PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

ATAQUES DE ENGENHARIA SOCIAL SOB A PERSPECTIVA DE ESTUDANTES DE DUAS INSTITUIÇÕES DE ENSINO SUPERIOR DO ESTADO DE SÃO PAULO: ESTUDO DE CASO

SOCIAL ENGINEERING ATTACKS FROM THE PERSPECTIVE OF STUDENTS FROM TWO HIGHER EDUCATION INSTITUTIONS IN THE STATE OF SÃO PAULO: A CASE STUDY

Adriano Ricardo Ruggero[1]

1- Engenheiro da Computação pelo Centro Regional Universitário Espírito Santo do Pinhal, especialista em Redes de Computadores pela UNICAMP e em Segurança da Informação pelo Centro Universitário Estácio Ribeirão Preto. Atualmente é docente da Faculdade de Tecnologia de Itapira e de Mogi Mirim.

Contato: adriano.ruggero@fatec.sp.gov.br

RESUMO

Um dos ativos de maior valor, seja para pessoas ou organizações, é a informação. Torna-se essencial, desta forma, protegê-la contra quaisquer tipos de ameaças. Este artigo realizou uma pesquisa para dimensionar a percepção de estudantes de cursos da área de TI quanto a ataques por meio de engenharia social. Para tal, foi aplicado um questionário a alunos dos seis períodos de duas instituições de ensino de nível superior do Estado de São Paulo. Foi possível observar que uma grande porcentagem dos entrevistados já foi alvo de abordagens deste tipo. Entretanto, boa parte dos respondentes não sabe ou erroneamente acredita saber identificar um ataque de engenharia social. Conclui-se que o fator humano é crucial para a implementação de políticas de segurança e que o conhecimento, por parte das pessoas envolvidas, das técnicas e de como identificar fraudes pode auxiliar a diminuir o sucesso dos ataques.

Palavras Chaves: Segurança. Informação. *Phishing*. Ataque. Engenharia social.

ABSTRACT

One of the most valuable assets, whether for people or organizations, is information. It becomes essential, therefore, to protect it against any kind of threats. This article carried out a survey to measure the perception of IT course students regarding attacks through social engineering. To this end, a questionnaire was applied to students from the six semesters of two higher education institutions in the State of São Paulo. It was possible to observe that a large percentage of respondents have already been the target of

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

approaches of this type. However, most respondents do not know or mistakenly believe they know how to identify a social engineering attack. It is concluded that the human factor is crucial for the implementation of security policies and that the knowledge, on the part of the people involved, of the techniques and of how to identify frauds can help to reduce the success of the attacks.

Keywords: Security. Information. Phishing. Attack. Social engineering.

INTRODUÇÃO

A informação é um ativo e, como qualquer outro, deve ser constantemente protegida para proporcionar a continuidade dos negócios. Contudo, em um mundo cada vez mais conectado, seja de forma impressa, escrita em papel, transmitida eletronicamente ou pelos correios, falada, apresentada em filmes ou armazenada em meios eletrônicos, ela se encontra exposta a um número crescente de ameaças e vulnerabilidades. Garantir a segurança da informação depende da implantação de controles adequados, que incluem políticas, processos, procedimentos, funções de *hardware* e *software* e estruturas organizacionais. Com vistas a garantir a continuidade do negócio e a segurança da organização, tais controles devem ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Entretanto, percebe-se que os investimentos em segurança da informação buscam minimizar os riscos inerentes ao uso dos computadores de maneira técnica, menosprezando a vulnerabilidade mais significativa: o fator humano. O uso da persuasão ou da influência sobre pessoas para obter vantagens, por meio da tecnologia ou não, pode ser definido como engenharia social (MITNICK; SIMON, 2003). Ataques que usam de engenharia social incluem, mas não se limitam a, o envio de mensagens de correio eletrônico que induzem o usuário a baixar e instalar programas maliciosos em seu equipamento, seguir *links* que o direcionam a *sites* fraudulentos ou ludibriá-lo para obter informações sigilosas (PEREIRA; MARTINS, 2014). Contudo, a Norma Brasileira ISSO/IEC 27002, da Associação Brasileira de Normas Técnicas, que traz o código de prática para controles de segurança da informação e orientações sobre políticas para segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013), sequer menciona o termo engenharia social. Reforçando a importância das implantações de políticas de segurança e também da participação ativa dos usuários, Mitnick e Simon (2003, p. 208) fazem a ressalta de que os controles efetivos de segurança são implementados pelo treinamento dos empregados, bem como por políticas e procedimentos bem documentados. Entretanto, é importante observar que as políticas de segurança, mesmo que sejam seguidas religiosamente por todos os empregados, não evitam todos os ataques da engenharia social, esclarecem os autores.

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

Levando-se em consideração o exposto, as hipóteses levantadas foram: qual a percepção dos usuários quanto a ataques de engenharia social? Uma pessoa sem treinamento específico em segurança da informação consegue identificar uma mensagem de correio eletrônico ou um *site* fraudulento?

