CONSCIENTIZAÇÃO DE PHISHING: ESTRATÉGIAS E IMPACTO NA SEGURANÇA CIBERNÉTICA

Ten MATHEUS AGUIAR **SELLA**
Ten **BRENDO BASTOS** MACEDO
Ten MATHEUS **MARQUES** DA SILVA DA PAZ BATISTA

RESUMO

Esta pesquisa buscou a conscientização acerca dos riscos provenientes de ameaças Phishing e, para tanto, buscou-se a implementação de uma ferramenta capaz de testar o grau de exposição de um determinado grupo de usuários a este tipo de ameaça. Foi realizada uma pesquisa aplicada de caráter exploratório com abordagem qualitativa, utilizando-se de uma metodologia cien#fica de análise bibliográ$ca com o intuito de evidenciar as t%cnicas de Phishing mais comuns e os métodos de conscientização mais eficazes. Uma vez levantados esses dados, partiu-se então para a de$nição da ferramenta a ser utilizada como "Phishing A) areness Tool", ferramenta esta capaz de prover recursos de simulação de Phishing, engajamento do usuário, detecção automatizada, avaliação con#nua, além de propiciar, relatórios e métricas. Visando este cenário, a ferramenta escolhida foi a - ophish. Para galgar terreno e atingir o objetivo estabelecido, foi empregada uma pesquisa aplicada de caráter explorat"rio com abordagem qualitativa utilizando-se de uma metodologia cien#fica de análise experimental no desenvolvimento de simulação de Phishing na ferramenta - ophish, a qual foi utilizada em teste prático com determinado grupo de indivíduos. De posse dos referidos testes e após uma análise detalhada de seus resultados, foi possível gerar um módulo de feedback e treinamento para os usuários por meio de uma cartilha de conscientização de Phishing.

Palavras-chave: *Phising, Conscientização, Ferramenta, 2iscos, Gophish*

1 INTRODUÇÃO

A segurança cibernética é uma preocupaçã o crescente em organizações militares devido ao aumento de ataques de *phishing*. Segundo Cardoso e Nunes (2020), "o ataque de *phishing* é uma das formas mais comuns de engenharia social, visando roubar informações sensíveis".

Isto posto, a finalidade desta pesquisa é propiciar a conscientização dos riscos e ameças referentes ao phishing dentro de determinada organização.

A evolução da tecnologia trouxe consigo diversos avanços no cotidiano de todos os indivíduos, entretanto, toda tecnologia, quando utilizada com más intenções, pode ser uma ferramenta extremamente perigosa. Dentre o vasto universo de mecanismos tecnológicos maliciosos, está o *phishing,* o qual se destaca como uma das ameaças mais insidiosas e amplamente disseminadas. Neste estudo, estará em voga a conscientização sobre *phishing*, suas estratégias e os impactos que essa prática tem na segurança das informações.

A conscientização sobre *phishing* é fundamental para proteger indivíduos e organizações contra esses ataques. Afinal, a primeira linha de defesa está nas mãos dos próprios usuários. Quando as pessoas compreendem as táticas empregadas por criminosos ficam alertas aos os sinais de *phishing*, a probabilidade de sucesso desses ataques diminui consideravelmente.

1.1 CONTE5TUALIZAÇÃO DO ESTUDO

O termo *phishing* é uma palavra derivada do inglês *"fishing"* (pesca) e reflete a ideia de lançar iscas *para* atrair vítimas desavisadas. Trata-se de uma técnica sofisticada em que atacantes se passam por entidades confiáveis (como bancos, empresas ou serviços online) para enganar usuários e obter informações sensíveis, como senhas, dados bancários e informações pessoais. Esses ataques ocorrem principalmente por meio de e-mails, mensagens de texto, redes sociais e inclusive clonados.

1.2 JUSTIFICATIVA

O presente estudo justifica-se frente à latente persistência de ataques *phishing*, representando assim uma possível ameaça presente para qualquer setor. Fato esse corroborado por Carvalho (2022):

> Dados do relatório *Strategic Securit6 Surve6* produzido pela *Dar0 2eading* apontam que, em 2021, 53% das organizações citaram o phishing como causa direta de incidentes de segurança.

Apesar do referido cenário, pouco há sobre a conscientização de tais ameaças e, visando preencher tal lacuna e entregar uma ferramenta clara e objetiva, este estudo produzirá uma cartilha pautada nos resultados de pesquisa bibliográfica combinada com uma pesquisa exploratória.

147DEFINIÇÃO DO PROBLEMA DE PESQUISA

Diante da crescente sofisticação dos ataques de *phishing* e da constante evolução das técnicas utilizadas por mentes mal-intencionadas, como é possível promover uma conscientização eficaz entre os usuários? Quais estratégias são mais adequadas para educar e proteger as pessoas contra essas ameaças? Como mostrar de maneira tangível os riscos dessa ameaça para o usuário?

1.4 OBJETI6OS DA PESQUISA

Este trabalho pretende: delimitar os principais atributos de uma ferramenta para testes de exposição ao *phishing*; investigar as estratégias de conscientização de phishing mais eficazes; avaliar o impacto dessas estratégias na segurança cibernética e propor diretrizes para a implementação de uma cartilha de conscientização e prevenção contra-ataques *phishing.*

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

O presente estudo está organizado da seguinte forma:

1.5.1 INTRODUÇÃO

Definida pela contextualizaçto, justificativa, problema de pesquisa, relevância e objetivos.

1.5.2 DESENVOLVIMENTO

Breve apresentaçto da problemática na qual a pesquisa se insere e se propõe a entregar uma soluçto viável de mitigaçto.

1.5.2.1 REVISÃO DA LITERATURA

A partir da literatura revisada, trata das estratégias de conscientizaçto, técnicas de *phishing* mais latentes, definir os principais atributos de uma ferramenta para testes de exposiçto ao *phishing* e escolhê-la de fato, além de delimitar o ativo que será empregado para disponibilizaçto online do serviço da campanha.

1492.2 METODOLOGIA DE PESQUISA

Visa expor um determinado grupo a simulações de *phishing* de maneira controlada e assim poder analisar e explorar os resultados obtidos da experimentaçto.

Sendo assim, a pesquisa foi conduzida em duas fases: uma fase de pré-campanha, na qual foi avaliada a vulnerabilidade inicial dos participantes, e uma fase de pós-campanha, na qual foi medida a eficácia da campanha educativa. Foram utilizados questionários e simulações de ataques de *phishing* para coletar dados

1.5.247APRESENTAÇÃO E ANÁLISE DE DADOS

Análise crítica e interpretativa dos dados coletados durante a pesquisa exploratória a fim de obter reflexões sobre os impactos observados.

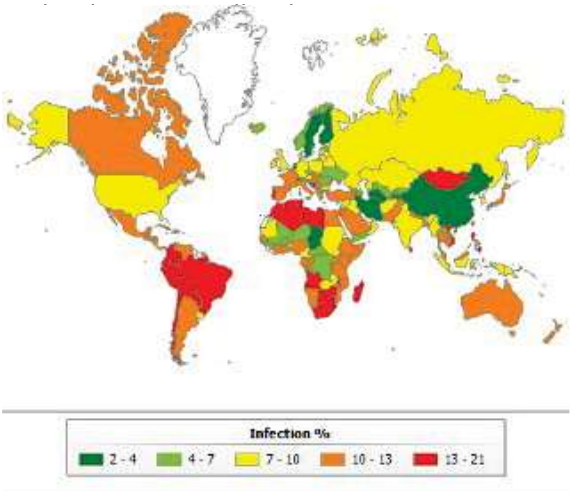
1.5.2.4 DISCUSSÃO DOS RESULTADOS

Síntese dos principais produtos obtidos com o estudo de modo a propiciar recomendações para a prática da confecçto da cartilha.

