AMEAÇAS DE ENGENHARIA SOCIAL À SEGURANÇA DA INFORMAÇÃO: FOCO EM PHISHING E PRETEXTING

THREATS OF SOCIAL ENGINEERING TO INFORMATION SECURITY: FOCUS ON PHISHING AND PRETEXTING

Celso Tadeu Manduca Ferreira Filho – celso.manduca@hotmail.com
Lucas Oukus Corcovia – lucas.corcovia1@gmail.com
Luiz Otávio Zanelato de Lima – luiz.zanelato@outlook.com
Renato dos Santos Alves – Renato.jcam@gmail.com
Faculdade de Tecnologia de Taquaritinga (FATEC) – São Paulo – Brasil

RESUMO

A Informação é tida como o maior bem de uma organização nos dias de hoje, por essa razão há uma necessidade crescente de protegê-la. Além disso, pessoas comuns são alvos de ataques de criminosos virtuais, que agem com o objetivo de roubar suas informações para poder aplicar um possível golpe de engenharia social. Por isso, o presente trabalho tem como objetivo expor o que é a engenharia social e sua relação com a segurança da informação, evidenciar os ataques mais comuns de engenharia social, esclarecer as ameaças de *Phishing* e *Pretexting* e apresentar métodos de prevenção a essas ameaças de engenharia social. Para a realização deste artigo, foram feitas revisões bibliográficas e consultas online acerca do tema. Atualmente, é possível notar que os ataques de engenharia social são frequentes, principalmente as ameaças de *Phishing* e *Pretexting*, gerando vulnerabilidade a segurança da informação. Logo, sugere-se técnicas, métodos e conscientização para que os usuários de sistemas de informação possam investigar e reconhecer um ataque desta natureza.

Palavras-chave: Engenharia Social. Phishing. Pretexting. Segurança da Informação.

ABSTRACT

Nowadays, information is considered as the greatest asset of an organization, so there is a significant need to protect it. In addition, ordinary people are targeted by virtual criminals' attacks, that act with the goal to steal their information, so they can apply a possible social engineering scam. Therefore, the present work aims to expose what is social engineering and its relationship with information security, to highlight the most common social engineering attacks, to clarify the threats of *Phishing* and *Pretexting* and to present methods of prevention to these threats of social engineering. For the accomplishment of this article, bibliographical reviews and online consultations on the subject were made. Currently, it is possible to note that social engineering attacks are frequent, especially *Phishing* and *Pretexting* threats, generating vulnerability to information security. Therefore, techniques, methods and awareness are suggested to users of information systems can investigate and recognize an attack of this nature.

Keywords: Social Engineering. Phishing. Pretexting. Information Security.

1 INTRODUÇÃO

O surgimento dos computadores e de sua interconexão em redes permitiu uma maior capacidade de processamento e de distribuição das informações. A Internet é a rede mundial de computadores que propicia uma maior rapidez, eficiência, aumento na produção e transmissão de dados. (GANDINI; SALOMÃO; JACOB, 2002).

Com o passar do tempo, a sociedade se torna cada vez mais dependente dos computadores e das redes, por conta dos benefícios oferecidos pela alta tecnologia que cresce em grande escala. Devido a isso, segundo Marciano e Marques (2006), várias formas de ameaças, tanto físicas quanto virtuais, se proliferam neste universo, comprometendo seriamente a segurança das pessoas, das informações e das transações que as envolvem. A Informação pode ser considerada um dos maiores patrimônios de uma organização nos dias atuais e, por conta disso, há uma necessidade crescente de protegê-la. (MOREIRA, 2013).

Marciano e Marques (2006) citam que a Tecnologia da informação é capaz de apresentar parte da solução para a segurança da informação não sendo, contudo, capaz de resolver. Com isso, é possível afirmar que não existem sistemas totalmente seguros, mas através da segurança da informação, há meios de reduzir esses riscos.

Embasado em trabalhos de investigação já publicados, o presente artigo se propõe a apresentar as ameaças de Engenharia Social. Este, busca contribuir para a identificação de regras e procedimentos para mitigar os riscos operacionais no uso de Tecnologias de Informação e Comunicação para o âmbito da segurança da informação.

2 SEGURANÇA DA INFORMAÇÃO

Entende-se por informação qualquer conteúdo ou conjunto de dados com valor para determinada organização ou pessoa. De acordo com Silva e Stein (2007), em dias atuais, a segurança da informação se tornou um problema na sociedade moderna, desde grandes empresas até indivíduos comuns, pois todos têm o direito de esperar que seus dados privados sejam mantidos em segurança e disponibilizados apenas a pessoas de seu interesse.