Com esta ideia em mente, foi realizada uma pesquisa *online* entre estudantes de cursos da área de Tecnologia da Informação de duas instituições de ensino do Estado de São Paulo. O objetivo foi mensurar a proporção de alunos, usuários frequentes de computadores e da *internet*, capazes de reconhecer *sites* e mensagens de correio eletrônico possivelmente fraudulentas, abordagens muito comuns para a prática de ataques de engenharia social.

Dimensionar a proporção de usuários que não estão cientes ou aptos a identificarem ameaças pode ajudar a desenvolver treinamentos em segurança da informação melhores e mais incisivos. Por suporem que os aspectos tecnológicos da segurança da informação já estão sendo tratados por *firewalls* e outras barreiras eletrônicas, as pessoas envolvidas tendem a descuidar-se. A conscientização faz com que cada usuário sinta-se parte da linha de frente que protege a segurança da organização (MITNICK; SIMON, 2003).

DESENVOLVIMENTO

O termo Segurança da Informação pode ser definido como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013). Caiçara Júnior (2008, p. 143) conceitua a Segurança da Informação como um “conjunto de meios, processos e medidas que visam, efetivamente, à proteção empresarial”. Segundo este autor, a segurança da informação objetiva assegurar a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações processadas pela organização. Como explanado por Nakamura e Geus (2007, p. 23), organizações de todos os tipos não podem se dar ao luxo de permanecerem fora do mundo conectado. Porém, seguindo o pensamento dos autores, assim como os processos e tecnologias evoluem, novos ataques e técnicas de invasão também surgem todos os dias, exigindo novas formas de proteção como resposta, o que leva a novas maneiras de se atacar, num ciclo completo e interminável.

Como amostra de alguns tipos de ameaça, citam-se (NAKAMURA; GEUS, 2007): *hackers* (de maneira geral e todas suas subdefinições), *dumpster diving* ou *trashing* (vasculhar o lixo ou a sucata da empresa em busca de informações úteis), ataques de engenharia social (exploração das fraquezas humanas e sociais), ataques físicos (roubo ou furto de equipamentos ou insumos), exploração de informações livres (em *sites* da internet ou redes sociais da empresa), captura de pacotes de rede, *port scanning* (varredura de portas de

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

rede), varredura de vulnerabilidades da rede, ataques de negação de serviço (DoS, DDoS), falhas em aplicativos e/ou sistemas operacionais, entre outros.

Com o intuito de se protegerem de tais ameaças, as empresas se vêm obrigadas a investir em medidas de segurança. Dentre estas, pode-se tomar como exemplo a criação e implementação de uma política de segurança, o uso de *firewalls*, a implantação de um sistema de detecção de intrusão (IDS – *Intrusion Detection System*), o uso de criptografia e política de troca de chaves, adoção de redes privadas virtuais (VPN) e sistemas robustos de autenticação (NAKAMURA; GEUS, 2007, p. 187).

Entretanto, segundo Mitnick e Simon (2003, p. 3),

> "Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis".

Pode-se inferir, ao se ler o texto citado, que independente do que uma empresa fizer ou investir para manter seus ativos (tudo o que deve ser protegido de ataques) ela ainda estará *à mercê* de pessoas mal-intencionadas. Contudo, ainda conforme os autores (p. 4), "citando o consultor de segurança Bruce Schneier, 'a segurança não é um produto, ela é um processo'. Além disso, a segurança não é um problema para a tecnologia — ela é um problema para as pessoas e a direção".

Reforçando a ideia de Nakamura e Geus (2007), Mitnick e Simon afirmam que os especialistas contribuem para a melhoria contínua das tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas. Por sua vez os atacantes investem cada vez mais na exploração do elemento humano da equação. "Quebrar a '*firewall* humana' quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo" (MITNICK; SIMON, 2003, p. 4).

Nesta mesma linha de pensamento, Marcelo e Pereira (2005) afirmam que qualquer instituição, por mais segura que seja, possui um ponto de desequilíbrio, um ponto fraco: o ser humano.

Destas afirmações, podemos depreender que, além de considerar os fatores tecnológicos de segurança, faz-mister atentar aos fatores humanos. Procedimentos de segurança podem falhar devido a reações não adequadas dos usuários. Estes devem entender e aceitar as exigências da segurança. A formalização de um treinamento é uma boa ideia a ser utilizada. Considerar estes

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

fatores diminui a chance de sucessos de ataques baseados em engenharia social (NAKAMURA; GEUS, 2007, p. 195).

