ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 2/2023

FABIANO DA COSTA AGUIAR, Cap Esp Com

Inovação nos treinamentos de prevenção à Engenharia Social: uma necessidade

Rio de Janeiro

2023

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 2/2023

FABIANO DA COSTA AGUIAR, Cap Esp Com

Inovação nos treinamentos de prevenção à Engenharia Social: uma necessidade

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Doutrina de Inteligência
Orientador: Danilo Bichir, Cap Inf

Rio de Janeiro
2023

FABIANO DA COSTA AGUIAR, Cap Esp Com

Inovação nos treinamentos de prevenção à Engenharia Social: uma necessidade

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

André da Costa Gonçalves, Prof Dr
EAOAR

_____

Danilo Bichir, Cap Inf
EAOAR

Rio de Janeiro

2023

RESUMO

A Engenharia Social é uma estratégia antiga e enganadora que visa obter informações sigilosas através da manipulação das pessoas. Na Força Aérea Brasileira (FAB), uma das medidas de proteção contra esses ataques é a realização de treinamentos na forma de palestras para todos os servidores, visando garantir a consciência de segurança da informação dos usuários. No entanto, executar tais treinamentos para todo o efetivo tem se mostrado uma tarefa complexa e custosa. Sendo assim, este ensaio defende a criação de um treinamento à distância para prevenção da Engenharia Social na FAB. O treinamento virtual é uma forma eficaz de alcançar todos os colaboradores e cumprir os treinamentos, disponibilizando conteúdo atualizado de forma prática e abrangente. Dessa forma, será permitido o acesso contínuo aos treinamentos, eliminando as dificuldades e as ausências nos eventos presenciais. Além disso, a eficácia do treinamento apresentado é comprovada pelo uso de métodos interativos, como jogos, simulações e vídeos, que proporcionam uma experiência prática e envolvente. Segundo os estudos, esse método é mais motivador e eficiente para o aprendizado. Com a implementação desse treinamento, a FAB poderia mitigar as dificuldades enfrentadas na conscientização do efetivo, promovendo uma cultura de segurança da informação mais forte e melhorando o aprendizado dos usuários, tornando-os menos suscetíveis a ataques maliciosos. Portanto, o treinamento à distância é uma solução eficaz para alcançar todo o efetivo e promover um ambiente mais seguro, podendo ainda ser aplicado em outras áreas para a proteção de informações sigilosas e a preservação da soberania do país.

Palavras-chave: Engenharia Social. Segurança da Informação. Conscientização. Treinamento.

1 INTRODUÇÃO

De acordo com Brasil (2008), a Engenharia Social é a arte de trapacear, de construir métodos e estratégias para enganar ou de ganhar a confiança para obtenção de informações, são ações antigas, oriundas dos tempos mais remotos. É um tipo de ataque, onde a principal “arma” utilizada é a habilidade de lidar com pessoas, induzindo-as a fornecer informações, executar programas e, muitas vezes, disponibilizar senhas de acesso. Tais investidas visam explorar as pessoas no intuito de ocasionar a perda, a indisponibilidade ou a violação da informação desejada. Os ataques são direcionados diretamente ao elo mais fraco de qualquer sistema de segurança: o ser humano.

Ao analisar as normas e procedimentos relativos ao tema no contexto da Força Aérea Brasileira (FAB), observa-se que as medidas para proteção dos conhecimentos são implementadas por meio de Ações de Contrainteligência, as quais buscam garantir um grau ideal de proteção. Tais ações são eminentemente preventivas e defensivas.

Segundo Brasil (2022), a Segurança Orgânica é o segmento da Contrainteligência responsável por garantir um grau de proteção ideal por meio de medidas preventivas e de obstrução contra ações que ameacem a salvaguarda de dados, conhecimentos e seus suportes: documentos, áreas e instalações, pessoal, material e meios de Tecnologia da Informação e Comunicações.

Apesar de tais medidas e ações serem bem definidas no Manual de Doutrina de Inteligência do Comando da Aeronáutica (MCA 200-1 de 2022), no Manual de Ações de Contrainteligência no COMAER (MCA 200-23 de 2017) e no Programa Básico de Trabalho Anual e Educação Continuada dos Elos do SINTAER (ICA 200-11 de 2013), os métodos estabelecidos para os treinamentos de conscientização do efetivo são de difícil execução.

Foi constatado ao longo dos últimos anos que cumprir esses treinamentos é uma tarefa complexa, principalmente para as Organizações Militares (OM) com efetivos mais numerosos. Reunir semestralmente todos os integrantes do efetivo em um auditório e fornecer instruções com conteúdo padronizado e atualizado é custoso. Vale ressaltar a defasagem dos Folhetos de Mentalidade de Segurança (FCA 200-2 de 2008) e de Prevenção à Engenharia Social (FCA 200-3 de 2009), que orientam os treinamentos.