De acordo com Santos (2009), a principal ameaça para qualquer segurança é o ser humano, pois todo processo de segurança se inicia e termina em um usuário do sistema. Com

isso, adotar um comportamento defensivo pode ser considerado uma questão de sobrevivência na era digital. O grande desafio da segurança, portanto, é desenvolver a cultura sobre os riscos deste novo mundo, cada vez mais real.

Com o avanço da tecnologia, as empresas que querem se manter cada vez mais competitivas são obrigadas a realizar investimentos maciços em tecnologia da informação. Entretanto, os esforços para promover a proteção das informações têm sido direcionados aos recursos físicos e lógicos, tornando-as, aparentemente, menos vulneráveis. (SILVA FILHO, 2009).

Conforme afirmam Laureano e Moraes (2005), nem toda informação é crucial a ponto de merecer cuidados especiais. Por outro lado, uma determinada informação pode ser vital mesmo que não seja percebido. Os autores classificam a informação organizacional de acordo com o seu nível de sigilo, seguindo a hierarquia: pública, interna, confidencial e secreta.

Portanto, se faz necessário promover dentro da organização uma cultura de segurança e assegurar boas práticas. Também é necessário a utilização de políticas de segurança da informação, padronização de procedimentos, aplicação de mecanismos de segurança, dentre outros. (SIEWERT, 2008).

3 ENGENHARIA SOCIAL

Em definição, engenharia social é uma técnica de utilizar a influência e a habilidade de enganar pessoas para persuadi-las, a fim de obter informações sigilosas com ou sem o uso de recursos tecnológicos, explorando a natureza humana, geralmente com a intenção de induzir o alvo a entregar suas senhas ou demais informações confidenciais, de natureza pessoal ou financeira (MITNICK, 2005).

Para Freitas (2018), Carvalho e Galvão (2015), a engenharia social é a aplicação de conhecimentos de um modo sociável de acordo com os anseios humanos para obter informações. Nota-se também que é a arte de manipular as pessoas visando contornar dispositivos de segurança.

Ou seja, de acordo com Alves (2010), o ponto mais importante a ser protegido consiste no fator humano, e que este tem sido deixado em segundo plano, quando deveria receber mais atenção. Os atacantes, sabendo dessa fraqueza, exploram cada vez mais este fator através da engenharia social.

Segundo Braga (2011), a engenharia social pode parecer algo tolo e que afeta somente o usuário leigo, mas, na verdade, é uma das maiores ameaças à segurança da informação na atualidade. Possivelmente, o fator humano jamais será removido dos sistemas computacionais, por isso sempre existirá a possibilidade de um ataque desse tipo.

3.1 Principais técnicas nos ataques

De acordo com Cialdini (2001), pode-se classificar as principais técnicas de ataque de engenharia social como:

- Retribuição: o ser humano, por natureza, sente necessidade de retribuir um favor que lhe tenha sido feito. Quando isso acontece, sente-se um sentimento de dívida para com a pessoa que nos prestou um favor e isso pode ser explorado pelo engenheiro social, resultando em trocas desiguais de favores ou informações pelo sentimento de culpa;
- Prova Social: é uma condição que pode ser usada como uma forma eficaz de influência em duas condições específicas: o primeiro é a incerteza, pois quando nos encontramos neste estado, somos mais propensos a olhar para o comportamento dos outros para descobrir o que fazer. A segunda é a semelhança, pois as pessoas são mais propensas a seguir o comportamento dos outros com quem se identificam;
- Simpatia: as pessoas tendem a ser mais sensíveis com pessoas que possui admiração. Os investigadores descobriram que a atratividade ou similaridade são fatores que podem influenciar. Quanto mais à vontade e amigável a vítima for com o atacante, maior é a probabilidade de a vítima fornecer a informação que o atacante pretende;
- Autoridade: quando se demonstra um determinado poder pela utilização de cargos, por natureza, o ser humano tende a responder afirmativamente a pedidos ou ordens de uma figura autoritária, por medo de repreensão ou pela esperança de uma recompensa;
- Escassez: em certos casos, a vítima pode se sentir atraída por ofertas e por pensar ser uma das poucas pessoas que irá possuir um item de valor; contudo, não imagina que possa estar enviando os seus dados pessoais à um engenheiro social através de uma página web falsa.

3.2 Principais fatores de ataque

Lively (2003), baseando-se nas seis condições humanas descritas por Cialdini (2001), cita os seguintes pontos de ataque explorados pelos engenheiros sociais:

- Descuido: é uma das principais falhas responsável pelo não cumprimento das medidas de segurança. A vítima acaba cometendo um ato irracional, auxiliando o engenheiro social principalmente na fase de planejamento do ataque;
- Zona de Conforto: o ser humano, em zona de conforto, encontra-se num estado mais relaxado e confortável, o que torna o seu desempenho limitado. Esse estado promove uma redução na capacidade de percepção da ameaça pela vítima, podendo ser explorado pelo atacante para a concretização de seus objetivos;
- Utilidade: por natureza, o ser humano sente necessidade em ser útil. O engenheiro social explora esta condição transmitindo à vítima a ideia de que necessita do seu apoio, se passando por uma pessoa com a necessidade de assistência, tentando dessa forma obter a informação de que necessita para atingir o objetivo, ou que poderá ser útil para o desenvolvimento do ataque;
- Medo: a vítima pode se sentir pressionada por alguém que, através da sua atitude e da forma como se apresenta, transmite a ideia de autoridade. O ser humano sob pressão do medo reduz a sua capacidade de desempenho e de ação.