Entretanto, ao se observar o espaço dedicado ao fator humano na Segurança da Informação nas obras consultadas, pode-se inferir que ele não é muito levado em consideração. No livro “Segurança de Redes em Ambientes Cooperativos” (NAKAMURA; GEUS, 2007), em seus 14 capítulos, apenas dois citam os usuários como parte integrante do processo da segurança: o capítulo 4 - “Os riscos que rondam as organizações” - relaciona a Engenharia Social como um risco aos ativos da instituição e o capítulo 6 - “Política de segurança” - relata a necessidade de treinamento dos envolvidos. Já o livro “Redes de computadores e a internet: uma abordagem Top-Down” (KUROSE; ROSS, 2010), que dedica um capítulo inteiro apenas à segurança das redes, sequer menciona a importância das pessoas envolvidas nas transações. Outrossim, a obra “Sistemas Integrados de Gestão ERP: uma abordagem gerencial” (CAIÇARA JUNIOR, 2008), que possui um capítulo dedicado inteiramente a política de segurança e trata de maneira muito didática o tema, aborda no citado assunto fatores referentes à contratação, demissão e uso dos equipamentos por funcionários, contratados e terceiros, com rápida referência a treinamentos. Posição diversa encontra-se no livro de Mitnick e Simon (2003) – A arte de enganar: Ataques de *Hackers* - Controlando o fator humano na segurança da informação -, mas esta é uma obra toda dedicada a este tema.

Em segurança da informação, podemos definir a engenharia social como “um conjunto de práticas utilizadas para a obtenção de informações relevantes ou sigilosas de uma organização ou indivíduo, por meio da persuasão, manipulação e influência das pessoas, seja com o uso ou não da tecnologia” (SILVA; ARAÚJO; AZEVEDO, 2013). A tecnologia, neste caso, é apenas um meio, uma ferramenta, para se alcançar os usuários, verdadeiras vítimas do atacante. De acordo com Pereira e Martins (2014), o engenheiro social é uma pessoa que decide explorar a natureza humana ao invés de buscar falhas técnicas em sistemas de informação, geralmente com a intenção de induzir o usuário de tais sistemas a instalar programas maliciosos ou entregar suas senhas ou quaisquer informações confidenciais, de natureza pessoal ou financeira, para uso benéfico – descobrir e relatar falhas, por exemplo, ou não. Para Braga (2011), quando se pensa na prevenção de um ataque a sistemas de informação, pensa-se na correção de falhas técnicas computacionais. Instalar sistemas de *firewall*, antivírus e detectores de programas maliciosos e manter os programas atualizados transmite uma sensação de segurança. Contudo, mesmo políticas de segurança da informação bem elaboradas, um simples deslize de algum usuário pode comprometer todo seu funcionamento. Segundo o autor, esta é uma segunda rota de invasão do sistema: o erro humano. Braga (2011) segue, definindo o erro humano como “todo comportamento inseguro, seja ele um ato contínuo ou fruto de um momento de distração, que pode ser usado por um atacante para que este consiga comprometer um sistema (BRAGA, 2011).

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

Ele ainda afirma que este problema não pode ser corrigido de maneira completa, mas apenas mitigado, e conclui que o fator humano é o elo mais fraco da segurança da informação.

Para tentar compreender a vulnerabilidade das pessoas envolvidas na segurança da informação é necessário entender os motivos que podem levá-las a serem manipuladas ou estarem sujeitas a ataques de engenharia social. Mitnick e Simon (2003, p. 196-198) citam o estudioso Robert B. Cialdini, que apresentou sua pesquisa na revista *Scientific American*, de fevereiro de 2001, resumindo-a em "seis tendências básicas da natureza humana". Conscientemente ou não, os engenheiros sociais as utilizam em suas tentativas de fraude. São elas: autoridade, afabilidade, reciprocidade, consistência, validação social e escassez. Pessoas tendem a acatar solicitações de outros em cargos ou posições relevantes (autoridade); atender pedidos de quem se passa por amável, agradável ou com interesses em comum (afabilidade); cumprir solicitações com a promessa de receber algo em troca (reciprocidade); acatar pedidos após comprometer-se ou adotar uma causa publicamente (consistência); cooperar quando tal fato parece estar de acordo com o pensamento da maioria (validação social) ou aceitar cooperar imaginando que algo está em falta, que outras pessoas estão disputando-o ou que estará disponível apenas por um curto período de tempo (escassez) (MITNICK; SIMON, 2003, p. 196-198). Segundo os autores, compreender como as pessoas podem ser influenciadas ajuda a perceber e evitar um ataque.

