Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

v. 12, n. 3
set-dez 2013

Editorial

Foco nas organizações

Foco na tecnologia

Ensaios

Fast track SBSI

Nominata de avaliadores

ISSN: 1677-3071

Revista hospedada em: http://revistas.facecla.com.br/index.php/reinfo
Forma de avaliação: *double blind review*

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente, mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

A PERSPECTIVA DE ANÁLISE COMPORTAMENTAL COMO FORMA DE COMBATE À ENGENHARIA SOCIAL E PHISHING

BEHAVIORAL ANALYSIS AS A MEANS TO PREVENT SOCIAL ENGINEERING AND PHISHING

(artigo submetido em outubro de 2013)

Gliner Dias Alencar
Doutorando em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE) e Analista de Planejamento, Gestão e Infraestrutura em Informações Geográficas e Estatísticas do IBGE
gda2@cin.ufpe.br

Marcelo Ferreira de Lima
Especialista em Auditoria de Sistemas e Informação pela UFPE, Analista de sistemas do Tribunal de Justiça do Estado de Pernambuco e Professor da Faculdade Joaquim Nabuco
marcelo.lima.br@gmail.com

André Caetano Alves Firmo
Mestre em Engenharia da Computação pela Universidade de Pernambuco (UPE), Arquiteto de TI no Tribunal de Justiça de Pernambuco e Professor da Faculdade Joaquim Nabuco
caetanofirmo@gmail.com

ABSTRACT

The increasing informatization of enterprises and the volume of information exchange in computer' networks spurred competition among organizations. This scenario promoted change in the information security threats, where social engineering and phishing became an increasingly promising method for attacks and information theft. This paper presents a study in companies of Grande Recife, state of Pernambuco, Brazil, with the objective of measuring the efficiency achieved through the continuous process of awareness building and training of employees of private organizations from areas external to IT about information security incident prevention and data security. The paper presents a strategy that does not rely on expensive tools acquisition costs by means of which the users, often considered the weak link in the security chain, can be transformed into another efficient layer of corporate protection.

Key-words: information security; social engineering; phishing; behavioral analysis.

RESUMO

A crescente informatização das empresas e o aumento do volume de troca de informações na rede de computadores impulsionou a concorrência e competitividade entre as instituições. Este cenário promoveu uma mudança nas ameaças de segurança da informação transformando engenharia social e *phishing* em métodos cada vez mais promissores para ataques e roubo de informação. Este trabalho apresenta um estudo realizado em empresas do Grande Recife, estado de Pernambuco, com o objetivo de mensurar a eficiência obtida por meio do processo contínuo de conscientização e treinamento de funcionários de empresas privadas de áreas externas à TI sobre segurança da informação e prevenção de incidentes de segurança de dados. 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.

Palavras-chave: segurança da informação; engenharia social; *phishing*; análise comportamental.

1 INTRODUÇÃO

É crescente a utilização da informação para os mais diversos fins e tomadas de decisões, aumentando a sua importância no meio corporativo e social. Neste contexto, é um grande desafio para as pessoas e organizações prover meios para promover e gerir a segurança da informação, visto que têm aumentado em quantidade e criticidade as informações e, consequentemente, também as ameaças que as cercam.

Para um efetivo gerenciamento e tratamento da segurança da informação, são necessárias ações para tratar e melhorar os processos, tecnologias e pessoas, como citam Gualberto *et al*. (2012) e Rigon e Westphall (2013). A presente pesquisa, com foco principal no elemento pessoa da tríade mencionada (processos, tecnologias e pessoas), 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, contribuindo para a diminuição, principalmente, de casos de engenharia social ou *phishing* sofridos pelos usuários.

Segundo Mitnick e Simon (2003) 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 fornecer informações restritas ou sigilosas, como senhas que dao 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 com que o atacado se relacione comumente ou até mesmo um órgão governamental com o qual o atacado tenha obrigações legais. Casos novos surgem com frequência assustadora e uma solução de combate ao problema parece estar distante.

Segundo pesquisa de Alencar, Queiroz e De Queiroz (2013), 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, Queiroz e De Queiroz (2013) ainda afirmam que as principais dificuldades para se implantar as ferramentas de SI na empresa são: restrições orçamentárias, falta de priorização, falta de conscientização dos funcionários e escassez de recursos humanos especializados, apontadas por 47%, 41%, 38% e 32% dos participantes da sua pesquisa, respectivamente.