4 ATAQUES COMUNS DE ENGENHARIA SOCIAL

Um engenheiro social experiente pode ter acesso a praticamente qualquer informação alvo usando as estratégias e táticas da sua habilidade. (MITNICK; SIMON 2003).

Os ataques mais comuns utilizam-se das técnicas mais simples como “Vasculhas no Lixo” na busca de informações sigilosas, até as mais sofisticadas. Nas subseções seguintes são delineados os tipos de ataques mais comuns de engenharia social.

4.1 Baiting

Neste tipo de ataque o engenheiro social se aproveita da curiosidade e ganância de suas vítimas, recorrendo ao uso de dispositivos físicos de armazenamento de dados como *CD-ROM*, *DVD*, *USB Flash Drives*, *HD*, disquetes, entre outros. Estes dispositivos são infectados pelo engenheiro social e são disponibilizados para as suas vítimas; por exemplo, ele pode deixar um *USB Flash Drive* esquecido num local visível para que atraia a atenção da vítima. Ao introduzir a unidade infectada no posto de trabalho, a vítima infecta o seu computador, e potencialmente toda a rede, expondo a empresa a riscos desconhecidos. (BUETLER, 2009).

4.2 Shoulder Surfing

Shoulder Surfing é uma técnica de observação direta e eficaz de obtenção de informações porque depende apenas da proximidade física entre o atacante e a vítima, observando diretamente a primeira "sobre o ombro" o que a segunda está a executar. Trata-se de uma técnica muito utilizada em espaços com várias pessoas. Esta técnica poderá ser desenvolvida através da utilização de alguns equipamentos, tais como, binóculos ou outros dispositivos que aumentem o alcance de visão. (LONG, 2008).

4.3 Falhas Humanas e Vasculhas no Lixo

O ser humano possui várias vulnerabilidades que são exploradas pelos engenheiros sociais, tais como: confiança, medo, curiosidade, instinto de querer ajudar, culpa, ingenuidade, entre outros. (RAFAEL, 2013).

Segundo Alves (2010), vasculhar o lixo da empresa é um dos grandes métodos usados por esses criminosos para conseguirem acessar informações sensíveis, pois muitas empresas não se preocupam com o destino do seu lixo ou sequer utilizam máquinas fragmentadoras ou trituradoras de papel para que os diversos documentos sigilosos não sejam recuperados por pessoas mal-intencionadas.

4.5 Internet e Redes sociais

De acordo com Rafael (2013), atualmente muitas informações podem ser coletadas através da internet e redes sociais sobre o alvo. Quando um engenheiro social precisa conhecer melhor seu alvo, esta técnica é utilizada, iniciando um estudo no site da empresa para melhor entendimento, pesquisas na internet e uma boa consulta nas redes sociais na qual é possível encontrar informações interessantes de funcionários da empresa, cargos, amizades, perfil pessoal, entre outros.

5 PHISHING E SEUS TIPOS DE ATAQUE

Phishing é um tipo de golpe utilizando-se de e-mails fraudulentos ou textos, ou sites falsos visando conseguir obter as informações pessoais valiosas, tais como suas identificações de *login* e senha, utilizando para roubar suas identidades ou dinheiro ou ambos. (FTC, 2017).

Utilizando-se de empatia, faz parecer que o ataque não seja falso, dando a sensação de segurança, falsificando logotipos e se passando por empresas legítimas e de credibilidade, ou fingindo ser alguém próximo da família. (FTC, 2017).