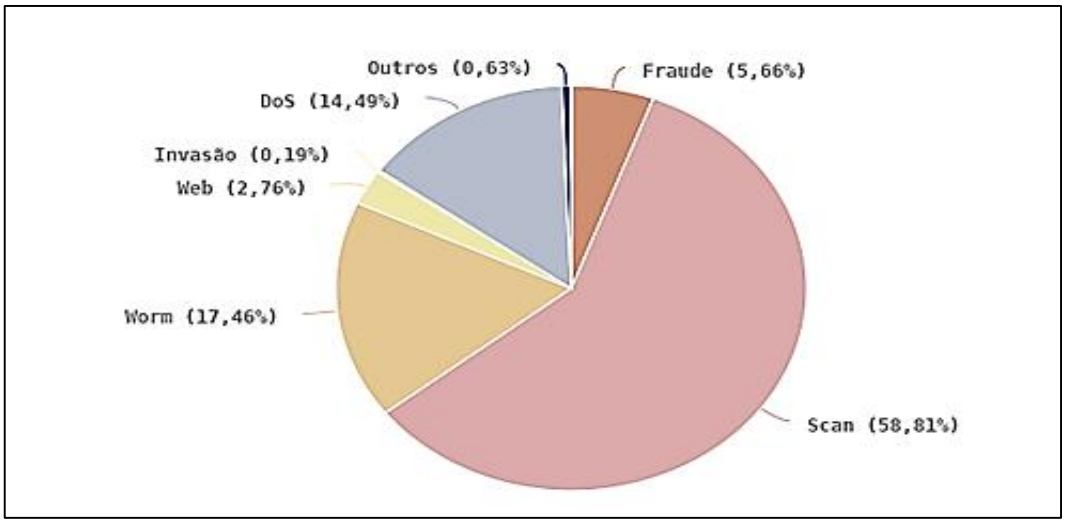
Neste ponto, torna-se conveniente quantificar os ataques e ameaças que se utilizam do fator humano ou da "boa-fé" dos usuários, comparando-os proporcionalmente a outros tipos. Para tal, uma boa base de dados é o Centro de Resposta a Incidentes de Segurança para a Internet no Brasil (CERT.br, 2020). O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. Por ser um ponto central para notificações de incidentes de segurança no Brasil, possui estatísticas e faz análise de tendência na área de segurança da informação.

De acordo com o CERT.br, nota-se que as ocorrências de "fraude" representam o quarto maior índice de incidentes, superando, inclusive, as tentativas de invasão (Figura 1). Cabe salientar que, dentre todos os tipos de incidentes relacionados na **Figura 1**, o único que depende do engodo, da dissimulação, da enganação e do abuso da boa-fé do usuário é a fraude. Por "fraude" entenda-se "tentativa de obter vantagem" (TIPOS DE ATAQUE, 2020). "No final, os ataques de engenharia social podem ter sucesso quando as pessoas são estúpidas ou, em geral, apenas desconhecem as boas práticas de segurança" (sic) (MITNICK; SIMON, 2003, p. 3).

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

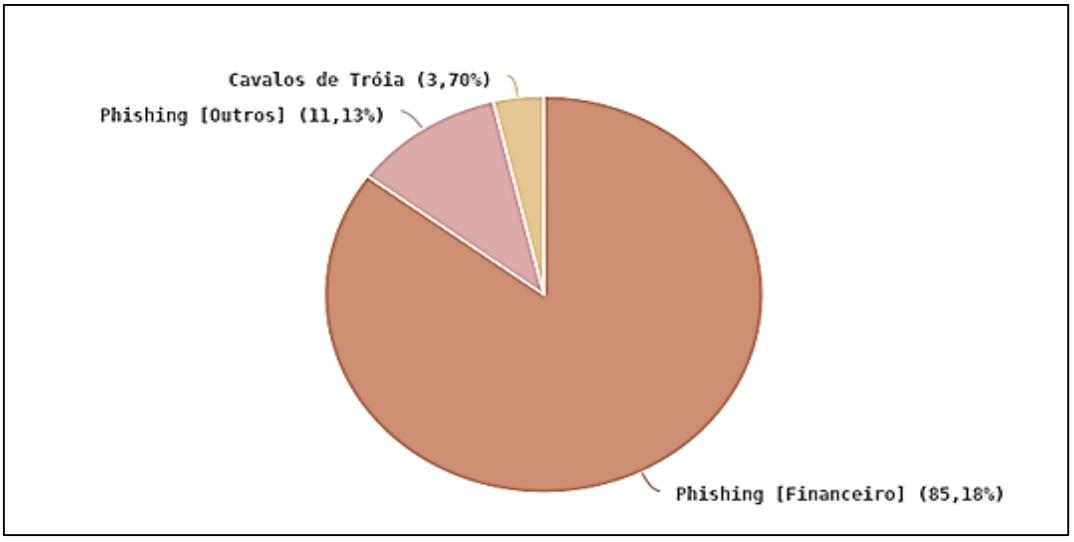
Figura 1. Porcentagem de incidentes de segurança no Brasil (2020)



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (TIPOS DE ATAQUE, 2020)

Detalhando as ocorrências de fraude, percebe-se que são relatados, basicamente, dois tipos de incidente: o *phishing* e o Cavalo de Tróia. Somados, os ataques do tipo *phishing* perfazem, segundo o CERT (Tipos de Ataque, 2020), mais de 96% dos incidentes de fraude relatados (**Figura 2**).