Com base nessas informações, este trabalho visa a demonstrar que é possível se criar uma camada a mais na Segurança da Informação, abordando um aspecto geralmente desprezado, o fator humano. Acredita-se que com esta visão, pode diminuir o dispêndio de recursos financeiros em segurança da informação, o que endereça a principal dificuldade apresentada pelas empresas analisadas por Alencar, Queiroz e De Queiroz (2013).

2 REFERENCIAL TEÓRICO

A área de segurança da informação, em seu sentido mais amplo, até mesmo por ser recente e abrangente, vem sendo abordada de forma multidisciplinar e trabalhada por diferentes áreas do conhecimento como a Administração, a Ciência da Computação, a Ciência da Informação, a Economia, as Engenharias, a Tecnologia da Informação, entre outras.

Particularmente, para este trabalho, junta a área de segurança da informação, com foco na engenharia social e *phishing*, com a perspectiva da análise comportamental da aprendizagem.

2.1 ENGENHARIA SOCIAL

A quantidade de pessoas envolvidas nos processos internos, associada à falta de uma correta política de gerenciamento e manuseio deste bem, faz com que as próprias pessoas envolvidas tornem-se um grande motivo de preocupação nas empresas, existindo diversos exemplos de empresas que sofreram grandes prejuízos pela colaboração direta ou indireta para tais ameaças (RAMOS, 2007). Casos relacionados à roubos de dados, perda de informações, sabotagem de TIC e engenharia social estão cada vez mais frequentes no noticiário.

É notória a participação humana nas mais diversas questões relacionadas à segurança da informação. Neste sentido, a literatura vem categorizando essas pessoas de acordo com suas ações, objetivos, conhecimento e metodologia de ataque. Como salientado por Nakamura e De Geus (2007), sendo corroborados por Ramos (2007), os principais grupos de pessoas que ameaçam as informações das organizações sãos: *Black hats, Coders*, *Cyberpunks,* Engenheiros sociais*, Gray hats, Insiders, Script kiddies e White hats*. Tal categorização não é excludente, desta forma uma mesma pessoa pode ter características inerentes a mais de um grupo ou transitar entre os grupos em determinado momento ou ação.

Alexandria (2009, p. 57) ressalta que a “engenharia social ocorre quando alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter acesso não autorizado a computadores ou informações sigilosas”. Corroborando esse entendimento, Nakamura e De Geus (2007) e Ramos (2007) compreendem a categoria de engenheiros sociais como incluindo pessoas que, ao invés de focarem na tecnologia, visam as vulnerabilidades do ambiente, principalmente humanas, para, utilizando suas habilidades de persuasão ou manipulação de outras pessoas, conseguir as informações desejadas.

Segundo Nakamura e De Geus (2007) e Ramos (2007), normalmente, os engenheiros sociais são “evoluções” dos iniciantes na arte de explorar vulnerabilidades (*Script Kiddies*) que continuaram na “profissão”. Os *Script Kiddies* buscam *sites* que fornecem *scripts* prontos ou utilizam ferramentas prontas de ataques para realizar seus feitos, muitas vezes sem mesmo entenderem em profundidade os códigos e metodologias em execução, mas sendo capazes de causar grandes prejuízos a empresas com seus ataques. *Script kiddies* e engenheiros sociais continuam, em função disso, representando problema para as organizações (COMPUTERWORLD.PT, 2010; PANDA, 2010).

Precisa-se ser entendido também que a engenharia social pode ser utilizada tanto de forma maléfica, como benéfica, para ajudar a melhorar a segurança da informação, como aborda Araujo (2005), para quem o trabalho na área de segurança da informação exige uma mistura de arte, ciência e técnicas. Além dos conhecimentos tradicionais, muitas vezes são requeridas características inerentes à engenharia social para melhor entendimento e resolução de problemas, assim como na realização de testes e validações de segurança (ARAUJO, 2005).