Existem vários tipos de ataques por *phishing*, dentre eles podemos destacar os seguintes:

- Phishing fraudulento: É o tipo mais comum de *phishing*. Consiste no invasor tentar obter informações confidenciais da vítima. Os invasores usam da informação para roubar dinheiro ou para iniciar novas vítimas. Um *e-mail* falso de um banco pedindo para clicar em um *link* e verificar os detalhes da sua conta é um exemplo de *phishing* fraudulento. (CISCO, 2018).
- Spear phishing: O *spear phishing* tem como alvo indivíduos específicos. Geralmente são realizadas pesquisas das vítimas nas redes sociais e em outros sites, podendo assim personalizar a comunicação, fazendo parecer mais autêntico. Geralmente é o primeiro passo usado para penetrar nas defesas das empresas para realizar um ataque direcionado. (CISCO, 2018).
- Whaling: O golpista identifica a vítima como sendo um "peixe grande", como um *CEO* por exemplo. Ele gastará o seu tempo arquitetando as melhores táticas e o momento oportuno para atacá-lo, inclusive gera-se uma preocupação extra, pelo alvo ser executivo e ter alto nível de acesso a informações sigilosas da empresa. (CISCO, 2018).
- Pharming: É semelhante ao *phishing* fraudulento, a diferença é que o atacante envia ao usuário um site falso com intensão de roubar as informações de *login* e senha. A vítima nem precisa clicar no *link* malicioso, pois mesmo que o usuário digite o endereço correto, o site será redirecionado ao site falso, devido a instalação de um programa que altera o *DNS* (*Domain Name System*) do site. (CISCO, 2018).

6 PRETEXTING NA ENGENHARIA SOCIAL

De acordo com Baer (2008 apud SILVA, 2013), a técnica de *pretexting* consiste na obtenção de informação sob um falso pretexto, indo além de uma simples mentira. É criado um cenário onde a vítima não se sinta desconfortável ou suspeite de que seja uma fraude, assim ela

executara a ação que o golpista deseja, que em uma outra circunstância não faria. Na maioria das vezes, o golpista se passa uma autoridade legítima, que transmite confiança para a vítima.

Os engenheiros sociais que fazem uso de *pretexting* tem como características as pesquisas, pois será necessário desenvolver muitos pretextos diferente ao longo de sua carreira, pois boas informações coletam técnicas que podem tanto fazer ou quebrar um pretexto, por exemplo, ser capaz de imitar o representante de suporte técnico perfeito torna-se inútil quando o alvo não faz uso de suporte externo. (SOCIAL-ENGINEERS, 2018).

Pretexting pode ocorrer por telefone, onde o impostor finge ser outra pessoa a fim de obter acesso a registros de chamadas ou outras informações de conta da vítima. Embora o *pretexting* possa envolver impostores profissionais, existem casos onde envolve conhecidos da vítima, por exemplo um ex-cônjuge ou membro da família. (T-MOBILE, 2018).

Existem casos onde *pretexting* pode ser benéfico, como o site *perverted-justice* expõe, trata-se de um grupo de pessoas que agem como menores de idade a fim de atrair a atenção de pedófilos e seduzi-los, para que possam ser presos. (SOCIAL-ENGINEERS, 2018).

7 ESTUDO DE CASO

Em 2016, Walter Stephan, CEO da *FACC* (*Fischer Advanced Composite Components*), que fabrica e projeta de peças de avião para as empresas Boeing e Airbus foi vítima de *phishing* por *e-mail*, onde o presidente da empresa havia pedido para realizar várias transferências secretas no montante de cerca de US$ 56,79 milhões, assim ele fez e foi imediatamente demito. Logo após o incidente, a diretoria envolveu o Departamento de Investigação Criminal e iniciou uma investigação, constatando que as atividades do ataque partiram de fora para dentro da empresa.

Em nota oficial, a empresa comunicou que o departamento de contabilidade financeira da *FACC Operations GmbH* havia sido fraudado com crime cibernético, mas deixaram claro que o dano foi apenas na saída de aproximadamente €50 milhões de fundos líquidos. A infraestrutura de TI (Tecnologia da Informação) da *FACC*, a segurança de dados, os direitos de PI (Propriedade Intelectual) e os negócios operacionais do grupo não foram afetados pelas atividades criminosa. A *FACC* ficou com um prejuízo operacional de € 23,4 milhões, em contrapartida, se não houvesse o incidente, a empresa estaria com um lucro operacional de € 18,6 milhões.

Quando a empresa informou sobre o incidente, suas ações caíram até 38%. Cerca de 20% do valor foi recuperado dos fundos nos bancos beneficiários, mas o restante do dinheiro foi perdido em contas da Eslováquia e Ásia.

