BB	Bradesco	Itaú	Hotmail	Gmail	Rede	*email* Corporativo	Total
A1	3	0	0	0	6	8	12	29
A2	4	2	1	0	7	8	15	37
A3	3	2	2	5	5	11	14	42
B1	0	0	2	1	1	5	11	20
B2	0	1	5	5	3	7	15	36
B3	1	0	5	6	9	7	11	39
C1	3	6	4	4	7	8	9	41
C2	2	8	9	7	6	11	19	62
C3	0	8	11	6	13	12	21	71
D1	2	5	1	4	3	7	11	33
D2	3	6	3	5	3	7	17	44
D3	7	4	0	8	9	5	17	50

Entre as empresas analisadas, a empresa C foi a que teve os piores resultados absolutos, o que poderia ressaltar a importância da correta divulgação da PSI e da segurança da informação como um todo na empresa e não apenas a sua implantação. Porém, a empresa B, que obteve o melhor resultado, encontra-se no mesmo estágio de maturidade. A empresa D, considerada a empresa com a menor maturidade em SI, visto que não possui uma PSI implantada nem divulgação alguma na área de segurança da informação, situou-se na terceira colocação e a empresa A, que, em teoria, encontra-se em um estágio mais avançado de segurança da informação e esperava-se que obtivesse os melhores resultados, galgou a segunda posição. Fatos que apontam a necessidade de uma análise mais aprofundada e abrangente para verificar o motivo dessas colocações não seguindo o, teórico, nível de maturidade das empresas. Porém, tais números indicam, mesmo que de forma simplória, uma possível ação para melhoria nos casos de *phishing* através de capacitação dos funcionários e, números melhores ainda, quando combinada a capacitação com reforços periódicos indiferentemente do nível de maturidade que se encontra a empresa.

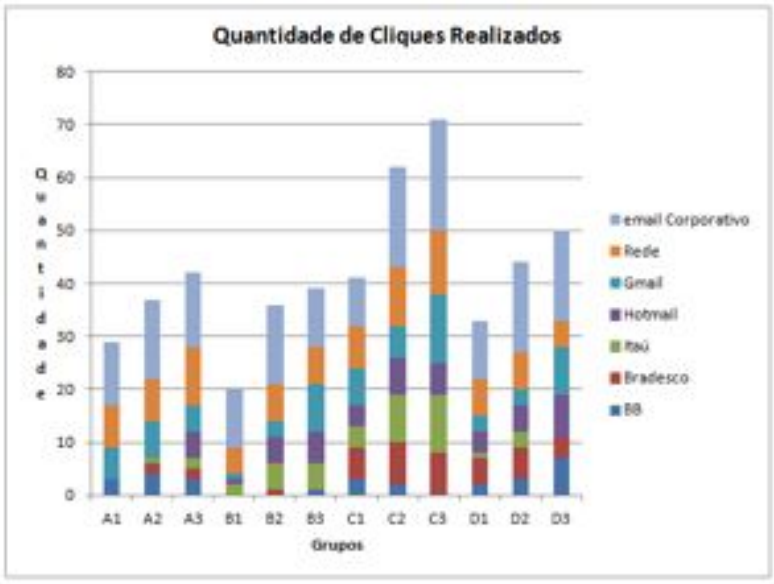

Gráfico 1. Quantidade de cliques realizados

5. Conclusões

A pesquisa demonstra que a engenharia social e o *phishing* continuam sendo um meio eficiente para se conseguir dados de funcionários em meio corporativo, principalmente quando se trata de dados internos da corporação, pois, pelos dados, percebe-se uma crença maior nas solicitações realizadas para se conseguir dados internos por meio de ferramentas internas, neste caso o correio corporativo.