2.2 PHISHING

A partir do início do século XXI perceberam-se alterações nos ataques, adotando-se procedimentos que são seguidos até os dias atuais. Tendo comumente finalidade financeira, e não mais busca por notoriedade, as ameaças são criadas para se propagar mais rápido. *Worms* e ataques são escritos para serem mais "inteligentes" e eficientes e são direcionados, ao invés de serem meramente oportunistas. Golpes de *phishing* são projetados para enganar pessoas buscando informações financeiras. Conjuntos de *botnets* podem controlar, de forma centralizada, milhares de sistemas, aumentando seu alcance. Há mercados negros para troca de informações e serviços. Nesse contexto, *insiders* representam o maior risco (CONTOS, 2006; MOORE, CLAYTON E ANDERSON, 2009).

A visão dos *spams* como grande entrave a produtividade e grande causador de perda financeira é comprovada pelo seu crescimento descontrolado, tendo quem afirme que quase todas as mensagens de *email* enviadas pela *Internet* são indesejadas, sendo a maioria *spam* ou *phishing* com cunho financeiro (MICROSOFT, 2010).

A Microsoft, em seu último relatório de inteligência sobre segurança, aponta que o Brasil teve uma média de 13,11 *sites* de *phishing* para cada 1.000 *hosts* no terceiro trimestre de 2012, enquanto a média global foi de 5,41. No quarto trimestre os dados tiveram uma ligeira queda, mas o Brasil ainda continua com números alarmantes, 12,59 contra 5,10 da média global (MICROSOFT, 2013).

O Gráfico 1 relata a proporção das categorias de *sites* ativos utilizados como *phishing* de janeiro a julho de 2010, onde se percebe uma maioria esmagadora de páginas financeiras (*financial sites*). Sendo uma técnica que tem apontado para outros meios como forma de captura de dados, tais quais *smishing* (*phishing* por SMS) e *vishing* (*phishing* por voz, utilizando redes VoIP).

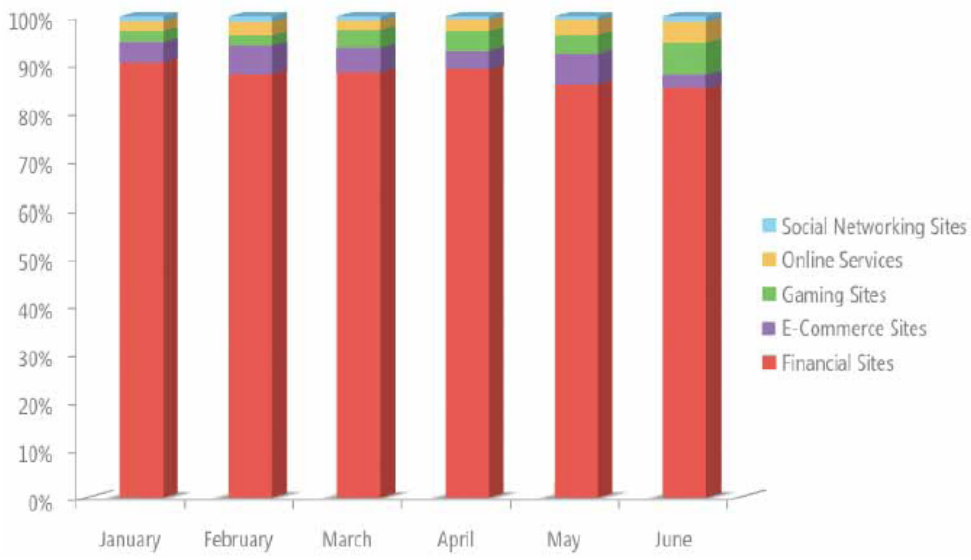

Gráfico 1. Sites de *phishing* ativos

Fonte: Microsoft (2010)

2.3 PROCESSOS DE APRENDIZAGEM

Uma preocupação sempre presente quando se trabalha no intuito de mudar comportamentos é a compreensão do processo da aprendizagem humana. Nessa linha, várias perspectivas teóricas trazem explicações por meio de abordagens que enfocam o efeito de fatores genéticos e ambientais. O presente estudo segue a perspectiva comportamental, conhecida como Análise Comportamental, que atribui o processo de aprendizagem humana ao estabelecimento de associações múltiplas entre cadeias de estímulo, resposta e consequências (CARRARA, 2005). Rose (2005, p. 31) contribui com tal pensamento ao apontar que “a perspectiva da Análise Comportamental leva a considerar que, em princípio, qualquer indivíduo é capaz de aprender, mesmo aqueles que apresentam limitações ou deficiências".