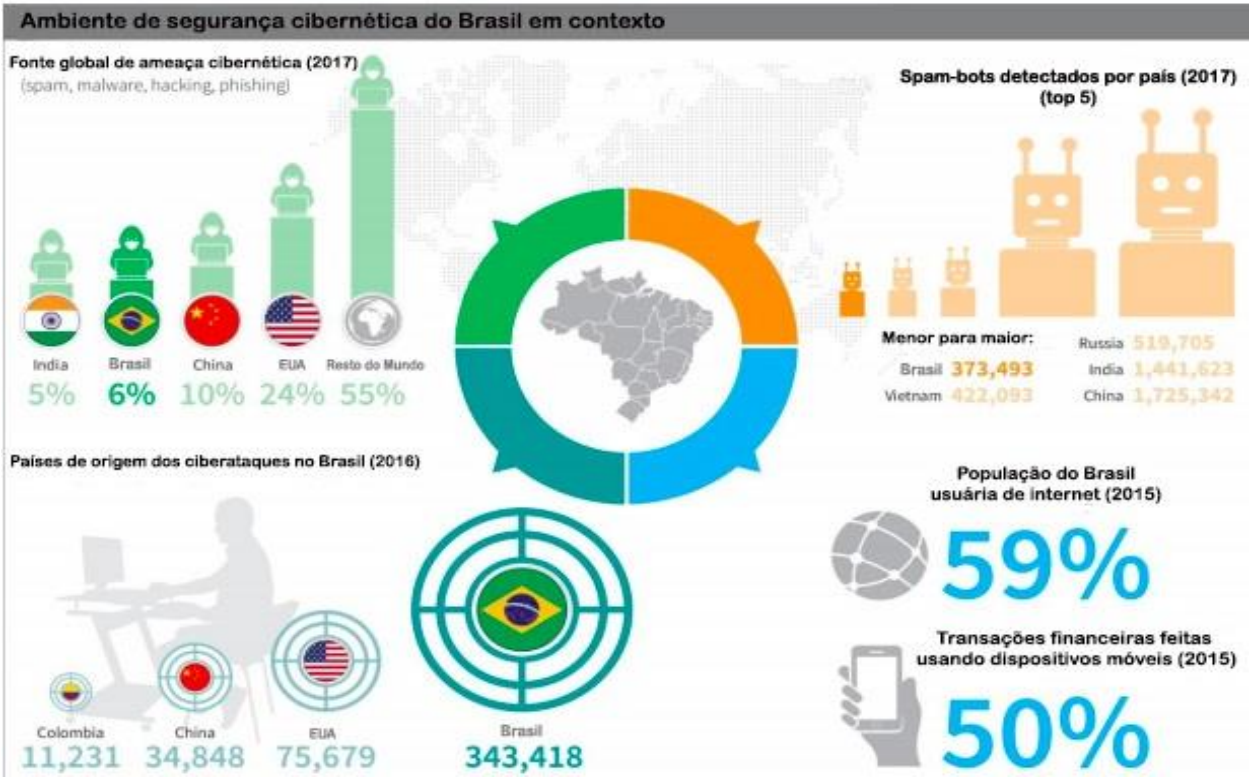
Stephan disse aos investidores que a fraude não foi por falha do serviço de internet ou da TI interna da empresa, mas sim por conta de um *e-mail* simulada em seu nome, o que não requer nenhum *hacking*.

A companhia chegou à conclusão de que Stephan violara severamente seus deveres, ainda mais com um caso envolvendo transações para um "falso presidente". O valor de mercado da empresa subiu após a demissão de Stephan do cargo de CEO.

8 O CENÁRIO ATUAL BRASILEIRO

De acordo com estatísticas do governo, crimes digitais têm crescido e se sofisticando no Brasil, afetando usuários casuais, empresa e redes governamentais. (JANES, 2017).

Figura 1 – Ambiente de Segurança cibernética do Brasil em contexto.



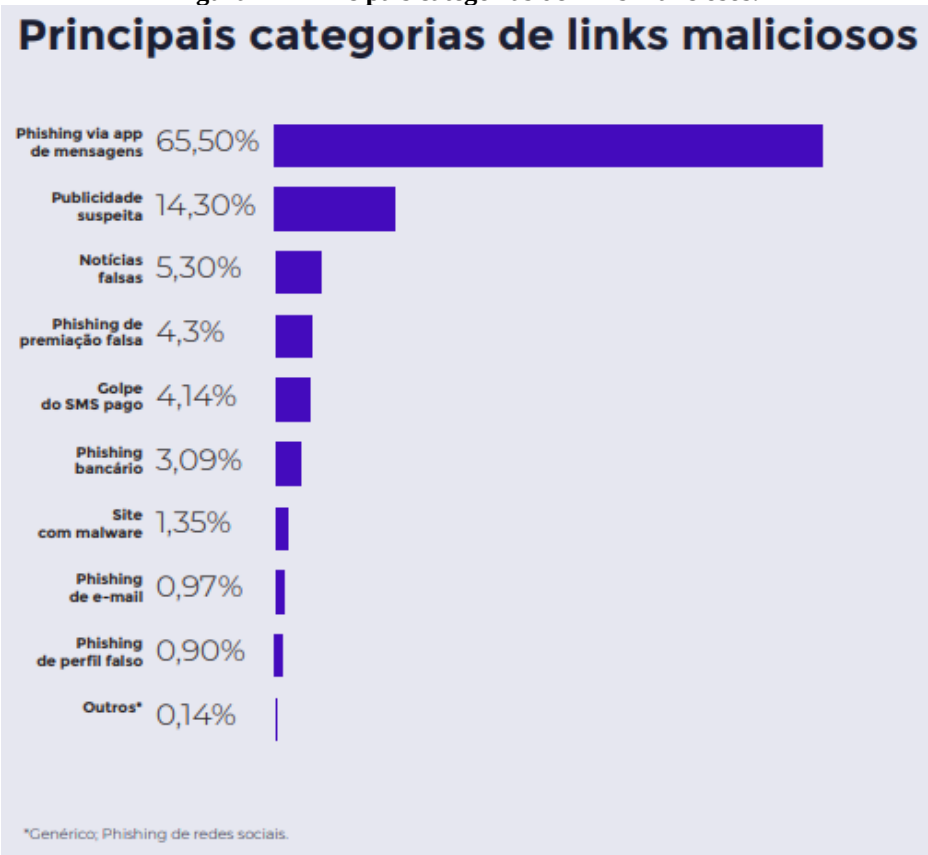
Fonte: Brazil's cyber security evironment in context. (IHS Markit)