Verificou-se também que a capacitação e conscientização contínua dos funcionários podem servir como fator de elevação do grau de segurança da informação da corporação, fortalecendo o que hoje representa o elo mais fraco da segurança da informação numa corporação. Segundo Alencar (2011), ao aplicar os questionários e, consequentemente, analisar as empresas e os respondentes foi possível perceber, na maioria dos casos, que se tem conhecimento dos problemas, dos métodos e tecnologias para melhorar o ambiente, bem como de que ações precisam ser feitas para que tais problemas sejam mitigados, contudo, não são realizadas as devidas ações e precauções necessárias. O que corrobora com o estudo de Shay et al. (2010), pois o mesmo fala que os usuários normalmente se sentem mais seguros utilizando senhas fortes para *login*, mesmo assim costumam usar senhas consideradas fracas.

Alencar (2011) ainda cita que a segurança da informação deve ser entendida como uma responsabilidade de todos. Afinal a informação existe porque alguém irá precisar dela em algum momento. Portanto, percebe-se a necessidade da mudança do pensamento das pessoas que fazem a segurança e dos demais envolvidos em cada etapa de qualquer processo do negócio. A segurança necessita ser entendida e pensada de forma mais ampla onde cada um tem que fazer a sua parte, por menor que seja, de forma segura. Nesta situação o aumento da segurança, em cada etapa ou camada irá gerar resultados melhores e aprimoramentos contínuos da segurança da informação e, consequentemente, da qualidade do serviço ou produto entregue.

Para que isto ocorra, é necessário mais do que um conjunto de treinamentos, é imprescindível uma política completa de divulgação, treinamento e conscientização que se integre, formando um processo educacional para os funcionários de uma forma geral (internos e externos à área de TI, assim como profissionais desde a área operacional até o alto escalão das empresas), permitindo que as práticas de segurança sejam incorporadas na rotina de trabalho de todos, como corrobora, entre outros, Alexandria (2009), Cunha (2007) e Marciano e Marques (2006).

Segundo Cunha (2007, p.2) "o simples treinamento dos recursos humanos também se mostra ineficaz, frente à contínua desatualização dos conhecimentos ministrados. É necessário educar as pessoas, indo muito além de simplesmente treiná-las", para que se tornem menos vulneráveis e mais uma camada de segurança.

Referências

Alencar, G. D. (2011) "Estratégias para Mitigação de Ameaças Internas", Centro de Informática, Universidade Federal de Pernambuco, Recife.

Alexandria, J. C. S. (2009) "Gestão da Segurança da Informação: Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica", Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo.

Cunha, R. (2007) "Treinando Macacos, Educando Pessoas", Fundação Getúlio Vargas, Rio de Janeiro.

Fonseca P. F. (2009). "Gestão de Segurança da Informação: O Fator Humano". Pontifícia Universidade Católica do Paraná. Curitiba.

Gualberto, E. S., Sousa Jr, R. T., Deus, F. E. G., Duque, C. G. (2012). InfoSecRM: Uma Abordagem Ontológica para a Gestão de Riscos de Segurança da Informação. In: *VIII Simpósio Brasileiro de Sistemas de Informação (SBSI 2012)*, p. 1-12, São Paulo.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., Menczer, F. (2007) "Social Phishing", In: Communications of the ACM, Volume 50, Issue 10, October, p. 94-100.

Marciano, J. L.; Marques. M. L. (2006) "O Enfoque Social da Segurança da Informação", In: Ci. Inf. Brasília, v. 35, n. 3, p. 89-98, Dezembro.

Mitnick, K. D., Simon, W. L. (2006), A Arte de Enganar, Makron, 1ª Edição.

Moore, T.; Clayton, R.; Anderson, R. (2009). The Economics of Online Crime. In: *Journal of Economic Perspectives*, v. 23, n. 3, p. 3-20.

Shay, R.; Komanduri, S.; Kelley, G. K.; Leon, P. G.; Mazurek, M. L.; Bauer, L.; Christin, N.; Cranor, L. F. (2010) "Encountering Stronger Password Requirements: User Attitudes and Behaviors", In: Symposium on Usable Privacy and Security, Redmond, EUA.

Soni, P.; Firake, S.; Meshram, B. B. (2011) "A phishing analysis of web based systems", In: International Conference on Communication, Computing & Security, pages 527-530.

Sullivan, R. J. (2010) "The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy", In: Workshop on the Economics of Information Security, Harvard University, EUA.