Na Análise Comportamental, o termo ‘comportamento’ pode ser entendido de duas formas: o comportamento respondente envolve reações

reflexas a estímulos específicos e o comportamento operante, por outro lado, envolve as consequências da resposta (BOCK, FURTADO E TEXEIRA, 2009). Estas consequências operam sobre o ambiente, modificando-o e modificando o comportamento subsequente, alterando a probabilidade de que respostas similares voltem a acorrer. Como afirmou Skinner (1957, p. 1, *apud* TOURINHO, 2011, p. 189), "os homens agem sobre o mundo e o modificam e, por sua vez, são modificados pelas consequências de sua ação".

O comportamento é, portanto, multideterminado, uma vez que cada conduta é influenciada pela interação entre muitos fatores orgânicos e ambientais. A aprendizagem é entendida como encadeamentos, combinações e generalizações de condicionamentos, responsável principal pela mudança de comportamentos (CARRARA, 2004).

Luna (2001) indica alguns processos básicos que podem ocasionar ou modificar o comportamento humano: a modelagem, as contingências de reforço e a repetição.

A modelagem é o método que visa à aprendizagem de uma nova resposta a partir do reforço seletivo das respostas intermediárias até que se alcance a resposta desejada. Este método é bastante utilizado no ensino da Matemática e da Física (CARRARA, 2005).

As contingências de reforço estão relacionadas à situação na qual o comportamento ocorre, ao próprio comportamento e às suas consequências. A ideia é que o tipo de consequência do comportamento aumenta a probabilidade de um determinado comportamento voltar a acontecer, ou seja, se alguém faz algo que produz uma consequência boa continua agindo assim (CARRARA, 2005).

Por fim, atividades que envolvem um grande número de repetições são aprendidas de modo mais eficaz, pois a associação feita entre os estímulos fortalece o armazenamento do conhecimento adquirido (CARRARA, 2005). Assim, "a pesquisa em Análise Comportamental tem demonstrado repetidamente que os limites estabelecidos por condições orgânicas podem ser ampliados através de procedimentos instrucionais adequados" (ROSE, 2005, p. 31).

A partir dessas considerações, no presente estudo, o planejamento metodológico buscou utilizar o conhecimento advindo da abordagem comportamental, no que diz respeito a fatores que favorecem a mudança de comportamento, para fortalecer a aprendizagem do comportamento preventivo acerca das ameaças relativas à engenharia social e *phishing*.

3 METODOLOGIA

O estudo consistiu em aplicar um treinamento sobre engenharia social e *phishing*, durante dois dias consecutivos, com dois 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 trinta funcionários de cada uma das quatro empresas que aceitaram participar da pesquisa. O treinamento, em formato de palestra, ocorreu em sala na própria empresautilizando vídeos e apresentação de *slides*, apresentando casos, debatendo e tirando 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 tivessem 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 quatro 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, foi enviado um *email* por dia com algum tipo de *phishing* para a conta de *email* corporativo de 45 usuários, quinze funcionários que realizaram o treinamento e receberam o reforço via *email* posteriormente (grupo 1), quinze funcionários que realizaram o treinamento e não receberam reforços posteriores via *email* (grupo 2) e mais quinze usuários que atendiam a todos os pré-requisitos dos demais, porém não participaram do treinamento e 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 foram enviados sete tipos de *phishing* diferentes, cada um deles, três vezes durante o período.

Todas as empresas utilizavam o correio eletrônico como ferramenta de comunicação corporativa e nenhuma das pesquisadas enviava 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, a partir da qual se solicitada que o usuário tentasse acessar o *link* em outro momento, não sendo contabilizado mais de um clique no mesmo *link* de um mesmo *email.*

4 DA PESQUISA REALIZADA

As quatro empresas participantes, tratadas aqui como empresa A, B, C e D, são todas empresas privadas do setor terciário, com sede na cidade do Recife, capital do estado de Pernambuco. Nenhuma delas tem atividade fim relacionada à área de TIC. Na Tabela 1 são detalhadas a abrangência,

quantidade de funcionários e de computadores das quatro 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

Fonte: elaborada pelos autores

Em relação à existência e divulgação de uma Política de Segurança da Informação (PSI) pelas empresas analisadas, pode-se observar os detalhes da amostra na Tabela 2, que aponta a empresa A como dispondo de 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 estariam 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). A importância dessa maturidade e formas de mensurá-la são discutidas por Rigon e Westphall (2013).