O Brasil frequentemente tem estado no topo do ranking mundial de crimes digitais, principalmente no que diz respeito a *botnets*, fraudes bancárias e *malware* financeiro. Em 2014 foi classificado pela empresa de segurança cibernética Kaspersky Lab como a primeira do mundo em ataques de *malware* bancário, com quase 300.000 usuários comprometidos.

Como pode ser visto na figura 1, segundo o recente relatório da Symantec, uma empresa de segurança cibernética, o Brasil aparece em terceiro lugar em termos de fontes de *malware*, *bots*, *spam* e ataques de *phishing*, com 5,4% das detecções de ameaças mundiais originadas no país. (JANES, 2017).

A quantidade de brasileiros que usa a internet pulou de menos de 3% da população em 2000 para mais de 66% em 2016. O crescimento de ataques registrados subiu acentuadamente, de menos de 10 mil em 1999, início do acompanhamento dos registros, para mais 1 milhão relatado em 2014, ano que o Brasil sediou a Copa do Mundo FIFA. (JANES, 2017).

Figura 2 – Principais categorias de links maliciosos.



Fonte: Relatório da Segurança Digital no Brasil Primeiro Trimestre 2018. (dfndr lab)

A figura 2, referente ao relatório da segurança digital no Brasil do dfndr lab, realizado no primeiro trimestre de 2018, aponta que os brasileiros em média clicam em 8 *links* maliciosos

por segundo. Ainda, é possível analisar que a grande maioria dos *links* são do tipo *phishing*, chegando a 56,9 milhões de *ciberataques*, impactando 1,9 milhões de pessoas. (PSAFE, 2018).

9 MEDIDAS DE SEGURANÇA

Para evitar ser vítima de *phishing*, existem várias medidas que podem ser adotadas, dentre elas:

- Cautela ao abrir anexos ou ao clicar em *links* em *e-mails*: Desconfie se receber *e-mails* de amigos com *links*, pois eles também podem ter sido vítimas e ajudam os criminosos a propagar novos *e-mails* maliciosos, o mesmo vale para instituições financeiras, agencias tarifárias, lojas *online*, companhia aéreas, agências de viagem, entre outros, mesmo porque elaborar um *e-mail* que pareça verídico não é difícil (KASPERSKY, 2015).
- Faça sua própria digitação: Se uma empresa ou organização que você conhece lhe enviar um *link* ou número de telefone, não clique. Use mecanismos de busca para procurar o site ou o número de telefone. Mesmo que um *link* ou número de telefone em um *e-mail* seja parecido com o real, os criminosos podem ocultar o destino verdadeiro (FTC, 2017).
- Faça a ligação se não tiver certeza: Não responda a *e-mails* que solicitem informações pessoais ou financeiras. Os "*phishers*", como são chamados os praticantes do golpe de *phishing*, usam táticas de pressão e atacam o medo. Se você acha que uma empresa, um amigo ou um membro da família realmente precisa de suas informações pessoais, atenda ao telefone e ligue para eles usando o número no site ou no catálogo de endereços, não o do *e-mail* (FTC, 2017).
- Autenticação de dois fatores: A autenticação de dois fatores exige sua senha e uma informação adicional para fazer *login* na sua conta. A segunda parte pode ser um código enviado para o seu telefone ou um número aleatório gerado por um aplicativo ou um *token*. Isso protege sua conta mesmo que sua senha seja comprometida (FTC, 2017).
- Segunda autenticação: Como precaução extra, você pode optar por mais de um tipo de segunda autenticação (por exemplo, um *PIN*) caso seu método principal (como um telefone) esteja indisponível (FTC, 2017).
- Segurança atualizada: Use o *software* de segurança em que você confia e certifique-se de configurá-lo para atualização automática (FTC, 2017).
- Verifique o *link* antes de abrir: Se possuir algum problema ortográfico, tenha certeza, criminosos estão tentando enganá-lo com uma página falsa (KASPERSKY, 2015).

