DOI: 10.5748/19CONTECSI/PSE/SEC/7138

PHISHING AND SOCIAL ENGINEERING: CONCEPT, MODALITIES, TECHNIQUES OF DETECTION AND PREVENTION OF FRAUD. A SYSTEMATIC REVIEW OF THE LITERATURE

PHISHING E ENGENHARIA SOCIAL: CONCEITOS, MODALIDADES, TÉCNICAS DE DETECÇÃO E PREVENÇÃO DE FRAUDES. UMA REVISÃO SISTEMÁTICA DA LITERATURA

Erica Vilela ; https://orcid.org/0000-0002-1588-3454
Instituto de Pesquisas Tecnológicas

Eduardo Takeo Ueda ; https://orcid.org/0000-0002-3776-961X
Instituto de Pesquisas Tecnológicas

Vagner Luiz Gava ; https://orcid.org/0000-0001-5965-957X
Instituto de Pesquisas Tecnológicas

PHISHING AND SOCIAL ENGINEERING: CONCEPT, MODALITIES, TECHNIQUES OF DETECTION AND PREVENTION OF FRAUD. A SYSTEMATIC REVIEW OF THE LITERATURE

ABSTRACT

Nowadays it is very common to hear about some kind of cyber fraud, such criminal conducts that were already continuously practiced years ago, have intensified and gained new modalities. With the advent of social isolation caused by the pandemic, the cybercrime known as phishing was the most executed fraud modality worldwide, which is explained by the increase of internet users that in their great majority are unaware of basic rules to prevent this type of attack. The objective of this paper is to present the concept of phishing and social engineering, to highlight the main and current phishing modalities, to explain how the attacks work and to propose some basic but effective ways to detect and combat this type of crime.

Keywords: phishing, social engineering, phishing techniques, cyber crimes, phisher.

PHISHING E ENGENHARIA SOCIAL: CONCEITOS, MODALIDADES, TÉCNICAS DE DETECÇÃO E PREVENÇÃO DE FRAUDES. UMA REVISÃO SISTEMÁTICA DA LITERATURA

RESUMO

Hoje em dia é muito comum ouvir falar sobre algum tipo de fraude cibernética, tais condutas criminosas que já eram continuamente praticadas há anos, intensificaram-se e ganharam novas modalidades. Com o advento do isolamento social provocado pela pandemia, o crime cibernético conhecido como phishing foi a modalidade de fraude mais executada no mundo inteiro, o que é explicado pelo aumento de usuários de internet que na sua grande maioria desconhecem regras básicas de se prevenir deste tipo de ataque. O objetivo deste trabalho é apresentar o conceito de phishing e engenharia social, destacar as principais e atuais modalidades de phishing, explanar o funcionamento dos ataques e propor algumas formas básicas, mas eficazes de detecção e combate a este tipo de crime.

Palavras-chave: phishing, engenharia social, técnicas phishing. ciber crimes, phisher.

1. Introdução

Inicialmente esta seção descreve o problema da pesquisa e os objetivos a serem alcançados, a questão de pesquisa, o método empregado e organização das demais seções deste trabalho.

Os crimes cibernéticos têm chamado a atenção no mundo, usuários domésticos, empresas e governos têm sido alvos de diversos tipos de ataques. Ransonware e phishing lideram o ranking dos ataques mais cometidos no Brasil e no mundo. É de conhecimento notório, que grande parte dos ataques se inicia com a engenharia social, que irá proporcionar o acesso a primeira credencial necessária para o hacker iniciar uma campanha phising.

O usuário de internet a qualquer tempo pode ser vítima de um ataque phishing, e ao cair na armadilha elaborada pelo atacante (phisher) o usuário fornece voluntária ou involuntariamente suas credenciais as quais serão utilizadas posteriormente pelo golpista para obter alguma vantagem ilícita. As informações cedidas ao falsário podem ser usadas para um ato mais simples de fraude ou para obter acesso a sistemas que possam ocasionar resultados devastadores seja para um único indivíduo ou uma grande corporação.

De acordo com Younis e Musbah(2020) a cibercriminalidade é um problema crescente com um risco cada vez maior devido ao vasto número de dispositivos ligados, tais como os smartphones. Para os autores, tem havido um aumento dramático na utilização diária de smartphones para navegação na Internet, jogos e utilização de redes sociais, além de transações bancárias e apps de comunicação.

Após a pandemia de Covid em 2020 a quantidade de usuários de internet aumentou significativamente, para Beppler et al.(2022) há uma correlação entre a pandemia e o aumento de crimes cibernéticos. Segundo o NIC.br, no Brasil 94% dos domicílios brasileiros possuem acesso à Internet, sendo que 99% utilizam o celular para acessar. Grande parte desses usuários se tornaram verdadeiros público-alvos de cibercriminosos, que aproveitam as vulnerabilidades dos aplicativos, a falha ou ausência de proteção dos dispositivos e a falta de cultura em cibersegurança.

Embora grande parte dos ataques sejam aproveitando uma vulnerabilidade encontrada nos dispositivos, o elo mais fraco ainda é o ser humano, que por meio da técnica de engenharia social, o atacante consegue persuadir a vítima a fornecer as informações que são de interesse do golpista.