Tabela 2. Existência e divulgação de PSI nas empresas analisadas

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

Fonte: elaborada pelos autores

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

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-se a coluna total), o que representa as três vezes que cada *email* foi enviado para os quinze componentes de cada grupo.

A Tabela 3 apresenta os resultados obtidos, mostrando que os usuários com capacitação e reforço (grupo 1), ou somente capacitação (grupo 2), em engenharia social e *phishing*, diminuem gradativamente a quantidade de cliques se comparado aos integrantes dos 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 são visualizados no Gráfico 2, ressaltando a importância da capacitação sobre SI, assim como de ações continuadas sobre o assunto no ambiente corporativo.

Tabela 3. Quantidade de cliques realizados sobre *links* que poderiam ser de *phishing*

	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

Fonte: elaborado pelos autores

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, encontrar-se-ia em um estágio mais avançado de segurança da informação e que esperava-se que obtivesse os melhores resultados, ficou a segunda posição.

Esses fatos apontam a necessidade de uma análise mais aprofundada e abrangente para verificar o motivo dessas colocações não seguindo o que se poderia esperar a partir da análise do seu nível de maturidade de implantação de políticas de segurança. Porém, tais números indicam, mesmo que de forma simplista, que uma ação de treinamento para reduzir os casos de *phishing* pode ser efetiva, tendo resultados ainda melhores quando combinada a capacitação com reforços periódicos, indiferentemente do nível de maturidade de segurança de informação em que se encontra a empresa.

