PHISHING SCAM NO AMBIENTE MILITAR: A EFICIÊNCIA DE UMA TÉCNICA DE PREVENÇÃO DE ATAQUES DE PHISHING CONTRA MILITARES

TEN CAIO DE SOUZA ALVES
TEN RICARDO HENRICK SANTOS CAETANO

RESUMO: O ambiente informacional compreende a modernidade do ambiente laboral. Locais de trabalho conectados com profissionais exercendo suas atribuições por meio de dispositivos eletrônicos em rede geram a necessidade de manter-se atualizado quanto às vulnerabilidades as quais estão expostos. Essa pesquisa busca verificar a eficiência de uma técnica de prevenção aos ataques do tipo Phishing Scam em diminuir os casos de exposição de militares a esse tipo de ameaça digital. Para tal objetivo foi realizada uma pesquisa experimental utilizando-se uma amostra de acessibilidade dividida em dois grupos, sendo que somente a um dos grupos foi distribuída uma cartilha de prevenção aos ataques de tipo Phishing Scam. Em seguida, foi realizado um ataque de Phishing Scam simulado nos dois grupos, onde foi computado o número de acessos ao link malicioso simulado. Após o experimento, comparando-se os resultados obtidos, houve uma grande diferença na exposição à ameaça por parte dos dois grupos, comprovando assim a hipótese de que uma orientação básica, simples e de fácil entendimento é eficiente na prevenção aos ataques de tipo Phishing.

Palavras Chaves: PHISHING SCAM. ENGENHARIA SOCIAL. PROTEÇÃO CIBERNÉTICA.

1 INTRODUÇÃO

A necessidade de emprego de dispositivos com acesso à internet no ambiente de trabalho tornou-se uma realidade quase que unânime nos dias de hoje.

Ferramentas digitais para gestão e administração são empregadas em larga escala, inclusive em dispositivos pessoais dos usuários como tablets, notebooks e smartphones.

Nesse escopo, surgem diversas ameaças que visam vantagens pecuniárias, acesso a banco de dados e derrubada de serviços prestados em rede.

Diversos desses ataques empregam técnicas de engenharia social para atingir o elo mais fraco dos sistemas de segurança: o usuário.

O Phishing Scam busca coletar dados do usuário de forma não autorizada, ludibriando o usuário através de um assunto de seu interesse, atraindo-o para uma armadilha.

Os militares do Exército Brasileiro também estão suscetíveis a ataques de engenharia social, contudo com uma orientação básica, é possível diminuir a ocorrência desses eventos com integrantes da instituição.

Um dos objetivos desse artigo é mostrar a importância de uma conscientização continuada sobre as principais técnicas utilizadas por golpistas e de prevenção contra esses ataques.

As técnicas de prevenção podem ter diversos níveis de complexidade. Neste trabalho contudo, será mostrada a eficiência de uma orientação simples e direta.

2 METODOLOGIA

Como base deste artigo, foi realizada, segundo Gil (2008), uma pesquisa experimental, utilizando dois grupos, um experimental e outro de controle, pegos de uma amostra por acessibilidade.

Os indivíduos do grupo experimental foram submetidos a um estímulo de influência, ou em outras palavras, à ação da variável independente (GIL, 2008). O grupo de controle foi submetido a nenhuma influência. Ambos os grupos são semelhantes, contendo militares de uma mesma Organização Militar (OM),

abrangendo desde a graduação de Soldado Recruta até o posto de Capitão, sendo cada grupo uma subunidade.

Após o delineamento da pesquisa, foi realizado um ataque Phishing Scam sem consequências para os integrantes dos grupos, para constatar se houve uma diferença significativa entre um grupo e outro, admitindo ou não a veracidade da hipótese.

As ações para a execução do experimento se deram de acordo com o quadro a seguir:

QUADRO 1 – Sequência das ações

AÇÃO	DATA/HORA
ENTREGA DO FOLHETO (APÊNDICE A)	02 JUN / 10:00h
ENVIO DA MENSAGEM (GP EXPERIMENTAL)	03 JUN / 10:50h
ENVIO DA MENSAGEM (GP CONTROLE)	03 JUN / 11:10h
LEVANTAMENTO DOS RESULTADOS	05 JUN / 14:30h

Fonte: os autores, 2022.