Ao analisar experiências de outras unidades, verificou-se ainda que o problema se estende a diversas OM em nossa força. Os treinamentos são deficientes nas unidades, e, por vezes, não alcançam seu potencial pleno em relação ao efetivo, deixando vulnerabilidades que podem ser facilmente exploradas. Sendo assim, este ensaio defende a criação de um treinamento à distância sobre prevenção à Engenharia Social para possibilitar o preparo do efetivo com eficácia.

Para isso, serão apresentados dois argumentos em apoio à tese. O primeiro argumento é que o treinamento a distância é uma forma viável de alcançar todos os colaboradores do efetivo, cumprindo o que está estabelecido nos programas de conscientização. O segundo argumento é que a prática das técnicas utilizadas pela Engenharia Social no ambiente virtual promove maior aprendizado, transformando os usuários em elos fortes e impedindo o sucesso das práticas maliciosas.

2 A PREVENÇÃO À ENGENHARIA SOCIAL

A Segurança da Informação desempenha um papel estratégico dentro das Organizações, tornando-se uma necessidade crescente e indispensável para qualquer setor da atividade humana. Sendo assim, é necessário que a informação seja sempre protegida adequadamente em todas as suas formas: digital, impressa, escrita, falada, etc. É comum a crença de que a Segurança da Informação pode ser alcançada por meio de tecnologia avançada e processos bem estruturados. No entanto, essa convicção é totalmente anulada quando as pessoas contornam os controles, ignoram avisos ou negligenciam a execução de procedimentos e protocolos prescritos.

O acesso não autorizado a técnicas, processos de inovação, pesquisas, planos operacionais e a conhecimentos tradicionais a eles associados, pode comprometer a consecução de objetivos estratégicos e resultar em prejuízos expressivos ao preparo e emprego da FAB.

Um dos grandes desafios para as Seções de Inteligência (SINT) das Organizações Militares é cumprir os programas de conscientização de forma adequada. Existem algumas razões para isso: quando existentes nas OM, as SINT têm redução de mão de obra; o treinamento de todo o efetivo demanda tempo e planejamento; e o efetivo das SINT não possui o preparo necessário para fornecer

um curso atualizado e de qualidade. Outro aspecto importante a ser mencionado é o avanço tecnológico, que fomenta novos métodos de ataque, cada vez mais sofisticados nas formas exploratívas, dificultando a eliminação de riscos e a detecção dos engenheiros sociais.

“Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente” (ARAUJO, 2005, p. 27).

É preocupante a falta de conscientização adequada sobre o assunto, o que abre uma brecha enorme para exploração pelos engenheiros sociais, que podem ser estrangeiros, naturais ou naturalizados. De qualquer forma, uma coisa é certa: possuem interesses antagônicos aos nossos. Os seus ataques podem ser classificados em dois modos, os diretos: pessoalmente, por telefonemas ou e-mails e os indiretos: focam na infraestrutura tecnológica através de vírus, *malwares*, *phishing*, etc.

> Dentro do mundo corporativo talvez haja poucos assuntos sobre os quais todos os empregados precisam ser treinados e que são ao mesmo tempo tão importantes e tão aborrecidos quanto a segurança. Os melhores programas de treinamento sobre a segurança das informações devem informar e prender a atenção e o entusiasmo dos aprendizes (FONSECA, 2009, p. 9).

A implementação pela FAB de um treinamento à distância sobre o tema, tem potencial para mitigar as dificuldades apresentadas no cumprimento dos programas atuais e inovar a forma como os militares e civis da FAB são treinados nesta área. O ambiente virtual da própria Organização é capaz de prover os treinamentos necessários e as suas revalidações de forma prática, abrangente e atemporal, atingindo novos servidores desde a sua chegada na unidade.

2.1 A eficácia do treinamento à distância

De forma geral, as organizações estão investindo cada vez mais em soluções de segurança, porém, estão esquecendo de investir nos recursos humanos. De nada adianta ter um ambiente de segurança eletrônica se o elo fraco é um colaborador indiscreto ou alheio às ameaças existentes. Os ataques para obtenção de informações, empregando os mencionados engenheiros sociais, estão em constante

evolução, tornando-se cada vez mais sofisticados e audaciosos, aproveitando principalmente a ingenuidade e despreparo dos usuários.

“É praticamente impossível eliminar brechas para a engenharia social sem trabalhar na melhoria do nível de conscientização sobre segurança da informação em todos os funcionários.” (ALDAWOOD; SKINNER, 2018, p. 65)

É possível notar unanimidade entre os teóricos sobre o tema. Há um consenso de que todo o efetivo, sem exceção, deve ser submetido a treinamentos periódicos, pois basta apenas um servidor inocente ou descuidado para comprometer qualquer plano de segurança.