2 DESENVOLVIMENTO

A conscientização sobre phishing é uma componente essencial da segurança cibernética moderna. Com o aumento da sofisticaçto dos ataques, as organizações precisam adotar estratégias eficazes para educar seus funcionários e proteger seus dados.

Nos últimos anos, o Brasil tem registrado um aumento significativo nos casos de *phishing*, um t ipo de fraude eletrônica na qual criminosos t entam obter informações pessoais e financeiras das vítimas por meio de mensagens enganosas. De acordo com um relatório da Kaspersky (empresa de cibersegurança), houve um crescimento de significativo nas tentativas de *phishing* no Brasil entre



Fonte: kaspersky, 2023.

O aumento expressivo está associado à retomada das atividades econômicas pós-pandemia e ao uso de ferramentas de Inteligência Artificial para criar conteúdos fraudulentos de forma automatizada.

Não obstante, o Brasil lidera o *ranking* de países mais afetados por ataques de *phishing* na América Latina, com 134 milhões de tentativas de ataque registradas no período analisado. Os setores mais visados incluem o governo e o setor financeiro, além dos usuários comuns da internet.

A pandemia de COVID-19 também contribuiu para o aumento dos ataques de phishing, com criminosos aproveitando a desinformação e o medo generalizado para disseminar golpes relacionados a programas de auxílio social e outras falsas promessas. Em 2021, por exemplo, houve um aumento de 41% nos ataques de *phishing* em comparação ao ano anterior.

FIGURA 2: Tentativas de Phishing na Pandemia

Fonte: Kaspersky Lab, 2020.

As informações obtidas evidenciam a relevância de implementar medidas de segurança robustas e de promover a conscientização dos usuários para a identificação e prevenção de tentativas de *phishing*. A educação digital e o uso de tecnologias de proteção são fundamentais para mitigar os riscos associados a esse tipo de ameaça.

2.1 REVISÃO DA LITERATURA

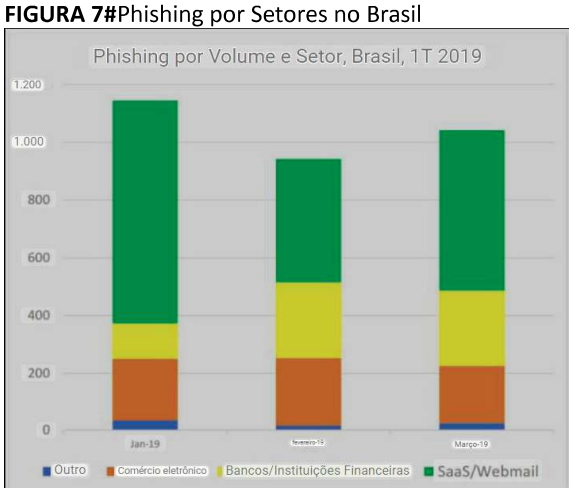
Inicialmente, é necessário definir de maneira clara o que é e como funciona um ataque *phishing*. Segundo *7 alwareb6tes* (2024):

> O *phishing* é uma forma de crime cibernético em que os criminosos tentam obter informações confidenciais por e-mail com links fraudulentos, solicitando que você preencha um formulário com suas informações de identificação pessoal. Em seguida, eles podem usar essas informações para obter suas credenciais on-line para perfis de mídia social, contas bancárias e muito mais.
>
> O *phishing* envolve o envio de mensagens falsas que parecem reais e urgentes, como e-mails, chamadas telefônicas ou mensagens de texto, para enganar as pessoas a compartilharem informações confidenciais. Os golpistas se passam por entidades legítimas, como bancos, e criam um senso de urgência para persuadir as vítimas a inserir dados

pessoais em sites falsos. Isso pode levar ao roubo de ident idade e a perdas financeiras.

Programas de treinamento contínuo ajudam os elementos de uma organização a reconhecer e responder adequadamente a tentativas de phishing, portanto, realizar simulações periódicas pode ajudar a identificar vulnerabilidades e reforçar o treinamento. Em vez de punir os indivíduos que caem em simulações, uma abordagem positiva que incentiva a identificação correta e recompensa os esforços pode ser mais eficaz. Afinal, segundo Noonan (2024), "O *Phishing* é um problema grave para empresas de todas dimensões e de todos os setores", situação essa demonstrada a seguir com gráfico que demonstra uma crescente dos casos no Brasil

FIGURA 7#Phishing por Setores no Brasil



Fonte: Phishing Activity Trends Report, produzido pelo Anti-Phishing Working Group (APWG).

Sendo assim, vale ressaltar a seguinte observação de Probst (2024):

> […] Além disso, novas tecnologias utilizadas por agentes maliciosos para além de sua finalidade legítima, como a inteligência artificial, aumentam o potencial danoso desta técnica criminosa. Por isto, implementar campanhas *anti-phishing* não é apenas uma medida preventiva, mas uma estratégia essencial de segurança.

Atualmente, as técnicas de phishing mais sofisticadas incluem o uso de IA, onde cibercriminosos criam mensagens personalizadas para enganar até os usuários mais experientes. O *vishing* utiliza chamadas telefônicas para obter dados pessoais, enquanto o *smishing* envia mensagens de texto enganosas. No *phishing* de aplicativos, criminosos desenvolvem apps falsos que imitam os legítimos. O voicemail *phishing* usa mensagens de voz falsas, e a engenharia social manipula psicologicamente as vítimas para obter informações confidenciais. Essas técnicas estão se tornando mais complexas, exigindo maior vigilância e medidas de segurança robustas de todos.

Desse modo, observa-se que o *phishing* constitui uma técnica de engenharia social empregada por agentes mal-intencionados com o intuito de ludibriar usuários e obter informações sensíveis, tais como senhas e dados bancários. Uma das maneiras de implementação dessa técnica é a utilização do - *ophish*, uma valiosa ferramenta de código aberto que possibilita a criação e execução de campanhas de *phishing* de maneira simplificada. Conforme estudos recentes, o - *ophish* é amplamente utilizado tanto por pesquisadores de segurança quanto por criminosos, devido à sua facilidade de uso e eficácia (SILVA, 2023).

A estrutura de uma campanha de *phishing* utilizando o - *ophish* geralmente envolve múltiplas etapas. Normalmente, o atacante começa por configurar um servidor de *phishing*, onde são hospedadas páginas fraudulentas que imitam sites legítimos. Subsequentemente, são elaborados e-mails de *phishing* que contêm links para essas páginas fraudulentas. Esses arquivos são enviados a um elevado número de vítimas potenciais. Quando uma vítima clica no link e insere suas informações na página fraudulenta, esses dados são capturados pelo servidor de *phishing* (SOUZA, 2022).