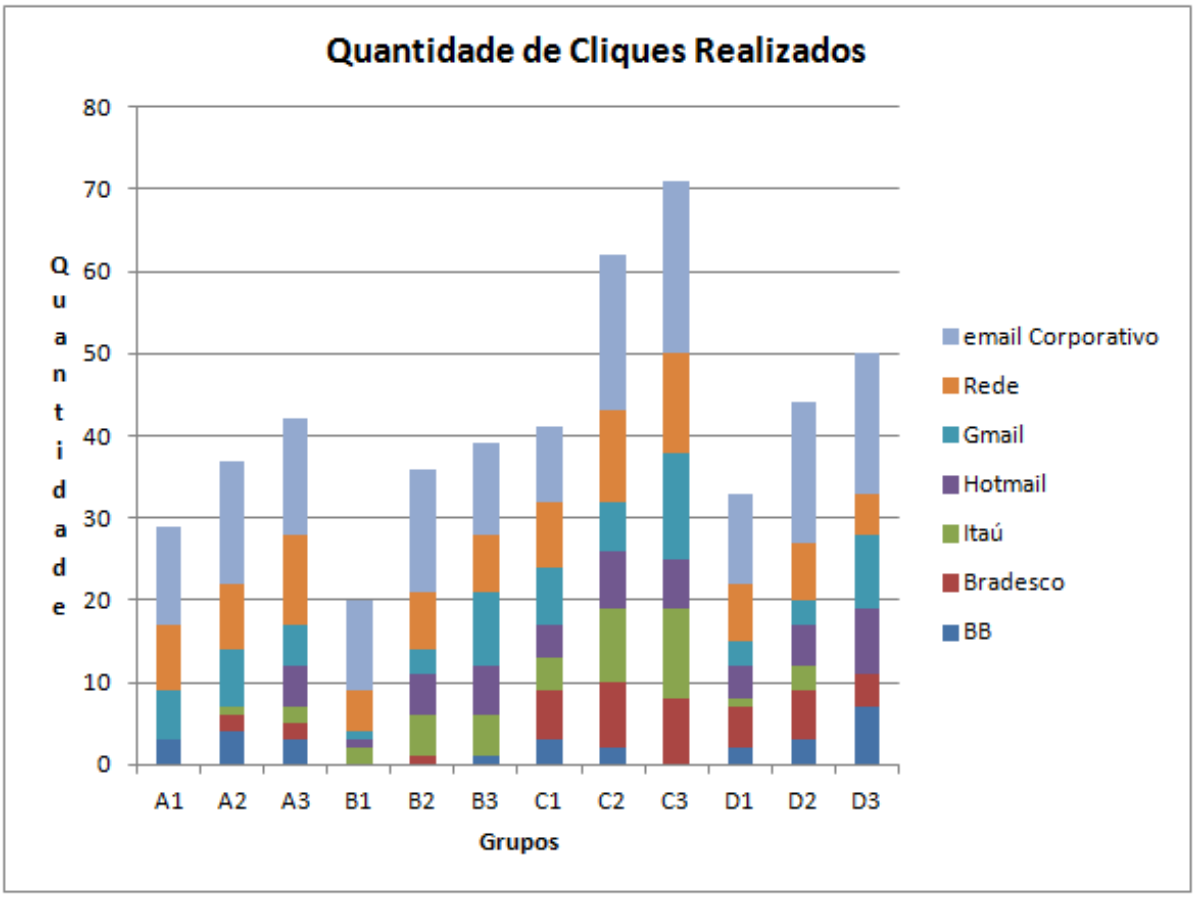

Gráfico 2. Quantidade de cliques realizados
Fonte: elaborado pelos autores

5 CONSIDERAÇÕES FINAIS

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 tratam 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.

Em consonância com a perspectiva da análise do comportamento, os resultados encontrados no grupo que recebeu sistematicamente informações acerca das ameaças relativas à engenharia social e *phishing* demonstram que o reforço por contingências e repetição podem ser instrumentos úteis na mudança comportamental das pessoas, uma vez que os usuários passaram a ter um comportamento mais preventivo, diminuindo a quantidade de vítimas de engenharia social e *phishing*, ou seja, obtiveram uma consequência positiva com a ação. O treinamento contribuiu para o comportamento preventivo, fazendo com que o usuário aumentasse a probabilidade de agir de modo mais prudente.

As mensagens enviadas três vezes por semana também auxiliaram na aprendizagem do comportamento preventivo, pois, a partir da repetição das informações, as associações puderam ser fortalecidas e armazenadas de modo eficaz.

Desta forma, acredita-se 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 em uma corporação: seus próprios funcionários.

Segundo Alencar, Queiroz e De Queiroz (2013), 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 tomadas para que tais problemas sejam mitigados. Contudo, não são realizadas as devidas ações e precauções necessárias. As evidências obtidas corroboram o estudo de Shay *et al.* (2010), que já havia percebido que os usuários normalmente se sentem mais seguros utilizando senhas fortes para *login*, mas, mesmo assim, costumam usar senhas consideradas fracas.

Alencar, Queiroz e De Queiroz (2013) ainda alertam 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. 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, gera 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 recomendam, 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 representem mais uma camada de segurança para proteger os dados empresariais.

Sabendo que a área estudada ainda carece de aprofundamentos e melhorias, percebe-se a necessidade de estudos futuros em diversas áreas, entre as quais:

- comparação dos resultados apresentados com outras técnicas de aprendizagem;
- aumento do tamanho da amostra de empresas e funcionários de forma a garantir que tais resultados não são pontuais, assim como detalhar o estudo para áreas ou setores específicos;
- verificação de se a metodologia obtém resultados positivos também relativamente a outras ameaças.

REFERÊNCIAS

ALENCAR, G. D.; QUEIROZ, A. A. L.; DE QUEIROZ, R. J. G. B. Insiders: análise e possibilidades de mitigação de ameaças internas. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 3, artigo 6, set-dez, 2013.

ALEXANDRIA, J. C. S. Gestão da segurança da informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. 2009. Tese - Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009.

ARAUJO, E. E. A vulnerabilidade humana na segurança da informação. 2005. Monografia – Faculdade de Ciências Aplicadas de Minas, Uberlândia, 2005.

BOCK, A. M. B.; FURTADO, O.; TEIXEIRA, M. L. T. *Psicologias:* uma introdução ao estudo de psicologia - conforme a nova ortografia. São Paulo: Saraiva, 2009.

CARRARA, K. (Org.). *Introdução à psicologia da educação:* seis abordagens. São Paulo: Avercamp, 2004.

CARRARA, K. *Behaviorismo radical:* Crítica e metacrítica. São Paulo: UNESP, 2005.