Figura 2. Detalhes dos tipos de fraude.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (Tentativas de fraude (percentual), 2020)

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

Phishing é um tipo de engenharia social em que o atacante, também chamado de *phisher*, tenta obter de maneira fraudulenta informações sensíveis ou confidenciais da vítima, simulando comunicações eletrônicas de fontes confiáveis ou organizações públicas. Pode ocorrer mediante uma mensagem de correio eletrônico que direciona o usuário a um *site* fraudulento que, por sua vez, recebe os dados em questão (JAKOBSSON; MYERS, 2007, p. 1).

Cavalo de troia é um programa que possui um código malicioso, feito para obter informações ou gerenciar arquivos do computador da vítima (MITNICK e SIMON, 2003, p. 48).

A empresa de Segurança *Everest Ridge*, de São Paulo, destaca que "e-mails de *spam* e *phishing* são responsáveis por 66% das infecções de *ransomware*. Em 2017, 48% das organizações foram afetadas pelo *ransomware*" (Estatísticas atualizadas sobre ataques cibernéticos, 2020).

Ransomware é um *malware* - um código malicioso – que usa de criptografia, normalmente, para tornar os dados do usuário inacessíveis, exigindo o pagamento de um resgate para disponibilizá-los novamente (Cartilha de segurança para a internet, 2020).

Dados da empresa de segurança cibernética *PurpleSec* corroboram as estatísticas, como segue:

- 98% dos ataques cibernéticos baseiam-se em engenharia social;
- Dados sobre falhas recentes de segurança apontam que 63% dos ataques bem-sucedidos são de fontes internas, sejam elas controle, erros ou fraude;
- 43% dos profissionais de TI disseram serem alvo de engenharia social no último ano;
- Funcionários recém contratados são mais suscetíveis a ataques de engenharia social (60% dos profissionais de TI citam contratações recentes como sendo de alto risco);
- 21% dos atuais ou ex-funcionários usam engenharia social para obterem vantagens financeiras, por vingança, curiosidade ou diversão;
- Tentativas de ataques usando engenharia social cresceram mais de 500% entre primeiro e o segundo trimestre de 2018 (2020 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends, 2020).

Segundo a *PurpleSec*, "e-mails direcionados, ou *spear phishing*, são relatados por empresas como sendo usados em 91% das violações de dados bem-sucedidas e 95% de todas as redes corporativas" (2020 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends, 2020).

Relata a empresa:

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

- 56% dos executivos de TI afirmam que os ataques de *spear phishing* são sua principal ameaça à segurança;
- 83% dos entrevistados sofreram ataques de *phishing* em 2018, um aumento de 76% com relação a 2017;
- Os golpes de comprometimento de e-mail comercial custaram às organizações US$ 676 milhões em 2017;
- 30% das mensagens de *phishing* são abertas por usuários-alvo e 12% desses usuários clicam no anexo ou *link* malicioso;
- Apenas 3% dos usuários-alvo relatam o recebimento de e-mails maliciosos aos superiores;
- 53% dos profissionais de TI e segurança afirmam ter experimentado um ataque de *spear phishing* em 2017;
- O comprometimento das credenciais cresceu 70% em relação a 2017, e aumentou 280% desde 2016;
- 50% dos sites de *phishing* agora usam HTTPS (2020 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends, 2020).

Nas palavras de Mitnick e Simon, “os empregados precisam conhecer os truques que os engenheiros sociais usam e devem ser treinados para não revelar os segredos de estado” (MITNICK; SIMON, 2003).

Isto posto, o presente estudo busca saber o nível de percepção de estudantes de cursos da área de Tecnologia da Informação em relação a tentativas de ataque com uso de engenharia.

METODOLOGIA

O presente estudo fez uso dos dados obtidos através de um questionário *online* realizado entre estudantes de cursos da área de Tecnologia da Informação em duas instituições de ensino superior de Estado de São Paulo (Apêndice I). Para a aplicação deste foi utilizada a plataforma *Forms*, da Microsoft, que permite a elaboração, disponibilização e análise de testes, questionários, pesquisas e votações (https://forms.office.com). As perguntas foram elaboradas baseadas no estudo de Pereira e Martins (2014).

Foram obtidas 54 respostas a um questionário com 12 questões objetivas de múltipla escolha e uma questão dissertativa (Apêndice II). Esta questão só seria respondida condicionalmente, ou seja: em uma das questões objetivas, uma das respostas direcionava o entrevistado a esta questão, para maiores esclarecimentos. Excetuando-se esta questão condicional e outra questão objetiva – também condicional -, todas eram obrigatórias (o formulário só

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

finalizaria e seria aceito após todas as questões serem devidamente preenchidas).

Os participantes foram alunos dos seis períodos dos cursos, que têm duração de 3 anos.