- Reportar tentativa de *phishing*: Ao descobrir uma tentativa de *phishing*, deve-se reportar a instituição que está sendo usada como isca e alertar outras. Isto ajudará a reduzir a tentativa do golpe e colaborará para a prisão dos criminosos (KASPERSKY, 2015).
- Não acessar contas de bancos em redes *Wi-Fi* públicas: Evite acessar sites financeiros em redes públicas, cafés ou na rua. Pode acontecer dessas conexões serem criadas pelos criminosos, com intuito de imitar endereços de sites durante a conexão, e redirecionar o tráfego de dados para sites falsos. É aconselhado utilizar dados móveis da operadora de telefonia ou aguardar até ter uma conexão de internet conhecida e confiável (KASPERSKY, 2015).

10 CONSIDERAÇÕES FINAIS

Tratar engenharia social de maneira a esclarecer o que realmente é essa prática, relacionar os principais ataques de engenharia social, definir o que são ameaças de *Phishing* e *Pretexting*, formas de prevenção a essas ameaças, relacionar essas a um estudo de caso, realizar uma análise da situação atual brasileira em relação a ataques cibernéticos e indicar formas de proteção a informação contra possíveis ataques foram discutidos neste artigo.

Como discutido, o engenheiro social usufrui de falhas humanas para conseguir informações, uma vez que a maioria dos usuários comuns e alguns profissionais internos das organizações ainda não são conhecedores da engenharia social, que acabam apresentando atitudes que põem em risco as suas informações ou informações sigilosas da própria empresa.

Há vários meios de ataque de engenharia social e para cada meio, muitas técnicas usadas em casos diversos, sempre sondando alguma fraqueza de uma pessoa ou de um grupo de pessoas. A maioria dos ataques consistem em obter informações privilegiadas ludibriando usuários de um certo sistema com persuasão, se passando por outra pessoa, adquirindo carisma e confiança da vítima.

A maior parte das organizações e usuários comuns possuem ferramentas defensivas contra ataques de diversos tipos, os quais requerem o usuário informar não apenas seu *login* e a senha, tal como apurar a existência de vírus em arquivos, entre outros. Entretanto, os sistemas recentes são suscetíveis a ataques considerados não técnicos, que são consequentes da engenharia social.

Portanto, a engenharia social pode ser utilizada tanto de forma benéfica quanto maléfica, dependerá apenas das decisões que o engenheiro social irá tomar para com essas informações.

REFERÊNCIAS

ALVES, Cássio B. **Segurança da informação vs. Engenharia Social: Como se proteger para não ser mais uma vítima.** Disponível em: <http://monografias.brasilescola.com/computacao/seguranca-informacao-vs-engenhariasocial-como-se-proteger.htm/>. Acesso em 13 set. 2018.

BAER, M. H. Corporate Policing and Corporate Governance: **What Can We Learn from Hewlett-Packard´s Pretexting Scandal.** University of Cincinnati Law Review, Corporate Law Symposium, 2008.

BRAGA, P. H. C. **Técnicas de Engenharia Social**. UFRJ, Rio de Janeiro, 15 fev. 2011. Disponível em: <https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_social.pdf>. Acesso em: 26 set. 2018.

BUETLER, I. **Social Engineering Test cases. From Compass.** Disponível em: < https://www.hacking-lab.com/misc/downloads/Social_Engineering_V2.0.pdf >. Acesso em 15 set. 2018.

CARVALHO, C.; GALVÃO, A. **Engenharia Social: Uma Análise de Ameaças e Cuidados aos Funcionários das Agências Bancárias de Santarém e Itaituba – Pará**. 2015. Disponível em <http://iespes.edu.br/revistaemfoco/index.php/Foco/article/view/61>. Acesso em 26 ago. 2018.

CIALDINI, R. B. **Influence: Science and Practice**. USA: Ally & Bancon. 2001.

CISCO. **O que é Phishing?**. 2018. Disponível em: <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>. Acesso em: 14 set. 2018.

CSO. **CEO fired after 'fake CEO' email scam cost firm $47m**. 2018. Disponível em: <https://www.cso.com.au/article/600535/ceo-fired-after-fake-ceo-email-scam-cost-firm-47m/>. Acesso em: 15 set. 2018.

FREITAS, C. M. de. **Segurança da Informação: Engenharia Social nas organizações**. 2018. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 03, Ed. 04, Vol. 04, pp. 116-124, ISSN:2448-0959. 2018.

FTC. **Phishing**. 2018. Disponível em: <https://www.consumer.ftc.gov/articles/0003-phishing>. Acesso em: 14 set. 2018.