Estudos indicam que as técnicas de engenharia social presentes nos e-mails de *phishing* aumenta significativamente a taxa de sucesso das campanhas. Isso é realizado através da coleta de informações sobre as vítimas, como nomes e cargos, para tornar os e-mails mais convincentes. Ademais, a utilização de técnicas de *spoofing* de e-mail, onde o endereço do remetente é falsificado para parecer que o e-mail foi enviado por uma

fonte confiável, também é comum (FERREIRA, 2021).

A eficácia do - *ophish* e de outras ferramentas de *phishing* ressalta a importância de medidas de segurança robustas, como a educação dos usuários e a implementação de autenticação multifator. Conforme apontado por especialistas, a conscientização sobre as técnicas de *phishing* e a adoção de boas práticas de segurança são essenciais para mitigar os riscos associados a essas ameaças (COSTA, 2020).

O - *ophish*, uma ferramenta de *phishing* de código aberto e gratuita, o qual foi concebido para atender às necessidades de empresas e testadores de penetração, proporcionando um ambiente robusto para a criação de campanhas de simulação de *phishing*. A escolha do - *ophish* como ferramenta de conscientização sobre os perigos dos golpes cibernéticos é justificada por diversos fatores positivos, conforme delineado em seu manual.

FIGURA 4: - *ophish,* código aberto

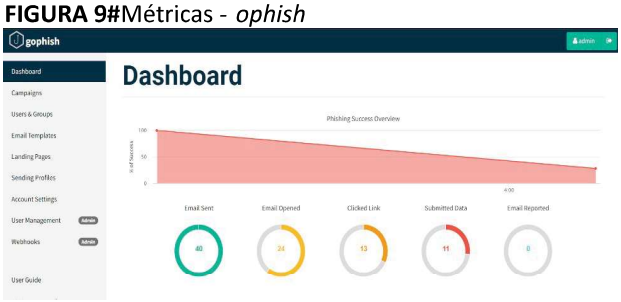
Fonte: Cyberpunk (2024).

Primeiramente, o - *ophish* destaca-se pela sua facilidade de uso e interface intuitiva, permitindo que usuários que detenham conhecimentos técnicos limitados possam configurar e executar campanhas de *phishing* de maneira eficaz. Essa acessibilidade é crucial para a implementação de programas de conscientização em larga escala, onde a simplicidade e a eficiência são essenciais (GOPHISH, 2024).

Além disso, o - *ophish* oferece flexibilidade na personalização das campanhas, permitindo a criação de e-mails e páginas de *phishing* que imitam com precisão os sites legítimos. Essa capacidade de personalização é fundamental para simular cenários realistas e, assim, aumentar a eficácia do treinamento dos usuários. A personalização também facilita a adaptação das campanhas às necessidades específicas de diferentes organizações, tornando o treinamento mais relevante e impactante (GOPHISH, 2024).

Outro ponto positivo do - *ophish* é a capacidade de monitoramento e análise detalhada dos resultados das campanhas. A ferramenta fornece métricas abrangentes sobre o comportamento dos usuários, como taxas de abertura de e-mails, cliques em links e submissão de dados. Essas informações são valiosas para identificar vulnerabilidades e ajustar as estratégias de segurança conforme necessário. A análise detalhada permite uma avaliação precisa da eficácia das campanhas de conscientização e do nível de preparação dos usuários contra-ataques de *phishing* (GOPHISH, 2024).

FIGURA 9#Métricas - *ophish*



Fonte: Os autores.

Por fim, o - *ophish* é uma ferramenta altamente escalável, capaz de suportar campanhas de *phishing* em organizações de qualquer tamanho. Sua arquitetura de código aberto permite que seja adaptado e expandido conforme as necessidades específicas de cada organização, garantindo que a ferramenta possa crescer junto com a empresa e suas demandas de segurança (GOPHISH, 2024).

Em suma, a escolha do - *ophish* para a conscientização sobre os perigos dos golpes cibernéticos é amplamente justificada por sua facilidade de uso, flexibilidade, capacidade de monitoramento e análise, e escalabilidade. Essas características fazem do - *ophish* uma ferramenta poderosa e eficaz para educar os usuários e fortalecer a postura de segurança de determinada organização frente aos latentes ataques de *phishing* do mundo atual.

Uma vez definida a ferramenta, é necessário partir à aplicabilidade da campanha de *phishing*, portanto, é imprescindível o emprego de um meio de disponibilização online da *landing page* empregada através do - *ophish,* de modo que o participante que tenha recebido o link em seu e-mail consiga acessar a partir de qualquer link de internet. Com base nisso, entra em voga a hospedagem na nuvem.

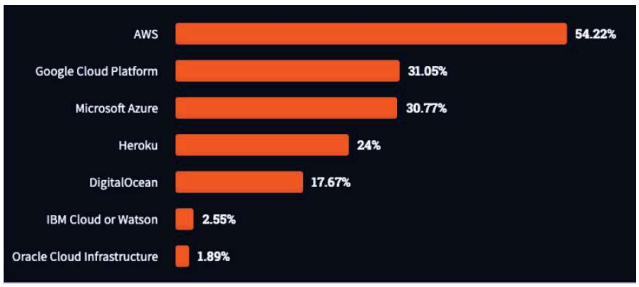
A hospedagem de serviços na nuvem tem se mostrado uma opção cada vez mais atrativa para empresas de todos os tamanhos devido à combinação de segurança robusta e facilidade de uso. A computação em nuvem permite que dados e aplicativos sejam armazenados em servidores remotos, acessíveis via internet, eliminando a necessidade de investimento em infraestrutura física. Entre as opções mais populares de serviços em nuvem estão Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP). A AWS, especificamente, destaca-se por sua escalabilidade e flexibilidade, permitindo que recursos sejam ajustados conforme a demanda do usuário. Além disso, a AWS oferece medidas de segurança rigorosas, como criptografia de dados e controle de acesso baseado em políticas. O plano gratuito da AWS é um grande atrativo, proporcionando acesso a uma variedade de serviços sem custos iniciais, o que é ideal para pequenas empresas e startups que desejam testar suas aplicações ou campanhas com um orçamento limitado (Amazon Web Services, 2024; Microsoft Azure, 2024; Google Cloud Platform, 2024).

TABELA 1: Comparação entre Serviços de Nuvem

Serviço	Flexibilidade	Segurança	Preço	Suporte
Amazon Web Services (AWS)	Alta	Alta	Variável	Excelente
Microsoft Azure	Alta	Alta	Variável	Bom
Google Cloud Platform (GCP)	Alta	Alta	Variável	Bom
Hostinger	! édia	! édia	con(mic	Regular
SiteGround	! édia	! édia	con(mic	Bom

Fonte: Elaborada pelos autores com base em Amazon Web Services (2024), Microsoft Azure (2024), Google Cloud Platform (2024), Hostinger (2024) e SiteGround (2024).

FIGURA <#Plataforma de nuvem mais usada



Fonte: Zup (2021).

O uso de AWS para uma campanha de phishing, por exemplo, oferece vantagens significativas. Os recursos gratuitos permitem a criação de ambientes de teste seguros e escaláveis, sem a necessidade de gastos adicionais. A flexibilidade da AWS facilita a personalização e o ajuste dos recursos para atender às necessidades específicas da campanha. Outro ponto positivo é a segurança oferecida pela AWS, garantindo que os dados estejam protegidos contra acessos não autorizados. A documentação extensa e o suporte técnico de qualidade também são fatores que facilitam a implementação e o gerenciamento dos serviços na nuvem (Amazon Web Services, 2024; Hostinger, 2024; SiteGround, 2024).