O treinamento à distância promove a transmissão ininterrupta e de forma abrangente a todo o efetivo, sendo capaz de mitigar as dificuldades atuais enfrentadas pelos setores de inteligência na execução das palestras previstas. Os servidores podem acessar o conteúdo no próprio ambiente virtual da OM sempre que necessário. Além disso, nos casos de afastamentos por quaisquer motivos, os usuários têm acesso remoto contínuo, eliminando a ocorrência de ausências nos treinamentos ou revalidações e tornando mais simples o controle de participação pelos elos de inteligência responsáveis.

Outro aspecto interessante do treinamento virtual é o aprimoramento do aprendizado. Nesse caso, os usuários têm mais flexibilidade para cumprir os treinamentos nos momentos oportunos, aumentando o foco no conteúdo e deixando de dividir a atenção com preocupações relacionadas a prazos e interrupções ocasionais.

Saleem e Hammoudeh (2018) reforçam essa ideia em seu artigo, alegando que a rede interna de uma empresa pode ser muito útil na facilitação dos programas de conscientização, integrando treinamentos de segurança projetados por pessoal capacitado e disponibilizando-os aos usuários.

Dessa maneira, considerando o cenário atual de evolução nas formas de ataque e a deficiência dos métodos atuais, o treinamento à distância revela-se como uma alternativa viável e eficaz para solucionar a dificuldade atual enfrentada pelos setores de inteligência em atingir a totalidade dos servidores, além de prover conteúdo de qualidade e atualizado por especialistas qualificados. Esse treinamento poderia ser facilmente implementado na FAB pelo Órgão Central de Inteligência, o CIAER.

2.2 A prática das técnicas e o aperfeiçoamento no aprendizado

Conforme concluem Aldawood e Skinner (2019a) em sua revisão de soluções para a engenharia social, dentre todos os métodos de mitigação, o desenvolvimento de treinamentos e conscientização dos funcionários em uma organização desempenha um papel fundamental na defesa contra essa prática. Com a mudança nos métodos dos treinamentos sobre o tema ao longo dos anos, implementou-se a utilização de ferramentas mais modernas, sendo citadas como as melhores soluções experimentadas, tais como: jogos sérios, laboratórios virtuais, torneios, simulações, vídeos e outros.

A utilização de um treinamento à distância que utilize algumas destas técnicas aumentará facilmente a motivação e o envolvimento dos servidores no tema, aprimorando o aprendizado e a manutenção da consciência de segurança no efetivo.

Grande parte dos usuários comuns julgam que os ataques à segurança da informação são protegidos pela tecnologia, por meio de ativos de segurança (*firewalls*, antivírus, etc). Portanto, é primordial executar treinamentos que envolvam e despertem a curiosidade dos colaboradores, fortalecendo assim a cultura de segurança da informação nas organizações.

> (…) as técnicas tradicionais de treinamento são muitas vezes ineficazes e difíceis de se sustentar. Além disso, a maioria dos treinamentos organizacionais não incorporam a prática de comportamentos de engenharia social - uma técnica que demonstramos promover resultados encorajando o pensamento adversário. Quando as pessoas executam as ações de seus adversários, elas entendem as suas potencialidades. (GIBONEY, 2023, p. 8)

No artigo supracitado são apresentados dois estudos que demonstram a eficácia e o estímulo produzido pela prática em um ambiente virtual realístico, divertido e envolvente, resultando em melhores níveis de aprendizado e consciência situacional.

Em outro estudo apresentado por Aldawood e Skinner (2019b), foram comparados métodos tradicionais e modernos para treinamentos de prevenção à engenharia social, expondo as principais limitações das organizações de forma geral. No desenvolvimento do estudo, evidenciou-se que os métodos mais recentes, que envolvem diversas técnicas mais modernas, apesar de possuírem custos mais elevados quando contratados, são mais eficazes em relação ao aprendizado dos funcionários e a segurança das organizações.

Na conjuntura atual, em que o mercado está cada vez mais competitivo e mais exposto a vulnerabilidades externas, as empresas buscam constantemente soluções mais viáveis e eficientes para superar suas dificuldades. É notório que os estudos mais recentes sobre treinamentos de prevenção à engenharia social apontam a forma interativa virtual como a que apresenta maior eficácia e motivação na aprendizagem dos funcionários.

3 CONCLUSÃO

Diante das dificuldades enfrentadas pelas organizações militares para cumprir efetivamente os programas de conscientização e treinamento sobre prevenção à Engenharia Social, fica evidente a necessidade de buscar soluções inovadoras e eficazes.