Para a montagem do artigo, além da pesquisa realizada, foi feita uma pesquisa bibliográfica, com fontes semelhantes ao assunto, para fundamentar os argumentos aqui apresentados.

3 RESULTADOS E DISCUSSÃO

3.1 A INTERNET

Criada na década de 1960, a Internet buscava conectar laboratórios e institutos de pesquisa para troca de dados. De lá até os dias atuais muita coisa mudou. O fenômeno do crescimento exponencial dessa rede de dados mundial gera imenso impacto em diversos setores de nossas vidas.

De acordo com Comer (2016), a difusão dos computadores pessoais de alta velocidade junto com redes mais rápidas mudou o foco de compartilhamento de recursos. O fluxo de dados deslocou-se de texto para gráficos, depois videoclipes e vídeos de alta definição. Algo semelhante ocorreu com os dados de áudio, possibilitando a transferência de dados multimidia.

Os telefones celulares antes usados exclusivamente para uso em ligações de voz, hoje têm novas capacidades e estão cada vez mais presentes no ambiente laboral. Com um único smartphone com acesso à internet, o usuário pode estabelecer conexão com ferramentas informatizadas e aplicações de gestão administrativa, planilhas e documentos de seu trabalho enquanto pode ainda checar as suas redes sociais, e-mails ou acessar sua conta bancária, por exemplo.

Nesse contexto, existem diversas vulnerabilidades dos usuários ou dos equipamentos que podem ser aproveitadas por golpistas. Segundo o Comitê Gestor da Internet no Brasil, em sua Cartilha de Segurança para Internet (2020), os ataques podem ocorrer no ambiente da Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas.

3.2 AMEAÇAS E VULNERABILIDADES

O aumento do número de ativos de informação gerou a necessidade de um estudo mais aprofundado para a proteção de suas vulnerabilidades. Mitnick e Simon (2003), citam em seu livro o seguinte:

> À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

Os autores ainda afirmam que o conhecimento para a realização de ataques contra dispositivos é complexo, fazendo com que as ameaças se concentrassem no elo mais fraco de qualquer rede: o usuário ou cliente (MITNICK E SIMON, 2003).

A proteção dos dispositivos pode ser feita através de protocolos e programas diversos, os quais podem ser implementados pelo gestor da rede, exemplo do firewall, ou contratados pelo usuário, como os antivírus pagos. Entretanto a prevenção de ataques diretos ao comportamento do usuário exige atenção.

Um dos métodos de ataque direto ao usuário é a Engenharia Social, que consiste em uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações (COMITÊ GESTOR DA INTERNET NO BRASIL, 2020). No contexto da segurança da informação, estas ações têm por objetivo aplicar golpes, ludibriar ou obter informações sigilosas e importantes da vítima.

Cardoso e Nunes (2020) dizem que os ataques realizados com maior probabilidade de êxito são aqueles que envolvem diversas técnicas de ataque e normalmente se iniciam com técnicas de Engenharia Social. O engenheiro social busca coletar o maior número de informações de seu alvo, criando com isso uma "isca" que atraia a vítima mais facilmente. Essa modalidade se enquadra como Phishing.

3.3 PHISHING

Conforme listado pelo Kaspersky Team (2022), cerca de 15,4% dos ataques de mensagens fraudulentas do tipo Phishing realizados, em 2021, no mundo foram feitos contra usuários brasileiros, somando mais de 5 milhões de tentativas de ataques desse tipo no ano. O documento ainda sugere que a principal técnica empregada foi a de adware que exibe propaganda indesejada às vítimas buscando obter lucro e programas que visam obter controle total do celular.

O Phishing Scam constitui-se de uma ameaça que busca obter dados pessoais ou financeiros pela utilização combinada de meios técnicos e engenharia social, (COMITÊ GESTOR DA INTERNET NO BRASIL, 2020).