ANÁLISE DOS RESULTADOS

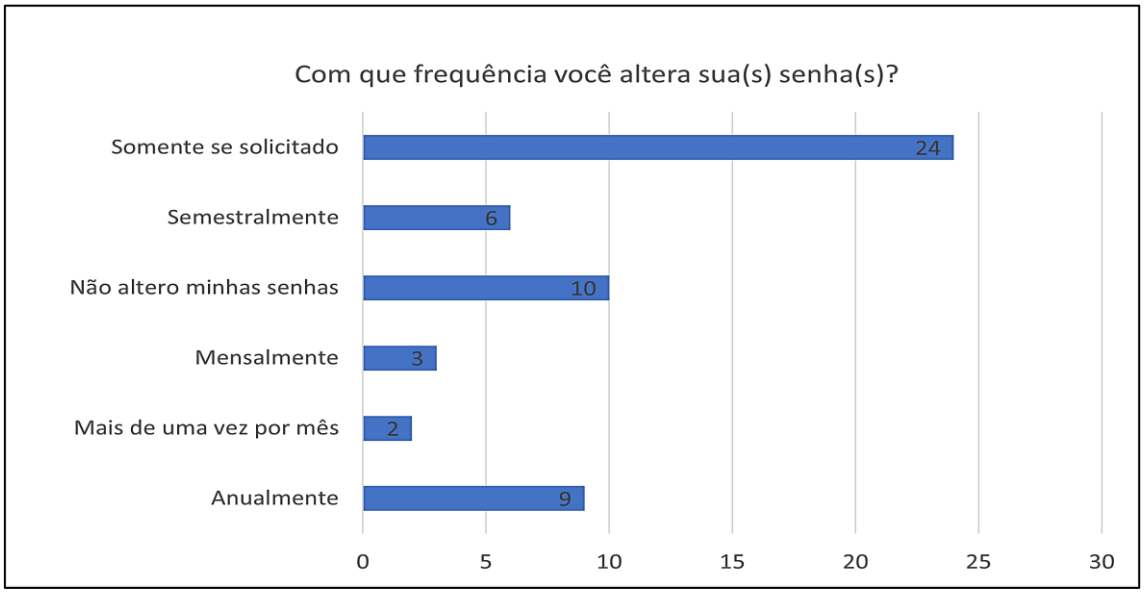
Tendo por base os dados obtidos com as respostas à pesquisa proposta, pode-se verificar a percepção dos alunos quanto à segurança da informação e a algumas estratégias de ataque por engenharia social.

De todos os pesquisados (n=54), 83% trabalham (n=45). Destes, 58% (n=26) trabalha na mesma área de estudo (Tecnologia da Informação). Dentre todos os entrevistados, 54% (n=29) têm idade entre 18 e 25 anos; 31% (n=17), têm entre 25 e 35 anos e 15% (n=8) têm mais que 35 anos. 91% dos pesquisados (n=49) declara-se ser do gênero masculino; 7% (n=4), do gênero feminino e 1% (n=1) não declarou seu gênero.

A maior parcela dos respondentes está cursando o 1º período de seu curso (n=18), seguida pelos discentes do 6º período (n=13). O 5º, 4º e 2º período participam com 11, 8 e 4 alunos, respectivamente. Nenhum dos respondentes declarou-se cursando o 3º período.

A **Figura 3** questiona sobre a frequência de alteração de suas senhas (não foram explicitadas quais, na pesquisa):

Figura 3. Frequência de alteração de senhas pelos entrevistados,



Fonte: obtido pelo autor.

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

Nota-se na **Figura 3** que 2 estudantes responderam que fazem este procedimento mais de uma vez por mês; 3, mensalmente; 6, a cada seis meses; 9, uma vez ao ano; 24 as alteram apenas se for solicitado e 10 dos entrevistados informaram não alterar suas senhas.

Quando perguntados sobre o uso de uma mesma senha para serviços ou *sites* diferentes, 54% (n=29) dos pesquisados responderam que utilizam; 46% (n=25) responderam que não utilizam.

Questionados se alguém, além dos próprios entrevistados, conhece ou usa alguma de suas senhas (em *sites* ou e-mails, por exemplo), 74% (n=40) afirmaram que não, enquanto 26% (n=14) responderam que sim.

Pode-se notar, observando-se estas três questões, que procedimentos básicos de segurança da informação não estão sendo rigorosamente seguidos.

Foi perguntado aos estudantes se estes têm por costume abrir e-mails provenientes de remetentes desconhecidos. Diante desta questão, 61% (n=33) responderam não abrir, ao passo que 30% (n=16) afirmaram abri-los algumas vezes e 9% (n=5) disseram o fazer sempre. Indagados se já receberam mensagens referentes a débitos, multas de veículos, solicitação de cadastros bancários ou conteúdo semelhante, 35% (n=19) responderam que não, enquanto 65% (n=35) declararam receber e-mails com tal conteúdo.

Perguntados sobre que atitude teriam perante uma mensagem informando sobre uma premiação e solicitando clicar em um *link* para maiores informações, 93% (n=50) dos entrevistados responderam que ignorariam; 4% (n=2) clicariam no *link*, mesma proporção de respondentes que disseram que seu comportamento dependeria da premiação.