TABELA 2: Vantagens do AWS

Vantagem	Descrição
Custo	Plano gratuito disponível para novos usuários
Facilidade de uso	nterface intuitiva e documentação abrangente
Escalabilidade	Alta escalabilidade para ajustar recursos
Segurança	Medidas de segurança robustas, incluindo criptografia
Suporte técnico	Suporte 24/7 e vasta comunidade de usuários
Ferramentas adicionais	Integraç, o com diversos serviços e APIs

Fonte: Elaborada pelos autores com base em Amazon Web Services (2024)5

Dessa forma, a AWS se apresenta como uma escolha sólida devido à sua combinação de escalabilidade, flexibilidade, segurança e custo-benefício. A disponibilidade de um plano gratuito torna a AWS uma opção acessível para iniciar projetos e campanhas sem grandes investimentos financeiros, ao mesmo tempo em que aproveita uma infraestrutura

de alta qualidade e suporte técnico especializado (Amazon Web Services, 2024).

2.2 MÉTODOS DE PESQUISA

Este estudo foi conduzido com o objetivo de produzir uma eficaz campanha de conscientização sobre *phishing* utilizando a ferramenta - *ophish*. O desenho da pesquisa seguiu um modelo experimental, onde os participantes foram expostos a simulações de ataques de *phishing* e posteriormente avaliados quanto à sua capacidade de identificar e evitar tais ataques. Sendo possível assim obter uma cartilha completa direcionada especificamente à condução e reprodução desta pesquisa em qualquer ambiente organizacional controlado.

A população-alvo deste estudo consistiu-se de alunos do curso de Oficial de Comunicações, curso de Gestão de Sistemas Táticos de Comando e Controle e curso de Telegrafista, cursos estes ministrados na Escola de Comunicações (ESCOM). A amostra foi composta por 37 alunos de diferentes especializações e níveis de familiaridade com o ambiente digital garantindo uma representação adequada de diferentes padrões de comportamento quando expostos à simulação de *phishing*.

2.2.1 PREPARAÇÃO DA CAMPANHA DE PHISHING

A fim de obter os e-mails dos destinatários pertencentes ao grupo foco do estudo, foi necessário fazer um levantamento junto ao integrante mais antigo do grupo, todavia, em um ambiente organizacional, é possível obter essa informação facilmente por meio da existência natural do cadastro dos integrantes.

Na sequência, utilizando a ferramenta - *ophish*, foi criada uma campanha de *phishing* simulada. O *template* do e-mail e da própria *landing page* da campanha foram construídos com base em técnicas de engenharia social atinentes ao referido grupo.

Os e-mails foram projetados para imitar comunicações legítimas da escola, incluindo logotipos e estilos de escrita comuns. O código fonte do *template* empregado no e-mail foi confeccionado pelos autores com auxílio de IA. O código fonte do *template* da página da campanha foi obtido diretamente da página do *"Captive Portal4* sendo necessárias apenas algumas modificações para o emprego.

2.2.2 EXECUÇÃO DA CAMPANHA

Os e-mails de *phishing* foram enviados aos participantes e estes, por sua vez, tiveram uma janela de aproximadamente cinco dias para travar contato ou nto com o e-mail em sua caixa de entrada. Cada participante recebeu um e-mail de *phishing*, sem aviso prévio, às cegas, para simular um cenário realista.

Uma vez recebido o e-mail, o indivíduo já está inserido no ambiente de pesquisa podendo ele abri-lo ou nto, clicar no link e até mesmo submeter dados solicitados, denotando claramente crença na veracidade da origem das solicitações.

Após a conclusto da campanha, é iniciada uma nova campanha a qual encaminha um e-mail informativo aos participantes sobre sua participaçto em uma campanha de conscientizaçto de *phishing,* além de solicitar o preenchimento de um questionário referente à experiência acompanhado de um link contendo um artigo sobre a tema em foco.

Foi confeccionado também um *script* em *p6thon,* o qual é capaz de coletar os dados resultantes de uma campanha do - *ophish* e ordená-los de maneira automática em uma tabela por participante. Essa tabela é remetida anexa ao e-mail de *feedback* da campanha.

2.247COLETA DE DADOS

A ferramenta - *ophish* registrou as interações dos participantes com os e-mails de *phishing*, incluindo se abriram o e-mail, clicaram em links ou forneceram informações sensíveis.

Após a campanha, foi enviado um questionário aos participant es para avaliar seu nível de conscientizaçto sobre *phishing* antes e depois da campanha.

2.2.4 TÉCNICAS DE ANÁLISE

2.2.4.1 ANÁLISE 8 UANTITATIVA

Os dados coletados pela ferramenta - *ophish* foram analisados para determinar a axa de sucesso dos e-mails de *phishing* (porcentagem de e-mails abertos, links clicados e informações fornecidas).

As respostas ao questionário foram analisadas para medir mudanças no nível de conscientizaçto dos participantes.

2.2.4.2 ANÁLISE 8 UALITATIVA

Comentários abertos dos participantes foram analisados para identificar percepções e sentimentos em relaçto à campanha de *phishing* e à conscientizaçto sobre segurança.

2.2.4.9 REPRODUTIBILIDADE DO ESTUDO

Para garantir que outros pesquisadores possam reproduzir este estudo, apresentar-se-á de maneira objetiva os passos necessários para sua execuçto. No entanto, é importante destacar que o objetivo principal desta pesquisa foi a elaboraçto de uma cartilha detalhada, que descreve todas as táticas, técnicas e procedimentos empregados na execuçto do estudo. Para uma compreensto mais aprofundada, é imprescindível a leitura da cartilha, que pode ser encontrada no Apêndice A – Instalaçto, Configuraçto e Operaçto do Sistema Empregado. Esta cartilha aborda os seguintes processos: implementaçto e configuraçto da máquina virtual no sistema de computaçto em nuvem (AWS); instalaçto e configuraçto da ferramenta - *ophish*; implementaçto dos templates de e-mail e *landing page* utilizados; *configuração* do método de envio SMTP; execuçto da campanha; acompanhamento da campanha; análise dos dados; aplicaçto do questionário e coleta de *feedback*.

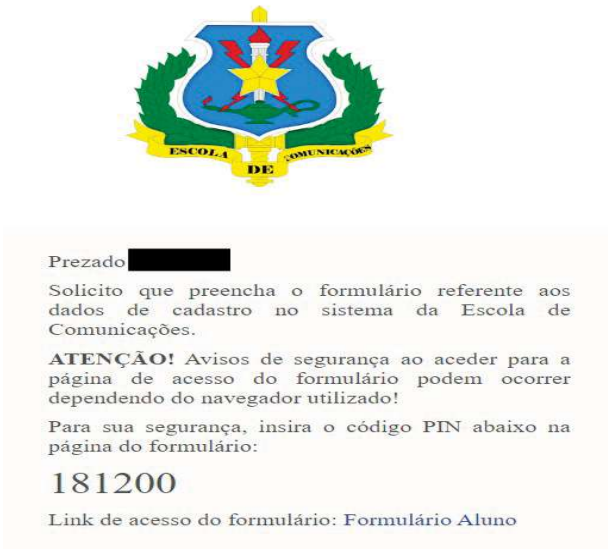
2.3 APRESENTAÇÃO E ANÁLISE DE DADOS

A coleta de dados nesta pesquisa se baseou nos resultados obtidos através da campanha hospedada pelo sistema - *ophish*. Tal coleta dividiu-se em dois momentos principais, os quais foram: Campanha Inicial de Conscientizaçto sobre p*hishing* (às cegas) e módulo de *feedback* pós campanha.