COMPUTERWORLD.PT. Especialistas de segurança revelam ameaças à segurança em 2010. ComputerWorld Portugal, 2010. Disponível em: http://www.computerworld.com.pt/2010/01/04/especialistas-de-seguranca-revelam-ameacas-a-seguranca-em-2010/. Acesso em: 30/07/2013.

CONTOS, B. T. *Enemy at the Water Cooler:* real-life stories of insider threats and enterprise security management countermeasures. EUA: Editora Elsevier Science, 2006.

CUNHA, R. Treinando macacos e educando pessoas. Monografia – Fundação Getúlio Vargas, Belo Horizonte, 2007.

GUALBERTO, E. S.; SOUSA JR, R. T.; DEUS, F. E. G.; DUQUE, C. G. Info-SecRM: uma abordagem ontológica para a gestão de riscos de segurança

da informação. In: Simpósio Brasileiro de Sistemas de Informação, 8., São Paulo. *Anais...* Universidade de São Paulo: SBC, 2012.

JAGATIC, T. N.; JOHNSON, N. A.; JAKOBSSON, M.; MENCZER, F. Social phishing. *Communications of the ACM*, v. 50, n. 10, p. 94-100, Oct 2007. http://dx.doi.org/10.1145/1290958.1290968

LUNA, S. V. A crise na educação e o behaviorismo. Que parte nos cabe nela? Temos soluções a oferecer? In: CARRARA, K. (Org.). *Educação, universidade e pesquisa*. São Paulo: Unesp, 2001.

MARCIANO, J. L.; MARQUES. M. L. O enfoque social da segurança da informação. *Ciência da Informação*, *Brasília*, v. 35, n. 3, p. 89-98, Dezembro, 2006. http://dx.doi.org/10.1590/S0100-19652006000300009

MICROSOFT. Security Intelligence Report, Volume 9. Microsoft, 2010. Disponível em: http://www.microsoft.com/security/sir/. Acesso em: 30/06/2013.

MICROSOFT. Security Intelligence Report, Volume 14. Microsoft, 2013. Disponível em: http://www.microsoft.com/security/sir/. Acesso em: 30/06/2013.

MITNICK, K. D.; SIMON, W. L. *A arte de enganar*, São Paulo: Pearson, 2003.

MOORE, T.; CLAYTON, R.; ANDERSON, R. The economics of online crime. *Journal of Economic Perspectives*, v. 23, n. 3, p. 3-20, Summer, 2009. http://dx.doi.org/10.1257/jep.23.3.3

NAKAMURA, E. T.; DE GEUS, P. L. *Segurança de redes em ambientes corporativos*. São Paulo: Novatec, 2007.

PANDA. 10 leading security trends in 2011. Panda Security, 2011. Disponível em: http://press.pandasecurity.com/news/10-leading-security-trends-in-2011/. Acesso em: 28/06/2013.

RAMOS, I. Q. Contribuição da Ciência da Informação para criação de um plano de segurança da informação. 2007. Dissertação – Centro de Ciências Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas, 2007.

RIGON, E. A.; WESTPHALL, C. M. Modelo de avaliação da maturidade da segurança da informação. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 1, artigo 3, jan-mai, 2013.

ROSE, J. A. Análise comportamental da aprendizagem de leitura e escrita. *Revista Brasileira de Análise do Comportamento / Brazilian Journal of Behavior Analysis*, v. 1, n. 1, p. 29-50, 2005.

SHAY, R.; KOMANDURI, S.; KELLEY, G. K.; LEON, P. G.; MAZUREK, M. L.; BAUER, L.; CHRISTIN, N.; CRANOR, L. F. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In: Symposium on Usable Privacy and Security, 6., Redmond - EUA. *Anais...* Carnegie Mellon University, 2010.

SONI, P.; FIRAKE, S.; MESHRAM, B. B. A phishing analysis of web based systems. In: International Conference on Communication, Computing & Security. *Anais...* National Institute of Technology Rourkela: ACM, 2011.

SULLIVAN, R. J. The changing nature of U.S. card payment fraud: issues for industry and public policy. In: Workshop on the Economics of Information Security, 9., Cambridge - EUA. *Anais...* Harvard University, 2010.

TOURINHO, E. Z. Notas sobre o behaviorismo de ontem e de hoje. *Psicologia: Reflexão e Crítica*, v. 24, n. 1, p. 186-194, 2011. http://dx.doi.org/10.1590/S0102-79722011000100022