Conforme evidenciado no decorrer deste ensaio, o formato de treinamento apresentado tem potencial para atingir com facilidade todos os colaboradores do efetivo, superando as limitações de tempo, recursos e logística encontradas nos métodos tradicionais. Além disso, a prática das técnicas utilizadas pela Engenharia Social em um ambiente virtual proporciona um aprendizado mais efetivo, convertendo os usuários em elos fortes e impedindo o sucesso de ataques maliciosos.

Nesse contexto, a implementação de um treinamento à distância surge como uma alternativa viável e promissora para alcançar os objetivos com eficácia. Ao adotar o treinamento à distância, a Força Aérea Brasileira (FAB) mitigará as vulnerabilidades existentes, oferecendo conteúdo atualizado e de qualidade, e promovendo a cultura de conscientização e segurança da informação em seu efetivo. Dessa forma, a criação desse treinamento à distância representa uma solução adequada para enfrentar os desafios e fortalecer a proteção dos conhecimentos e das informações estratégicas da FAB. O método apresentado também poderia ser utilizado em outras áreas, como no Controle do Espaço Aéreo, em treinamentos operacionais, estudos dirigidos ou em outras áreas que enfrentem dificuldades semelhantes ou que necessitem de inovação de métodos inadequados.

REFERÊNCIAS

ALDAWOOD, Hussain; SKINNER, Geoffrey. **An academic review of current industrial and commercial cyber security social engineering solutions.** In: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019a. p. 110-115. DOI 10.1145/3309074.3309083. Disponível em: Proceedings Template - WORD (researchgate.net). Acesso em: 15/06/2023.

ALDAWOOD, Hussain; SKINNER, Geoffrey. **Educating and raising awareness on cyber security social engineering:** A literature review. In: 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE). IEEE, 2018. p. 62-68. DOI 10.1109/TALE.2018.8615162. Disponível em: https://ieeexplore.ieee.org/document/8615162. Acesso em: 16/06/2023.

ALDAWOOD, Hussain; SKINNER, Geoffrey. **Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues.** Future Internet, v. 11, n. 3, p. 73, 2019b. DOI 10.3390/fi11030073. Disponível em: https://www.mdpi.com/1999-5903/11/3/73. Acesso em: 16/06/2023.

ARAUJO, Eduardo E. **A vulnerabilidade humana na segurança da informação.** Orientador: Prof. Esp. Flamaryon Guerin Gomes Borges. 2005. 48 f.Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação)-Faculdades Uniminas, Uberlândia, 2005. Disponível em: https://silo.tips/download/a-vulnerabilidade-humana-na-segurana-da-informaao. Acesso em: 15/06/2023.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria Nº 3/CIAER, de 19 de Dezembro de 2008. Aprova a edição do Folheto que dispõe sobre Mentalidade de Segurança (FCA 200-2). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 13, f. 351, 21 Jan. 2009. Disponível em: https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=9817 Acesso em:10/06/2023.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria Nº 02/CIAER, de 8 de Outubro de 2009. Aprova a edição do Folheto que dispõe sobre Prevenção à Engenharia Social (FCA 200-3). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 206, f. 7420, 06 Nov. 2009. Disponível em: https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=2356. Acesso em: 16/06/2023.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria CIAER Nº 22/SED-DPL, de 19 de Junho de 2017. Aprova a edição do Manual que dispõe sobre as Ações de Contrainteligência no Comando da Aeronáutica (MCA 200-23). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 109, f. 6309, 28 Jun. 2017. Disponível em: https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=2384. Acesso em: 16/06/2023.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria EMAER Nº 5/CEMAER, de 23 de Fevereiro de 2022. Aprova a reedição da Doutrina de Inteligência da Aeronáutica (MCA 200-1)**. Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 041, f. 2788, 02 Mar. 2022. Disponível em:

https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=32194. Acesso em: 16/06/2023.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação: O Fator Humano.** 2009. Artigo (Pós Graduação em Redes e Segurança de Computadores)– Pontifícia Universidade Católica do Paraná, Curitiba, v. 42, 2009. Disponível em: https://www.cursosavante.com.br/cursos/curso533/conteudo7486.pdf. Acesso em: 16/06/2023.

GIBONEY, Justin Scott; SCHUETZLER, Ryan M.; GRIMES, G. Mark. **Know your enemy:** Conversational agents for security, education, training, and awareness at scale. Computers & Security, v. 129, p. 103207, 2023. DOI 10.1016/j.cose.2023.103207. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404823001177. Acesso em: 16/06/2023.

SALEEM, Jibran; HAMMOUDEH, Mohammad. **Defense methods against social engineering attacks.** Computer and network security essentials, p. 603-618, 2018. DOI 10.1007/978-3-319-58424-9_35. Disponível em: (PDF) Defense Methods Against Social Engineering Attacks (researchgate.net) Acesso em: 21/06/2023.