2.4 CAMPANHA INICIAL

Foram disparados e-mails para os 37 alunos participantes da pesquisa. Esse e-mail continha um PIN e descrevia a necessidade de fornecê-lo na subsequente página de redirecionamento para um formulário de atualizaçto cadastral para alunos da EsCom.

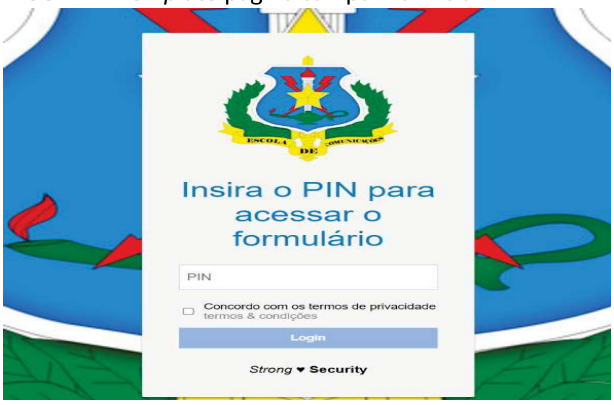
FIGURA !# **emplate* e-mail campanha inicial



Fonte: Os autores.

O intuito de utilizar a sistemática do código PIN para redirecionamento do acesso ao formulário é causar uma falsa sensação de segurança no participante de modo a legitimar o acesso ao formulário subsequente.

FIGURA =#**emplate* página campanha inicial



Fonte: Os autores.

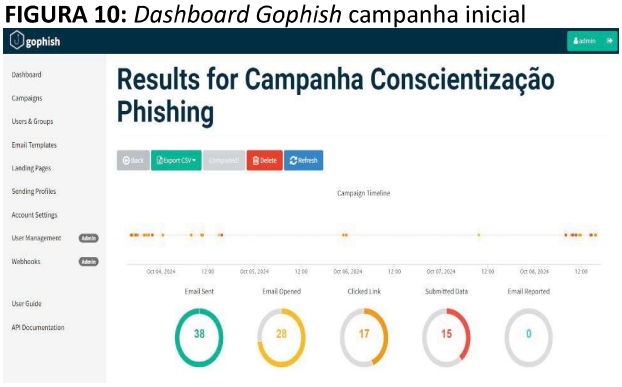
Uma vez passado pela página de redirecionamento, o participante chega a um formulário - *oogle !orms*, este já não mais hospedado pelo sistema - *ophish,* mas sim no próprio sistema - *oogle*. A essa altura, pressupõe-se que o participante acredita na legitimidade da solicitação e está disposto a fornecer os dados, sejam estes quais forem. Ainda assim, os dados requeridos foram triviais, haja vista o objetivo desta pesquisa ser meramente educacional.

FIGURA >#Formulário campanha inicial

Fonte: Os autores.

A campanha esteve ativa durante aproximadamente 5 (cinco) dias e os dados obtidos podem ser visualizados de maneira geral através do próprio *dashboard* do sistema:

FIGURA 10: *Dashboard Gophish* campanha inicial



Fonte: Os autores.

Com o intuito de otimizar a visualização dos resultados da campanha bem como remeter tais resultados de maneira clara e objetiva para os participantes, foi empregado um *script* em *p6thon* o qual entrega uma tabela contendo os resultados de maneira organizada e objetiva. A íntegra e descrição desse *script* encontrar-se-á no anexo A.9.1 do apêndice A referente à cartilha de conscientização produto dessa pesquisa:

TABELA 7#Tabela de resultados pelo *script*

status	ip	email	Grad	Sobrenome
Enviou Dados	132.255.30.164	araujo2bec@gmail.com	Ten	Araujo
Enviou Dados	13.64.229.66	leonardoneves48@hotmail.com	Ten	Neves
Enviou Dados	177.8.80.142	rocha.matheussilva@eb.mil.br	Ten	Rocha
Enviou Dados	177.8.80.142	pedrohcdwattimo@gmail.com	Ten	Wattimo
Email Enviado	-	dasilva.lopes@eb.mil.br	Ten	Jonathas
Email Opened	66.249.88.198	mbcd08@gmail.com	Ten	Brandalize
Clicou no link	189.6.31.40	capbrandao2011@gmail.com	Cap	Brandão
Email Enviado	-	wanderleysd@gmail.com	Cap	Wanderley
Email Opened	66.249.91.131	marcoshotsizzle12@gmail.com	Sgt	Marcos Resende
Enviou Dados	187.73.144.228	philipzim02@gmail.com	Sgt	Philip
Enviou Dados	177.10.57.229	alencar.work3@gmail.com	Sgt	Lucas Alves
Email Enviado	-	crlerbes@gmail.com	Sgt	Erbes
Enviou Dados	187.43.181.184	sgtricciele@gmail.com	Sgt	Ricciele
Email Opened	66.249.91.131	israelchaga@gmail.com	Sgt	Israel Chagas
Email Opened	66.249.83.83	leeo7kennedy@gmail.com	Sgt	Kennedy
Email Opened	66.102.8.131	caiodesouza242@gmail.com	Sgt	Caio
Email Enviado	-	vccostab0@gmail.com	Sgt	Victor Costa
Enviou Dados	66.249.88.199	luanepcn05@gmail.com	Sgt	Luan Martins
Email Opened	66.249.91.131	vasconcelosgn@gmail.com	Ten	Vasconcelos
Email Opened	66.249.91.131	cad5043pedrocosta@gmail.com	Ten	Pedro Chaves
Email Opened	177.8.80.142	wesley.tri@hotmail.com	Ten	Wesley
Clicou no link	189.112.10.6	victorhugovelasque@gmail.com	Ten	Velasque
Email Enviado	-	olimpio8179@hotmail.com	Ten	Olimpio
Enviou Dados	191.58.137.0	vitorpaladi@hotmail.com	Ten	Paladini
Enviou Dados	191.56.49.113	robertomarques94@gmail.com	Ten	Roberto Marques
Email Opened	66.102.8.130	willianv.vduarte@gmail.com	Ten	Victor Ventura
Email Enviado	-	pedrocestarioli@hotmail.com	Ten	Cestarioli
Enviou Dados	177.8.80.142	guicabralg@gmail.com	Ten	Gomes
Email Opened	66.249.91.133	bergf2911@gmail.com	Ten	Berg
Email Enviado	-	wendellgomes.pereira@eb.mil.br	Ten	Wendell Gomes
Enviou Dados	177.8.80.142	vitor.villela@eb.mil.br	Ten	Vilela
Email Enviado	-	david_sumaio@outlook.com	Ten	Sumaio
Enviou Dados	177.8.80.142	sella.matheus@eb.mil.br	Ten	Sella
Email Enviado	-	thyago3551@gmail.com	Ten	Thyago Henrique
Email Opened	66.249.88.198	cirojosepadua@gmail.com	Ten	Padua
Email Enviado	-	pauloc.dealmeida89@gmail.com	Ten	Custódio
Enviou Dados	177.8.80.142	calmeida.santos@eb.mil.br	Ten	C Almeida
Enviou Dados	177.8.80.142	erick.schlotefeldt@eb.mil.br	Ten	Schlotefeldt