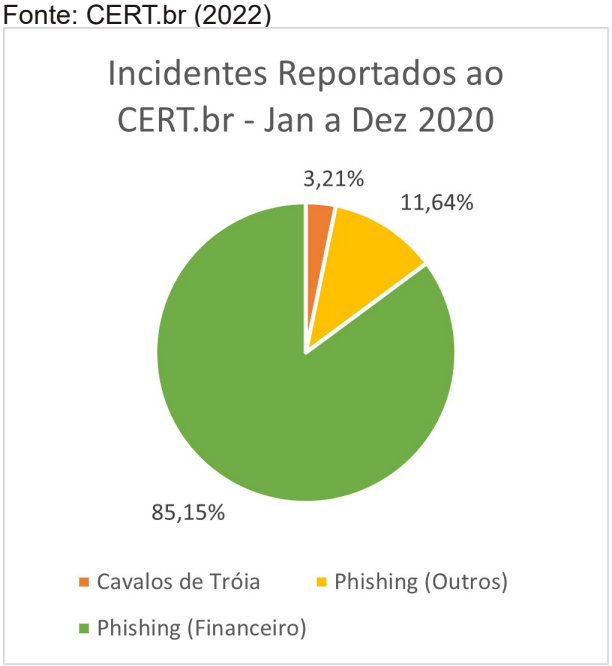
O documento "Mensagens fraudu-lentas: Phishing" da UFRGS (2022), define o Phishing como "a versão eletrônica do conto do vigário". Dessa maneira, o usuário é induzido a agir conforme um comportamento esperado com base na isca utilizada em uma página ou aplicação maliciosa, onde seus dados serão capturados.

Golpes do tipo Phishing constituem uma das principais ameaças na atualidade. E-mails e mensagens fraudulentas são reportadas e computadas por diversas entidades.

No gráfico 1, que segue, pode-se observar que das tentativas de ataque reportadas ao portal CERT.br apenas pouco mais de 3% não foram de ataques do tipo Phishing.

GRÁFICO 1 – Incidentes reportados ao CERT.br

Fonte: CERT.br (2022)



3.3.1 FASES DE UM ATAQUE TIPO PHISHING SCAM

Os ataques do tipo Phishing podem ser focalizados ou empregar as técnicas de envio de mensagens do tipo SPAM onde muitos usuários recebem a tentativa de golpe. De acordo com Martins (2008), indepen-dentemente do enfoque da fraude, esses ataques costumam seguir as mesmas fases, sendo elas:

3.3.1.1 PLANEJAMENTO

Nessa fase o atacante define as demandas iniciais da fraude tais como: tipo de alvo, artimanhas e objetivos do golpe.

3.3.1.2 PREPARAÇÃO

Fase em que o atacante desenvolve todo o material necessário ao ataque. Inclui criação e-mail e páginas falsas, programação de equipamentos, criação de redes e/ou servidores.

3.3.1.3 ATAQUE

Fase na qual ocorre efetivamente o ataque que pode ocorrer por meio de aplicações de mensagens instantâneas, e-mails, sites e páginas falsas ou infecção de redes.

3.3.1.4 COLETA

Etapa em que os dados obtidos pelo golpista são coletados. Nessa fase o golpista espera ter disponível dados que a vítima inseriu em uma das plataformas maliciosas criada pelo fraudador.

3.3.1.5 FRAUDE

Agora em posse dos dados da vítima, o fraudador utiliza os dados coletados para obter a vantagem desejada. Podendo passar-se pela vítima, o golpista pode empregar os dados para obter vantagem pecuniária, seja empregando os dados bancários da vítima ou venda desses dados a quem interessa.

É importante ressaltar que o autor do golpe pode ter motivações diversas além da costumeira vantagem financeira.

3.3.1.6 PÓS-ATAQUE

Nessa fase o atacante busca apagar todos os registros do golpe realizado e desativar a estrutura montada para o golpe. É onde realiza-se também um balanço dos resultados obtidos e lavagem do recurso obtido, se for o caso.

3.4 OS ATAQUES DO TIPO PHISHING EM AMBIENTE MILITAR

Todo usuário deve ter em mente que a rede que hospeda sua conexão pode ser afetada pelas suas ações quando conectado. Um ataque de Phishing pode resultar em coleta ou subscrição de dados disponíveis na rede.