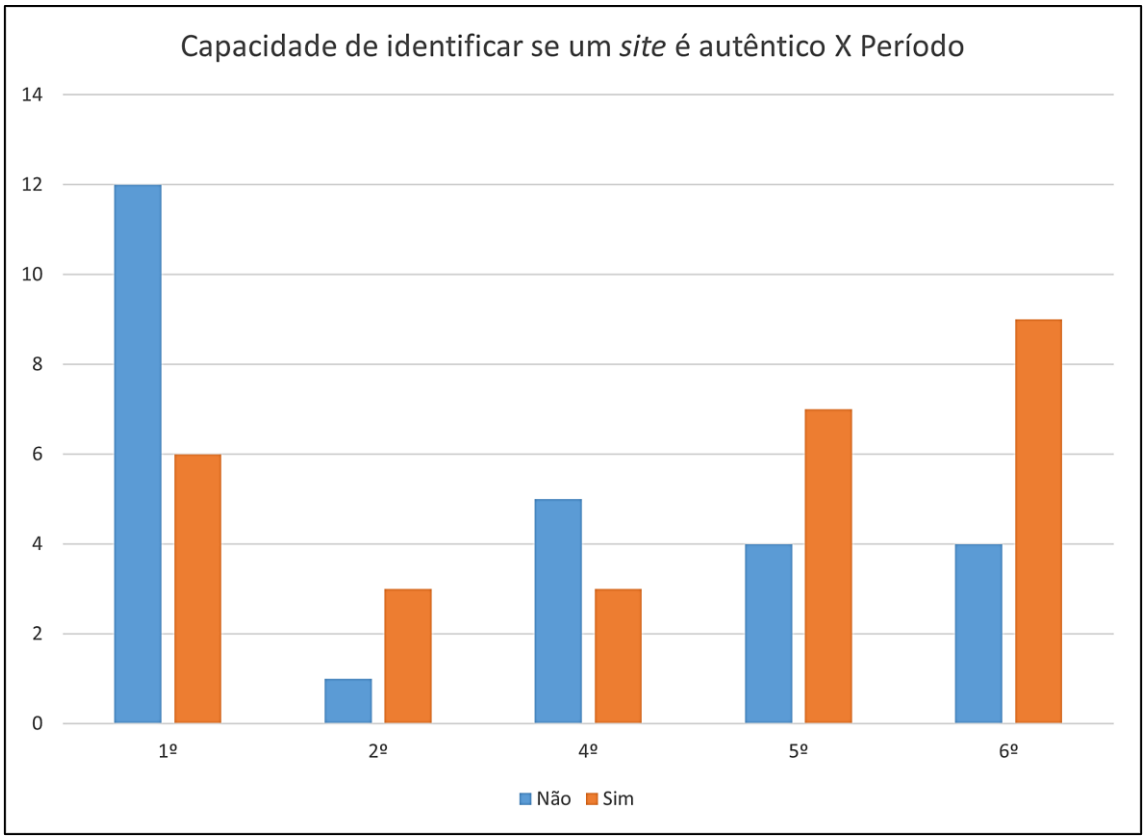
Quando indagados se saberiam identificar se um *site* é autêntico, 52% dos alunos (n=28) afirmaram que sim, enquanto 48% (n=26) responderam que não saberiam.

Visualizando as respostas a esta questão por período do curso, nota-se que a capacidade dos alunos em identificar se uma página de internet é autêntica tende a aumentar com o decorrer da formação acadêmica. Dos 18 respondentes cursando o 1º período, apenas 6 afirmaram ser capazes de tal coisa; dos 6 estudantes que estão no 2º período, 5 declararam ter tal conhecimento; no 5º período, dos 11 entrevistados 7 responderam saber fazer tal identificação e dos 13 alunos do 6º período, 9 se disseram aptos a verificar a autenticidade de um *site*. A exceção veio no 4º período, no qual dentre os 8 respondentes somente 3 afirmaram ter tal desenvoltura. Não houve participantes que se declararam alunos do 3º período. Estes dados podem ser visualizados na **Figura 4**:

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

Figura 4. Capacidade de identificar se um site é autêntico *versus* período.



Fonte: obtido pelo autor.

Contudo, esta questão, quando respondida afirmativamente, conduzia a outra pergunta, para identificar como o estudante consegue verificar a veracidade de determinado *site*. Esta era uma questão que permitia respostas dissertativas, pois teve a intenção de observar os métodos utilizados pelos respondentes e analisá-los

As respostas a esta pergunta condicional foram variadas. Dentre tantas, seguem algumas como exemplo:

- “Pesquisando se tem CNPJ”;
- “Através do domínio”;
- “Pela autenticação de site seguro”;
- “Pelo cadeado ao lado da url”;
- “Verifico se existe um cadeado ao lado esquerda onde está a url, verifico a url. Domínio” (sic);
- “Pelo https”;

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

- “Através da url do mesmo” (sic);
- “Verifico se no *link* o nome do site está escrito da forma correta, ou vou até a página principal e tento navegar para a página derivada”;
- “Através de vários métodos, mas especialmente através do *'whois'*, onde consigo consultar o proprietário da página”;
- “Normalmente verifico se o endereço não é estranho; a extensão (.com, .GOV, etc); se for de uma instituição, procuro no *Google* para confirmar; verifico as informações de contato e sobre; etc.”.