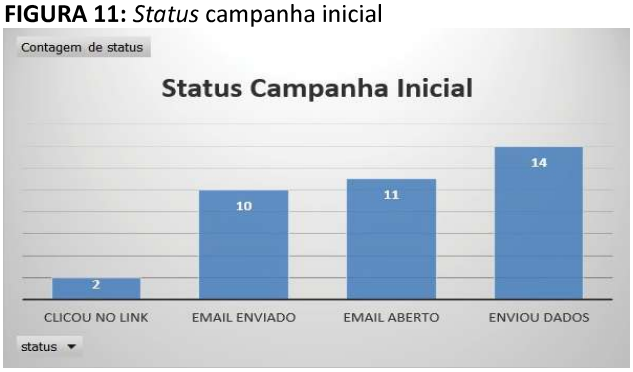
Fonte: Os autores.

Agora, com os dados resultantes da campanha aplicada, é possível observar que o grupo participante é heterogêneo. Em um universo de 37 participantes, todos com diferentes níveis de conhecimento e contato com ameaças cibernéticas, como *phishing*, foi possível subdividi-los em quatro subgrupos: 26% não abriram o e-mail; 28% abriram o e-mail; 5% abriram o e-mail e clicaram no link; e 44% clicaram no link e submeteram os dados solicitados.

Esses resultados revelam diferentes reações dos participantes ao interagirem com a campanha, lembrando que o contato foi às cegas, sem influências externas. O fato de alguns indivíduos não abrirem o e-mail pode indicar desatenção ou desconfiança na procedência do e-mail. Em ambos os casos, isso é significativo, pois um possível atacante poderia tentar múltiplas vezes até capturar a atenção da vítima.

Nos demais subgrupos, a vulnerabilidade em relação às ameaças *phishing* se torna evidente. Apenas abrir o e-mail já pode infectar a máquina da vítima, dependendo do conteúdo malicioso. Portanto, a conscientização desses subgrupos é crucial para que eles possam identificar sinais suspeitos e evitar ao máximo a exposição a essas ameaças.

FIGURA 11: *Status* campanha inicial



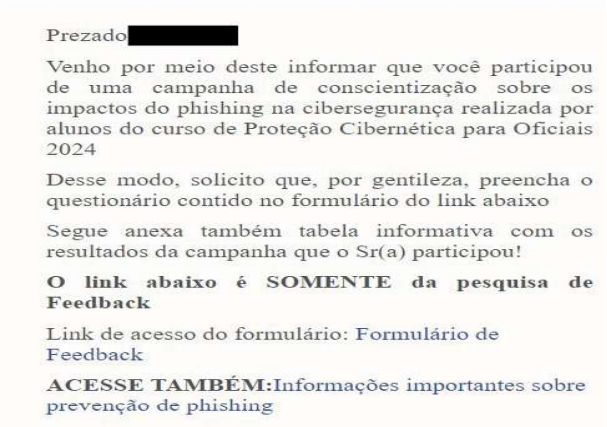
Fonte: Os autores.

247.2 MÓDULO DE FEEDBACK

Uma vez concluída a campanha inicial, é chegado o momento de promover o *feedback* aos participantes a fim de implantar de fato a ideia de conscientização sobre a ameaça *phishing,* além de colher dados referentes a experiência de participação e contato prévio com *phishing*. Tais dados serão de grande valia para o melhoramento de campanhas futuras e retificação do aprendizado.

O módulo consiste em um e-mail disparado através do próprio - *ophish* para todos os participantes da campanha inicial, contendo: um informativo sobre sua participação na campanha com a tabela de resultados anexa, um link para um material online sobre conscientização contra *phishing* e solicita a resposta a breves 12 (doze) questões sobre as experiências prévias e posteriores à participação na campanha. O questionário encontra-se pormenorizado no apêndice referente à cartilha de conscientização de *phishing.*

FIGURA 12: *Template* e-mail *feedback*



Prezado [redacted]

Venho por meio deste informar que você participou de uma campanha de conscientização sobre os impactos do phishing na cibersegurança realizada por alunos do curso de Proteção Cibernética para Oficiais 2024

Desse modo, solicito que, por gentileza, preencha o questionário contido no formulário do link abaixo

Segue anexa também tabela informativa com os resultados da campanha que o Sr(a) participou!

O link abaixo é SOMENTE da pesquisa de Feedback

Link de acesso do formulário: Formulário de Feedback

ACESSE TAMBÉM: Informações importantes sobre prevenção de phishing

Fonte: Os autores.

2.4 DISCUSSÃO DOS RESULTADOS

Os resultados obtidos pela campanha de conscientização sobre *phishing* indicam uma variedade de respostas e níveis de vulnerabilidade entre os 37 participantes. Esse comportamento heterogêneo destaca a complexidade em lidar com ameaças cibernéticas e a necessidade de estratégias adaptativas de conscientização.

Primeiramente, a constatação de que 26% dos participantes não abriram o e-mail de *phishing* pode ser interpretada de duas formas: desatenção ou desconfiança. A desatenção sugere que campanhas de *phishing* repetidas podem eventualmente capturar a atenção dessas pessoas. Por outro lado, a desconfiança é um sinal positivo de que algumas pessoas estão adotando uma postura cautelosa, essencial para a segurança cibernética.

Para os 28% que abriram o e-mail, mas não clicaram nos *links*, é evidente que há um grau de curiosidade ou necessidade de verificar o conteúdo. No entanto, este grupo ainda mostra uma vulnerabilidade significativa, pois o simples ato de abrir o e-mail pode expor o usuário a ameaças, dependendo do conteúdo malicioso inserido.

A porcentagem de participantes que clicaram no link (5%) e, mais alarmante, aqueles que submeteram dados (44%), expõe

uma séria falha na capacidade de identificar e evitar tentativas de *phishing*. Esses indivíduos sto os mais suscetíveis a ataques e reforçam a urgência de intensificar os programas de conscientizaçto e treinamento.

As diferentes reações dos participantes, sem influências externas, enfatizam a necessidade de abordagens personalizadas na educaçto sobre segurança cibernética. A campanha demonstrou que, enquanto alguns indivíduos mostram um nível básico de precauçto, muitos ainda carecem de conhecimento e habilidades necessárias para se proteger adequadamente de ataques *phishing*.

Portanto, os resultados sublinham a importância de estratégias contínuas e dinâmicas de conscientizaçto, envolvendo simulações realistas, *feedback* imediato e atualizaçto constante das técnicas de defesa. Melhorar a conscientizaçto e a educaçto sobre *phishing* é crucial para reduzir as vulnerabilidades e fortalecer a postura de segurança cibernética dos indivíduos.