Exemplos disso são os Ataques Cibernéticos Titan Rain, em 2003, e Shady Rat, em 2006, quando, possivelmente, hackers de origem chinesa teriam enviado Phishing por meio de e-mail personalizado para pessoas de várias instituições do mundo, sendo a grande maioria contra americanos (YIP, 2016).

Aplicações de apoio a decisão com funcionamento em rede podem de igual modo ser afetadas, impactando decisiva-mente no Comando e Controle (C^2) do escalão atacado.

Dados disponíveis em softwares como o C^2 em combate e Pacificador, amplamente utilizados pelo Exército Brasileiro, podem ser passíveis de sofrer inserções de informações incorretas, como a de posições geográficas da tropa ou dados de planejamento falsos. Isso seria possível de ocorrer por meio da coleta de credenciais do gestor do sistema alvo.

Com a atual guerra Russa-Ucraniana (2022) é possível ver o emprego massivo do Phishing como meio de se obter dados do inimigo, conforme se vê na citação abaixo.

> Hackers de Rússia e Belarus atacam Ucrânia com Phishing, diz Google.
> [...] O Grupo de Análise de Ameaças do Google, que trabalha na prevenção a hackers e envio de avisos sobre eles aos usuários, disse em uma publicação na segunda-feira (7) que nas últimas duas semanas o grupo de hackers russo FancyBear, também conhecido como APT28, enviou e-mails de Phishing para a empresa de mídia ucraniana UkrNet.

> [...] Em outro caso, o Ghostwriter/UNC1151, de Belarus, e que o Google descreveu como uma ameaça, vem tentando roubar credenciais de contas por meio de tentativas de Phishing contra os governos polonês e ucraniano e organizações militares. (REUTERS, 2022)

3.5 EXPERIMENTO

Segundo Gil (2008), o experimento representa o melhor exemplo de pesquisa científica. Seguindo essa ideia, foi realizada uma pesquisa experimental, de acordo com a metodologia antes apresentada.

Na elaboração da pesquisa em tela, utilizou-se dois grupos, integrantes de uma OM da Guarnição de Brasília, valor unidade, para a realização de um estudo de caso. Após autorizado pelo Comandante dessa instituição, conforme solicitação feita por meio do Documento Interno do Exército (DIEx) anexado a este artigo, deu-se início ao estudo que contou com a participação de duas subunidades dessa OM.

Os grupos experimental e de controle foram selecionados e cada um deles contou com o efetivo de 150 militares, integrantes de duas subunidades diferentes.

Ao grupo experimental foi entregue um folheto acerca de Boas Práticas contra o Phishing Scam¸ que consta no Apêndice A.

Já o efetivo do grupo de controle não recebeu nenhuma orientação sobre como proceder em caso de ser alvo de Phishing.

Para o experimento, um ataque simulado foi realizado por meio do aplicativo de mensagens Whatsapp, visando o melhor aproveitamento de êxito nos resultados obtidos.

O ataque constou do envio de uma propaganda, figura 1 e 2, e de uma mensagem, figura 3, por meio do aplicativo de mensagens instantâneas Whatsapp dos integrantes de ambos os grupos.

FIGURA 1 – Propaganda distribuída (frente)

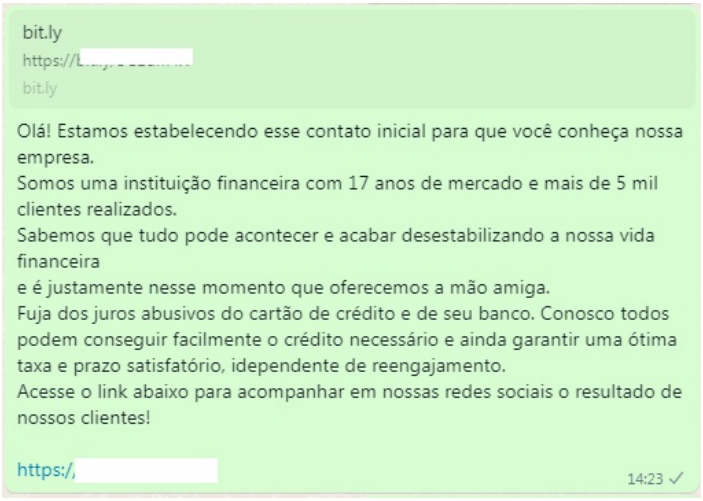
Fonte: os autores, 2022.