Dentre as respostas elencadas, infere-se que alguns dos entrevistados possuem conhecimentos relativos à identificação de *sites* possivelmente fraudulentos. O uso do “*Whois*” é um excelente exemplo. Entretanto, verificar a autenticidade de um *site* apenas pela URL, pelo domínio ou pela presença do “https” na barra de endereços, que supostamente indicaria um *site* seguro, não garante a veracidade da página em questão.

Desta forma, alguns dos alunos que responderam saber identificar se um *site* é autêntico podem ter uma falsa sensação de segurança. Cruzando-se as informações da questão que indaga se os entrevistados sabem identificar se determinado *site* é autêntico com as respostas sobre como eles fazem esta identificação, o número de entrevistados que não sabem verificar a autenticidade de uma página de internet chega a 83% (n=45).

CONCLUSÕES

A partir dos resultados apresentados, pode-se concluir que mesmo estudantes de cursos da área de Tecnologia da Informação tendem a não observar conceitos básicos de segurança, como o compartilhamento de senhas e a frequência de troca destas. Há um lapso, também, quanto à identificação de *sites* fraudulentos que, conforme demonstrado, tende a diminuir com o correr da formação acadêmica dos entrevistados.

Outro aspecto expressivo a ser considerado é o comportamento da falsa sensação de segurança. Apesar de 52% dos alunos perguntados afirmarem saber identificar páginas de internet falsas, esta porcentagem chega a 85% dos entrevistados quando estes são inqueridos sobre os métodos para verificação utilizados. Esta impressão errônea de segurança pode ser mais prejudicial que o reconhecimento da própria incapacidade quanto à apuração da veracidade de um *site*, posto que se toma uma página falsa como autêntica.

Estas observações reforçam a ideia que levar em consideração o fator humano é imprescindível para a implementação de políticas de segurança e que

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

saber os tipos de técnicas e o conhecimento de como identificar fraudes podem auxiliar na prevenção de ataques por meio de engenharia social.

REFERÊNCIAS

2020 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends. **PurpleSec**, 2020. Disponivel em: <https://purplesec.us/resources/cyber-security-statistics/>. Acesso em: 22 Out 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação**. Rio de Janeiro. 2013.

BRAGA, P. H. D. C. Técnicas de Engenharia Social. **Grupo de Resposta a Incidentes de Segurança**, Rio de Janeiro, 2011. Disponivel em: <https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_social.pdf>.

CAIÇARA JUNIOR, C. **Sistemas Integrados de Gestão ERP:** uma abordagem gerencial. 3ª. ed. Curitiba: Ibpex, 2008.

CARTILHA de segurança para a internet. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**, 2020. Disponivel em: <https://cartilha.cert.br/ransomware/>. Acesso em: 15 Outubro 2020.

ESTATÍSTICAS atualizadas sobre ataques cibernéticos. **Everest Ridge**, 2020. Disponivel em: <https://everestridge.com.br/estatisticas-atualizadas-sobre-ataques-ciberneticos/>. Acesso em: 22 Out 2020.

Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**, 2020. Disponivel em: <https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html>. Acesso em: 15 Out 2020.

JAKOBSSON, M.; MYERS, S. **Phishing and Countermeasures:** Understanding the Increasing Problem of Electronic Identity Theft. Hoboken, New Jersey: Wiley-Interscience, 2007.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet:** Uma Abordagem Top-Down. 5ª. ed. São Paulo: Addison Wesley, 2010.

MARCELO, A.; PEREIRA, M. A. D. A. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

PROSPECTUS
ISSN 2674-8576

DOI: https://doi.org/10.5281/zenodo.7213756 Artigo Original

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar - Ataques de Hackers:** Controlando o fator humano na Segurança da Informação. São Paulo: Pearson Makron Books, 2003.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec Editora, 2007.

PEREIRA, L. D. D.; MARTINS, D. M. S. ENGENHARIA SOCIAL: SEGURANÇA DA INFORMAÇÃO APLICADA À GESTÃO. **Caderno de Estudos em Sistemas da Informação**, 2014.

SILVA, N. B. X.; ARAÚJO, W. J. D.; AZEVEDO, P. M. D. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana de Ciência da Computação**, Brasília, v. 6, n. 2, p. 37-55, Agosto/Dezembro 2013.

TENTATIVAS de fraude (percentual). **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**, 2020. Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html>. Acesso em: 15 Out 2020.

TIPOS de Ataque. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**, 2020. Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html>. Acesso em: 06 Out 2020.

O autor declarou não haver qualquer potencial conflito de interesses referente a este artigo.