CONCLUSÃO

Esta pesquisa destacou a importância da conscientizaçto sobre ameaças de *phishing*, especialmente no ambiente organizacional militar, onde a segurança cibernética é essencial. Ao implementar uma ferramenta de simulaçto de *phishing*, como o - *ophish*, foi possível avaliar o nível de vulnerabilidade dos usuários e estruturar uma resposta educacional adaptada às necessidades identificadas. A pesquisa nto apenas testou o comportamento dos usuários, mas também desenvolveu um módulo de *feedback* e treinamento que oferece aos participantes os recursos necessários para melhorar sua capacidade de identificar e evitar ataques de *phishing* no futuro.

Os resultados da campanha mostraram a diversidade de respostas entre os participantes, que variaram desde aqueles que nto abriram o e-mail até os que submeteram dados, refletindo graus variados de conscientizaçto e vulnerabilidade em relaçto às ameaças de *phishing*. Esses resultados demonstram a necessidade de abordagens personalizadas e contínuas de conscientização, reforçando que a educação em segurança cibernética deve ser um processo constante e adaptável. A abordagem prática da pesquisa, através do uso do - *ophish*, permitiu aos participantes vivenciarem um cenário simulado de ataque, proporcionando uma experiência de aprendizagem prática e significativa.

Para o Exército Brasileiro, as contribuições destas pesquisas são valiosas e podem ser aplicadas em várias áreas. Contra o *phishing*, a conscientização e o treinamento podem ser estendidos a grupos de usuários diversificados, abrangendo não só a seção de informática das Organizações Militares, mas também todas as áreas onde o acesso a informações sensíveis representa um ponto crítico de segurança. A implementação de campanhas regulares de conscientização, com simulações de *phishing* e relatórios de desempenho, pode fortalecer a postura de segurança organizacional e reduzir as vulnerabilidades frente a ataques cibernéticos. Essa prática, quando amplamente adotada, promove uma cultura de segurança digital, que se torna um ativo estratégico, elevando o nível de proteção em todos os níveis da instituição.

É imprescindível integrar métodos de conscientização e treinamento que considerem aspectos psicológicos e culturais dos usuários, além de práticas contínuas para fortalecer a retenção de conhecimento. Campanhas que incluam simulações técnicas e abordagens interativas podem sensibilizar mais eficazmente os participantes, tornando-os mais atentos. A aplicação de métodos variados e de longo prazo contribui para uma postura sólida frente a ameaças, que evoluem constantemente e demandam vigilância permanente, afinal, tais ameças estão em constante evolução, logo é cada vez mais latente a continuidade de conscientização.

Em síntese, a pesquisa conseguiu responder à questão proposta, que visava entender como promover a conscientização efetiva sobre *phishing* em um ambiente organizacional. A aplicação do - *ophish* e o

desenvolvimento de uma cartilha educacional constituem um modelo replicável, adaptável a diferentes contextos dentro do Exército Brasileiro e de outras organizações. A eficácia do treinamento foi comprovada pelos resultados, que mostraram uma melhora no entendimento e na precaução dos usuários em relação aos ataques de *phishing*. Este estudo reforça a importância de investir em campanhas de conscientização cibernética, que devem ser contínuas e aprimoradas para acompanhar a evolução das ameaças digitais. Dessa forma, conclui-se o ciclo argumentativo proposto desde a introdução, reafirmando a necessidade de uma abordagem proativa para a educação em segurança digital e destacando o valor de uma postura de vigilância constante.

7.1 RESULTADOS

A campanha de simulação de *phishing* realizada com o uso da ferramenta - *ophish* proporcionou *insights* valiosos sobre o comportamento e o nível de conscientização dos usuários em relação às ameaças de *phishing*. Os resultados mostraram uma variedade de respostas dos participantes, desde aqueles que evitaram interagir com o e-mail suspeito até os que chegaram a submeter dados pessoais. Esses diferentes graus de vulnerabilidade destacam que, apesar de haver um nível geral de conscientização, muitos usuários ainda possuem lacunas de conhecimento que podem comprometer a segurança organizacional. A análise detalhada dos resultados permitiu desenvolver um módulo de *feedback* e treinamento específico, que se mostrou eficaz em melhorar a capacidade dos usuários de identificar e evitar futuros ataques de *phishing*.

7.2 IMPLICAÇÕES PR; TICAS E TEÓRICAS

As implicações práticas deste estudo são significativas para o contexto militar, onde a segurança cibernética é crucial. A aplicação da ferramenta Gophish demonstrou ser uma abordagem prática para testar vulnerabilidades e fornecer um treinamento de conscientização em segurança digital. Em termos práticos, a pesquisa sugere que campanhas de simulação de *phishing* e treinamentos regulares podem reduzir as vulnerabilidades institucionais e reforçar a cultura de segurança digital no Exército Brasileiro. Teoricamente, o estudo contribui para o campo da conscientização em cibersegurança ao demonstrar que uma abordagem prática e personalizada pode ser mais eficaz do que métodos tradicionais de conscientização. Além disso, destaca-se a importância de uma metodologia adaptável que seja capaz de evoluir de acordo com as ameaças cibernéticas em constante mudança.

7.3 LIMITAÇÕES E CONSIDERAÇÕES

Embora a pesquisa tenha gerado resultados importantes, algumas limitações devem ser consideradas. Primeiramente, o estudo foi aplicado a um grupo específico de usuários, o que limita a generalização dos resultados para outros grupos ou setores. Além disso, o tempo de exposição dos participantes à campanha de conscientização foi relativamente curto, o que pode ter influenciado a retenção de conhecimento a longo prazo. Outra limitação foi a dependência de uma única ferramenta (- *ophish*) para simulação de *phishing*, não abrangendo outras possíveis técnicas e abordagens de conscientização. Essas limitações sugerem a necessidade de cautela ao extrapolar os resultados e reforçam a importância de estudos complementares com amostras mais diversificadas e diferentes ferramentas de conscientização.

7.4 RECOMENDAÇÕES E DIREÇÕES FUTURAS

Para pesquisas futuras, recomenda-se expandir o tamanho e a diversidade da amostra, incluindo participantes de diferentes setores e níveis de acesso a informações sensíveis. Essa expansão permitirá uma avaliação mais ampla da eficácia das campanhas de conscientização de *phishing* em

diferentes contextos. Sugere-se também a realização de campanhas de conscientização de longo prazo, permitindo analisar a retenção de conhecimento e possíveis mudanças de comportamento em relação às ameaças de *phishing*. Além disso, futuras pesquisas poderiam explorar a eficácia de outras ferramentas e abordagens de conscientização, como treinamentos "gameficados" ou sistemas de alerta em tempo real. No contexto organizacional militar, recomenda-se a implementação de campanhas regulares e a criação de políticas institucionais que promovam a educação em cibersegurança como parte da rotina de trabalho dos usuários, fortalecendo uma postura proativa e adaptativa frente as ameaças digitais.