FIGURA 2 – Propaganda distribuída (verso)

Fonte: os autores, 2022.

Na mensagem, figura 3 abaixo, constava informações acerca de uma oportunidade de crédito de um órgão fictício, bem como um link para o acesso.

FIGURA 3 – Mensagem enviada em aplicativo de mensagens instantâneas WhatsApp



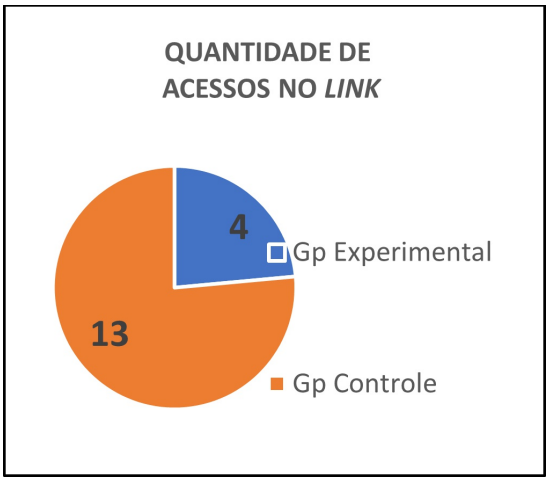
Fonte: os autores, 2022.

O link direcionava o usuário para um site não existente, não causando nenhuma ação danosa ao militar que clicou, nem a OM, tampouco houve qualquer tipo de coleta de quaisquer informações pessoais, de hardware ou software do indivíduo. O objetivo era somente a coleta da quantidade de acessos ou clicks realizados por cada grupo.

Por causa de uma proteção do próprio aplicativo Whatsapp, o link de acesso somente ficava válido para acesso direto se a vítima adicionasse o número de telefone da origem das mensagens em sua lista de contatos.

Os resultados obtidos foram os observados na figura 4 adiante:

FIGURA 4 – Quantidade de acessos no link

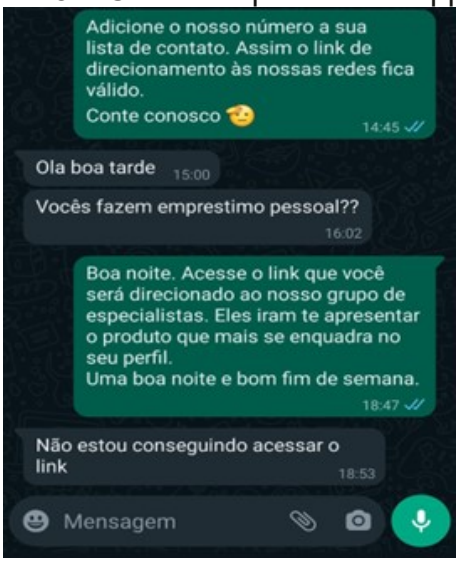


Fonte: os autores, 2022

Nota-se que o número de acessos ao link malicioso enviado por meio da mensagem pelo grupo de controle foi 325% maior do que do grupo que teve acesso ao folheto do Apêndice A. Correlacionando essa diferença com a apresentação do folheto para os indivíduos do grupo experimental, conclui-se que houve uma diminuição direta de aproximadamente dois terços no número de cliques no link malicioso, o que representa diretamente uma diminuição de usuários infectados caso não fosse um ataque simulado.

Alguns indivíduos ainda tentaram contato com a instituição fictícia através do WhatsApp, como exemplificado na figura 5, buscando mais informações acerca da oportunidade ofertada, abrindo brechas para que fossem vítimas de um ataque de Engenharia Social mais individualizado.

FIGURA 5 – Conversa pelo Whatsapp



Fonte: os autores, 2022.