GANDINI, J. A. D.; SALOMÃO, D. P. S.; JACOB, C. **A segurança dos documentos digitais**. 2002. Disponível em: <https://jus.com.br/artigos/2677/a-seguranca-dos-documentos-digitais>. Acesso em 07 set. 2018.

JANES. **Brazil struggles with effective cyber-crime response**. 2017. Disponível em: <https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf>. Acesso em 17 set. 2018.

KASPERSKY. **10 dicas para se proteger do phishing.** 2015. Disponível em: <https://www.kaspersky.com.br/blog/phishing-ten-tips/5819/>. Acesso em: 15 set. 2018.

KNOWBE4. **CEO Fraud Costs Boeing Vendor 54 MillionDollars.** 2018. Disponível em: <https://blog.knowbe4.com/ceo-fraud-costs-boeing-vendor-54-million-dollarsinosas>. Acesso em: 15 set. 2018.

LAUREANO, M. A. P.; MORAES, P. E. S. **Segurança como estratégia de gestão da informação**. 2005. Disponível em: <http://www.mlaureano.org/projects/seguranca/economia_tecnologia_seguranca.pdf>. Acesso em: 07 set. 2018.

LIVELY, C. E. Jr.; **Psychological Based Social Engineering**. SANS Institute. 2003. Disponível em: <http://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780>. Acesso em: 01 set. 2018.

LONG, J. **No Tech Hacking.** Syngress Publishing, Inc, 2008.

MARCIANO, J. L.; MARQUES, M. L. **O Enfoque Social da Segurança da Informação**. Brasília, 2006. Disponível em: <http://revista.ibict.br/ciinf/article/view/1116/1250>. Acesso em: 02 set. 2018.

MITNICK, K., SIMON, W. **A Arte de Invadir: As Verdadeiras Histórias por Trás das Ações de Hackers, Intrusos e Criminosos Eletrônicos**. São Paulo: Person, 2005.

MITNICK, K., SIMON, W. **A Arte de Invadir: Ataques de Hackers: Controlando o fator humano na segurança da informação**. São Paulo: Person, 2003.

MOREIRA, A. **A importância da segurança da informação**, 2013. Disponível em: <http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao>. Acesso em: 25 ago. 2018.

PSAFE. **Relatório da Segurança Digital no Brasil Primeiro trimestre – 2018.** 2018. Disponível em <https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/05/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-Primeiro-trimestre-de-2018-1.pdf>. Acesso em 18 set. 2018.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL: Um Perigo Eminente.** 2003. 11 f. Monografia (Pós-Graduação em Gestão Empresarial e Estratégias de Informática - ICPG. Instituto Catarinense de Pós-Graduação.

RAFAEL, Gustavo de C. **Engenharia Social: as técnicas de ataques mais utilizadas.** Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em 13 set. 2018.

SANTOS, A. H. G. **A história da segurança da informação**. 2009. Disponível em: <http://www.slideshare.net/andrehor/a-histria-da-segurana-da-informao-presentation-902879>. Acesso em: 01 set. 2018.

SANTOS, L. A. F. dos. **Segurança da informação**. UTFPR, Paraná, 2009. Disponível em: <http://www.slideshare.net/luiz_arthur/seguranca-da-informao-introduo>. Acesso em: 25 ago. 2018.

SIEWERT, V. C. **A Constante Evolução Da Segurança Da Informação**. CTAI, Florianópolis, 2008. Disponível em: <https://www.yumpu.com/pt/document/view/16975663/a-constante-evolucao-da-seguranca-da-informacao>. Acesso em: 26 ago. 2018.

SILVA FILHO, A. M. **Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações**. 2009. Disponível em: <http://softwarelivre.org/brasil/entendendo-e-evitando-a-engenharia-social-protegendo-sistemas-e-informacoes>. Acesso em: 05 set. 2018.

SILVA, D. R. P. da; STEIN, L. M. **Segurança da informação: uma reflexão sobre o componente humano**. PUCRS, Porto Alegre, 2007. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410>. Acesso em: Acesso em: 07 set. 2018.

SILVA, Francisco José Albino Faria Castro. **Classificação Taxonómica dos Ataques de Engenharia Social**. 2013. 132 f. Dissertação (Mestrado em Segurança dos Sistemas de Informação) - Faculdade de Engenharia. Universidade Católica Portuguesa, Sintra.

SOCIAL-ENGINEER. **The Social Engineering Framework**. 2018. Disponível em: <https://www.social-engineer.org/framework/influencing-others/pretexting/>. Acesso em: 14 set. 2018.

T-MOBILE. **Pretexting.** 2018. Disponível em: <https://www.t-mobile.com/responsibility/privacy/fraud-spam/pretexting>. Acesso em: 15 set. 2018.