ABSTRACT

*This research aimed to raise awareness about the risks associated) ith Phishing threats and, for that purpose, sought to implement a tool capable of testing the exposure level of a specific group of users to this type of threat (n applied explorator6 study) ith a qualitative approach) as conducted, using a scientific methodology of bibliographic analysis to highlight the most common Phishing techniques and the most e8ective awareness methods (9er gathering this data, the next step) as to de$ne the tool to be used as a 'Phishing ( ) areness *ool,') hich) ould provide resources for Phishing simulation, user engagement, automated detection, continuous evaluation, as) ell as generating reports and metrics. In this context, the chosen tool) as - ophish. *o gain ground and achieve the established objective, an applied explorator6 study) ith a qualitative approach) as employed, using a scientific methodology of experimental analysis to develop a Phishing simulation on the - ophish tool,) hich) as then tested) ith a specific group of individuals. ; ased on these tests and after a detailed analysis of their results, it) as possible to create a feedback and training module for users through a Phishing awareness guide*

Keywords<*Phishing, A) areness, Tool, Risks, Gophish*

REFERÊNCIAS

ALVES, C. de S.; CAETANO, R. H. S. **PB)$B)-(Sc&+ - Am/)*- %' Militar# A EC,)D-,)& 2* um& T' ,-), & 2* Pr*E*-. F 2* A%aque$ 2* PB)$B)-(C - tr& M)1)%*$**. O Comunicante, v. 12, n. 1, 2022.

AMAZON WEB SERVICES. **A+& G - H */ SerE),*$ IAH SJ**. 2024. Disponível em: <https://aws.amazon.com/>. Acesso em: 5 out. 2024.

CARDOSO, D. M. F.; NUNES, D. B. **Pr %*. F C - tr& A%aque$ 2* PB)$B)-(- Ex' r,)% Br&$)1i*** . O Comunicante, v. 10, n. 1, 2020.

CARVALHO, Leonardo. **PB)$B)-(# &)+ por%-,)& 2& C -$,)*- 0G&.F * 2 Tr*)-&+ *- % *+ $*(ur&-. & -& pr*E*-. F 2*$%& &+*&.&4** Disponível em: https://www.tempest.com.br/blog/phishing-a-importancia-da-conscientizacao-e-do-treinamento-em-seguranca-na-prevencao-desta-ameaca/#:~:text=O%20phishing%20continua%20representando%20uma,percentual%20era%20de%2051%25). Acesso em: 5 out. 2024.

COSTA, M. A. **T' ,-), &$ 2* phishing * + *2)2&$ 2* $*(ur&-. &4R*E)$%& 2* Se(ur&-. &2& InMr+ &.F** , v. 15, n. 3, p. 45-58, 2020.

CYBERPUNK. **Gophish: Ope-NSour, * PB)$B)-(T 1O)%4** Disponível em: <https://www.cyberpunk.rs/gophish-open-source-phishing-toolkit>. Acesso em: 5 out. 2024.

DEEPEN, Desai; HEGDE, Rohit. **Aum*- % 2 $ &%aque$ 2* phishing# r*1&6r) 2* phishing 2* 2024 2& Thr*&tLabG4** Disponível em: https://www.zscaler.com/br/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report?formCode=MG0AV3. Acesso em: 5 out. 2024.

DOS SANTOS, Demian. **C -$,)*- 0G&.F sobr* phishing * $*(ur&-. &#, + que M*quê-,)& tr*inar $ $*us Mncionár) $R4** Disponível em: https://www.diariodeti.com.br/conscientizacao-sobre-phishing-e-seguranca-com-que-frequencia-treinar-os-seus-funcionarios/. Acesso em: 5 out. 2024.

FALOURD, Guillaume. **STAC@O6ERFLOH SUR6EY 2021# O 8UE APRENDEMOS COM A PESQUISA**. Disponível em: https://zup.com.br/blog/stack-overflow-survey-2021. Acesso em 07 out. 2024.

FERREIRA, L. R. **Spoofi- (2* *N- &)1* suas)+ plic&.T*$4** Jornal de Cibersegurança, v. 10, n. 2, p. 123-134, 2021.

GARTNER. **Gar%-*r For*, &$s H or12U)2* IT Spe-2)-(% Gr U 94V)- 20234** Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2023-04-06-gartner-forecasts-worldwide-it-spending-to-grow-5-percent-in-2023>. Acesso em: 5 out. 2024.

GOOGLE CLOUD PLATFORM. **G (1* Cloud P1&V r+ IGCP)4** 2024. Disponível em: <https://cloud.google.com/>. Acesso em: 5 out. 2024.

GOPHISH. **Gophish User Guide**. 2024. Disponível em: https://docs.getgophish.com/user-guide. Acesso em: 20 set. 2024.

HARÁN, Juan Manuel. **C&+panhas 2* phishing**

, - 0nuam apr*$*- %&-2 , r*$,)+ *- % - Br&$)14 H *Liv*Se, ur)%X 03 set. 2019. Disponível em: https://www.welivesecurity.com/br/2019/09/03/campanhas-de-phishing-continuam-apresentando-crescimento-no-brasil/. Acesso em: 26 set. 2024.

HOSTINGER. **Hos0- (*r4** 2024. Disponível em: <https://www.hostinger.com.br/>. Acesso em: 5 out. 2024.

KASPERSKY. **Panor&+& 2* A+ *&.&$ 2023**. Disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/. Acesso em: 2 out. 2024.

KASPERSKY. **PB)$B)-(por H B&tsApp *+ 2022**. Disponível em: https://www.kaspersky.com.br/blog/phishing-whatsapp-antiphishing-informacoes-pessoais-dados-financeiros/21113/. Acesso em: 2 out. 2024

MALWAREBYTES. **O que ' phishingR**. Disponível em: https://www.malwarebytes.com/pt-br/phishing. Acesso em: 5 out. 2024.

MICROSOFT AZURE. **M),r $ Z Azur***. 2024. Disponível em: <https://azure.microsoft.com/>. Acesso em: 5 out. 2024.

NOOLAN. **O que ' um& $)+ ulaçF 2* phishingR** Disponível em: https://www.metacompliance.com/pt/blog/phishing-and-ransomware/what-is-a-phishing-simulation. Acesso em: 5 out. 2024.

PROBST. **Cultur& positiE& par& aum*- %ar & $*(ur&-. & ,)/*r-' 0, & , orpor&0E&** Disponível em: https://www.grantthornton.com.br/insights/artigos-e-publicacoes/campanha-anti-phishing-cultura-positiva-para-aumentar-a-securanca-cibernetica-corporativa/. Acesso em: 5 out. 2024.

ROOTSEC. **C)-, + *lhor*$ $)+ ulador*$ 2* phishing**. Disponível em: https://rootsec.com.br/cinco-melhores-simuladores-de-phishing/. Acesso em: 6 out. 2024.

SILVA, J. P. GoPhish: **Um& Mrr&+*- %&2* , P2)(&/*r% par&, &+ panhas 2* phishing**. Revista de Tecnologia da Informação, v. 22, n. 1, p. 78-89, 2023.

SITEGROUND. **Sit*Ground**. 2024. Disponível em: <https://www.siteground.com/>. Acesso em: 5 out. 2024.

SOFTWARE TESTING HELP. **Top 4 BEST Ngr O Alt*r-&0E*$ In 2024**: Review And Comparison. Disponível em: https://www.softwaretestinghelp.com/ngrok-alternatives/. Acesso em: 26 set. 2024.

SOUZA, A. B. **Estrutur& 2* , &+ panhas 2* phishing**. Revista Brasileira de Segurança Digital, v. 18, n. 4, p. 67-79, 2022.