3.6 PROTEÇÃO DO USUÁRIO

Segundo a "Recomendação nº 01/2019: golpe de Phishing" do Departamento de Segurança da Informação do Governo Brasileiro (2022), ainda que a utilização de ferramentas antiphishings ou antimalwares previna ou mitigue parte considerável desses golpes, alguns deles chegam às vítimas sem serem detectadas. Isso ocorre porque muitas vezes as mensagens maliciosas são enviadas de remetentes conhecidos (que podem ter sido invadidos ou forjados) ou ainda por se utilizarem quase que exclusivamente o ataque

de engenharia social para persuadir as vítimas.

O National Cyber Security Centre (2022), divide a defesa de ataques de Phishing contra uma organização em 4 camadas. Para efeitos desse artigo, será dado foco na camada 2 (dois) que envolve orientações para os usuários identificarem e reportarem ataques Phishing.

3.6.1 IDENTIFICAÇÃO

De maneira simples, as orientações devem evitar a ocorrência de dois principais fatos: que o usuário não divulgue informações sensíveis e que não efetue o clique em links maliciosos. Para que isso não ocorra, o usuário deve ter conhecimento para identificar as mensagens suspeitas. O Departamento de Segurança da Informação do Governo Brasileiro (2022), ainda cita os elementos presentes nas mensagens que ajudam a caracterizá-las:

- São mensagens que chamam a atenção, apresentando-se como originária de instituições familiares ao usuário (seus bancos, Serasa, Receita Federal etc.);
- Persuadem o usuário da necessidade de recadastro de senha, atualizações de software, recebimento de prêmio ou vantagem financeira etc;
- Solicita dados pessoais, tais como login e senha, dados bancários, número de CPF, telefone e endereço, o que normalmente instituições não solicitam via e-mail;
- A mensagem possui tom de urgência, ligada a ameaças de bloqueio, suspensão de serviços, etc.;
- Solicitações de cliques em links, o que deve sempre servir de fonte de suspeita. Tais links servem para redirecionar o usuário para um site malicioso, com páginas imitando o formato e arte de instituições legítimas. Uma armadilha comum é a existência de um link com a promessa de não se receber mais outro tratando do assunto citado no atual;
- Ocorrências de erros ortográficos, por vezes grosseiros, que também podem indicar que o texto original foi traduzido por meio de algum aplicativo; e
- A mensagem pode abordar assuntos relacionados a eventos atuais ou épocas específicas, como os relativos ao envio do Imposto de Renda, enviados pela Receita Federal.

3.6.2 PREVENÇÃO

O Comitê Gestor da Internet no Brasil (2020) enumera algumas medidas de prevenção ao Phishing:

- Fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;
- Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há por que recadastrar dados ou atualizar módulos de segurança);
- Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos; e
- Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
- Seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador Web;
- Verifique o link apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o link real para o phishing. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso; e
- Utilize mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing.

O usuário se conscientizando de que ele é responsável pelas informações que ele detém, sejam elas pessoais ou corporativas, e estando atento de que existem pessoas interessadas em acessá-las, já dificulta a probabilidade de um ataque.

4. CONCLUSÕES

A busca pela eficiência nas orientações de prevenção e identificação de ataques Phishing tem grande validade. No desenvolvimento do experimento foi possível testar uma orientação simples e de fácil entendimento e planejada para o público a que se destinava. Foi possível avaliar o alcance das orientações emanadas na cartilha e comprovar a validade de emprego desse tipo de técnica para a prevenção de uma das maiores ameaças na internet.

Os resultados do experimento mostram que uma orientação básica, simples e direta pode sim ser eficaz. Tal premissa não se aplica somente aos ataques do tipo Phishing Scam, diversas outras ameaças podem ser combatidas com esse tipo de abordagem.

As vulnerabilidades descobertas a cada dia fazem com que o conhecimento do usuário sobre proteção de dispositivos de tecnologia da informação tenha que estar também atualizado. Muitas vezes interessado somente na utilização do serviço oferecido, o cliente agora deve também preocupar-se se é confiável, legítimo e seguro.

A manutenção do estado de preparação do público interno em segurança de redes já é uma tarefa difícil. O Exército Brasileiro ganha um óbice além das outras instituições por possuir muitos jovens que anualmente entram na Força e tem acesso aos mais variados tipos de informações inerentes às atividades militares. Uma capacitação simples e objetiva é primordial para a segurança dos dados que transitam nas redes internas de uma OM.

As orientações de segurança em TI aos integrantes de uma rede devem ser focadas nos ataques de maior ocorrência na rede em questão. Um ataque que usa engenharia social é focado em um público previamente estudado pelo atacante. Da mesma maneira, as orientações devem ser específicas de acordo com o perfil do usuário. Uma busca constante pelo desenvolvimento de técnicas de segurança, objetiva a efetividade dos procedimentos contra invasores, evitando até os ataques mais planejados e complexos.

5. REFERÊNCIAS

CARDOSO, Daniel Moura Félix; NUNES, Daniel Bomfim. Proteção contra ataques de phishing scam no Exército Brasileiro. O Comunicante, Brasília, v. 10, n. 1, p. 5-15, jan. 2020.

CERT.BR. Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/fraude.html. Acesso em: 25 maio 2022.

COMER, Douglas Earl. Redes de Computadores e Internet. 6ª. ed. [S. l.]: Bookman Editora, 2016. 584 p. ISBN 8582603738, 9788582603734.

COMITÊ GESTOR DA INTERNET NO BRASIL. Cartilha de Segurança para Internet. 2. ed. São Paulo: Cert.Br, 2012. 142 p. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 30 maio 2022. Cartilha de Segurança para Internet Cert.Br (2020)

Departamento de Segurança da Informação do Governo Brasileiro (ed.). Recomendação nº 01/2019 Golpe de Phishing. Disponível em: https://www.gov.br/ctir/pt-br/centrais-de-conteudo/publicacoes/recomendacoes-pdf/2019/recomendacao_2019_01_golpe_phishing.pdf. Acesso em: 01 jun. 2022.

DFNDR LAB. Relatório da Segurança Digital no Brasil: primeiro trimestre - 2018. Primeiro trimestre - 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: 23 maio 2022.

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas S.A, 2008.

KASPERSKY TEAM (ed.). Ciberataques crescem 23% no Brasil em 2021. Disponível em: https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021 pesquisa/18020/ #:~:text=Ao%20comparar%20os%20oito%20 primeiros,e%20Peru%20(507%20mil. Acesso em: 25 maio 2022.

MARTINS, Diego de Oliveira. Phishing Scam: A fraude do Século 21, 40 f. Universidade Federal do Rio de Janeiro, 2008.

MITNICK, Kevin D.; SIMON, William L.. A Arte de Enganar: ataques de hackers - controlando o fator humano na segurança da informação. São Paulo: Pearson Universidades, 2003.

NATIONAL CYBER SECURITY CENTRE. Phishing attacks: defending your organisation. defending your organisation. Disponível em: https://www.ncsc.gov.uk/ guidance/phishing. Acesso em: 20 maio 2022.

REUTERS. Hackers de Rússia e Belarus atacam Ucrânia com phishing, diz Google. Disponível em: https://g1.globo.com/ tecnologia/noticia/2022/03/08/hackers-de-russia-e-belarus-atacam-ucrania-com-phishing-diz-google.ghtml. Acesso em: 20 maio 2022.

UFRGS. (ed.). Mensagens Fraudulentas: phishing. Disponível em: http://www.ufrgs.br/ tri/Documentos/mensagens-fraudulentas-phishing. Acesso em: 26 maio 2022.

YIP, Ki Nang. Phishing Attacks in the Gover-nment and Military. 2016. Disponível em: https: //resources.infosecinstitute.com/topic/ phishing-at tacks-in-the-government-and-military/. Ace-sso em: 15 jun. 2022.

APÊNDICE A – FOLHETO DE BOAS PRÁTICAS DE PREVENÇÃO AO PHISHING SCAM

GOLPE DE PHISHING

FIQUE LIGADO PRA NÃO CAIR NESSE TIPO DE Ggolpe!

O Brasil foi o país mais atacado por golpes do tipo Phishing Scam no mundo em 2021*

Neste tipo de ameaça o golpista te induz a ceder suas informações. Normalmente empregam mensagens fraudulentas elaboradas para dispertar o interesse da vítima.

*Fonte: Portal Kaspersky.

Leia o verso para algumas dicas de prevenção.

COMO SE PREVENIR

Por que caímos:

- Urgência
- Desejo de agradar
- Curiosidade
- Ambição
- Medo
- Orgulho

O que eles desejam:

Senhas

Dados bancários

Dados pessoais

Sinais indicadores de fraude:

- Erros de gramática e/ou digitação.
- Endereço do remetente.
- Algo que pareça ser muito bom pra ser verdade.
- Mensagens não solicitadas que te indiquem:
  - Links a serem clicados.
  - Páginas de login ou autenticação.
  - Anexos suspeitos.

Para reportar incidentes envie um e-mail de notificação para cert@cert.br

ANEXO A – SOLICITAÇÃO DE APOIO A PESQUISA CIENTÍFICA

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ESCOLA DE COMUNICAÇÕES
(C Instr Trans do 1º BE/1921)
ESCOLA CORONEL HYGINO CORSETTI

DIEx nº 26-SPGD/Div Ens/Cmdo
EB: 64499.001594/2022-18

Brasília, DF, 26 de maio de 2022.

Do Comandante da Escola de Comunicações
Ao Sr Comandante do Batalhão da Guarda Presidencial
Assunto: Solicitação de apoio a pesquisa científica

1. Solicito a autorização para que os **1º Ten** Caio de Souza **Alves** e **1º Ten** Ricardo Henrick Santos **Caetano**, alunos do Curso de Oficial de Comunicações de 2022, ministrado pela Es Com, possam realizar um trabalho de campo no BGP, contribuindo com a pesquisa científica que estão realizando, visando atender o requisito de entrega de trabalho científico para aprovação na pós-graduação "*lato-sensu*" do referido curso.

2. O objetivo da pesquisa é verificar se os militares do Exército sabem identificar e como proceder caso sejam alvos da ameaça cibernética "*Phishing Scam*", que hoje é atualmente utilizada por organizações criminosas com foco em fraudes e golpes, mas pode também ser utilizada como uma forma de obtenção de informações inimigas em situação de operações no amplo espectro dos conflitos armados.

3. A atividade será desenvolvida da seguinte forma:

a. Serão necessárias duas SU do BGP para a realização do trabalho de campo. Para isso, será necessário a disponibilização da relação telefônica de seus integrantes, preferencialmente os que possuírem contas no aplicativo "Whatsapp";

b. Uma mensagem será enviada ao aplicativo de mensagens instantâneas "*Whatsapp*" dos militares, contendo informações acerca de uma oportunidade de crédito de um órgão fictício, bem como um "*link*" para o acesso;

c. O "*link*" irá direcionar o usuário para um site não existente, não causando nenhuma ação danosa ao militar ou a OM, nem mesmo a coleta de quaisquer informação pessoal;

d. O objetivo será contabilizar a quantidade de acessos de cada SU, comparando futuramente os resultados obtidos; e

e. Apenas uma das SU receberá, antes do envio do "*link*", um folheto acerca de Boas Práticas contra o "*Phishing Scam*", alertando sobre o perigo dessa atividade. Isso visa realizar a comparação entre os militares da SU que receberá o folheto a respeito do "*Phishing Scam*" *(amostra de controle)* com os da SU que não receberá (amostra).

4. Outrossim, visando não prejudicar a execução do trabalho de campo, solicito, ainda, que não seja divulgada a atividade antes da execução do envio do link aos militares das SU (amostras do trabalho). Após isso, poderá ser divulgada, servindo até como forma de alerta e instrução da própria OM em relação ao risco do ""*Phishing Scam*".

ENIO CORRÊA DE SOUZA - TC
Comandante da Escola de Comunicações

"1822-2022 - BICENTENÁRIO DA INDEPENDÊNCIA DO BRASIL SOBERANIA E LIBERDADE"