Os ataques phishing nos últimos anos tem se posicionados como uma das principais e mais grave tipo de ameaça ao usuário de internet, o número de ataques aumentaram exponencialmente nos últimos 3 anos e as perdas econômicas das empresas devido a estes ataques ultrapassam trilhões de dólares no mundo de acordo com Morgan(2020). Outro dado que reforça a ocorrência frequente de phishing na maioria dos incidentes de segurança é que conforme relatório de 2022 da força tarefa de IBM 41% dos ataques usam o phishing como acesso inicial.

Para Younis e Musbah(2020) Muitas soluções têm sido propostas para prevenir e detectar ataques de phishing, tais como métodos de conscientização dos usuários e ferramentas de detecção. No entanto, o phishing ainda está no topo dos ataques com um elevado número de vítimas, uma das principais razões é a falta de conhecimento dos

usuários. Um estudo de 2021 da Karspersky no Brasil corrobora para esta afirmação, este estudo apresenta que as equipes de colaboradores são carentes de conhecimentos básicos sobre cibersegurança para se proteger, pois apenas 54% das empresas oferecem treinamentos de conscientização.

Com base no exposto, pode-se compreender a necessidade de conhecer mais a fundo os tipos de ataque phishing e as propostas de prevenção e combate.

O objetivo principal deste trabalho é apresentar uma revisão sistemática da literatura apresentando o que há de mais atual em termos de fraudes cibernéticas ocasionadas por phishing que utilizam na maioria das vezes como principal técnica a engenharia social. Desta forma, o trabalho estará realizando um mapeamento dos de alguns tipos de phishing e as principais técnicas de detecção e combate aos ataques.

De modo a alcançar tal objetivo, esta pesquisa procura responder à seguinte questão:

Quais são as tipos de técnicas mais recentes de phishing e quais são as técnicas de detecção e combate mais utilizadas para cada caso?

A divisão do artigo foi feita em 4 seções. A Seção 1 traz a fundamentação teórica com uma visão geral sobre phishing, tipos de phishing, métodos de ataques e detecção. A Seção 2 apresenta o método de revisão sistemática da literatura adotado neste trabalho. A Seção 3 fornece a análise e os resultados obtidos na revisão sistemática e a Seção 4 traz as conclusões, limitações e sugestões para futuros trabalhos de pesquisa e aplicação prática dos conceitos nas organizações como na sociedade como um todo.

2. Fundamentação teórica

Nesta seção será apresentada uma visão geral sobre phishing, conceitos, técnicas de invasão e técnicas de detecção.

2.1 Phishing

Nesta subseção é apresentada uma visão geral do termo phishing como crime cibernético, primeiramente com definições na literatura trazendo conceitos gerais sobre o tema e depois o desenvolvimento do assunto aprofundando na conceito técnico .

O termo phishing é utilizado desde a década de 90, o termo deriva da analogia da operação de "pesca" em inglês, fishing. A frase "ph" vem de "phreaking", telefone, que era o método muito comum usado para atacar sistemas telefônicos durante a década de 1970.

Phishing é um tipo de ataque de engenharia social que busca por meio de mensagem fraudulenta (por exemplo, e-mail) enganar as vítimas e persuadi-las a divulgar desde credenciais de conta a outras informações sensíveis. Os atacantes (phishers) usam então os dados roubados para os seus próprios interesses monetários (OEST et al., 2021). Os crimes cibernéticos possuem a característica de ausência de limite temporal e geográfico indivíduos, governos, corporações privadas, sistemas de infraestrutura crítica como os de água, energia e telecomunicações são frequentemente alvos de ataques cibernéticos orquestrados por criminosos onde as motivações variam desde financeiras à políticas. As consequências decorrentes de um incidente de segurança podem ser desastrosas dependendo do nível de comprometimento e rapidez de resposta ao incidente. Desta forma, é de fácil compreensão

que a cooperação entre países, entre os setores público e privado é essencial para criação de políticas e estratégias de prevenção e combate a esses tipos de crimes.

Em um ataque de phishing, o(s) atacante(s) recolhe(m) os dados sensíveis do cliente (ou seja, conta de usuário, dados de login, números de cartão de crédito/débito, etc.) utilizando e-mails falsificados ou sites falsos. Os sites de phishing são pontos de entrada bem comuns para ataques de engenharia social, incluindo numerosas fraudes em sites web. Em tais tipos de ataques o(s) atacante(s) cria(m) páginas web copiando o comportamento de sites legítimos e envia URL(s) para as vítimas escolhidas por meio de mensagens de spam, textos, ou redes sociais (BASIT et al., 2021).

Para Srivastava e Gupta(2021) phishing é o método mais comum usado por invasores hoje em dia. A ameaça ao ciberespaço é grande e variada, mas se houver um bom mecanismo de detecção de phishing, grande parte dos problemas que surgem devido a ameaças cibernéticas seria reduzido.

Para Swarnalatha et al.(2021) phishing é uma grande ameaça para todos os usuários de internet no mundo, todo e qualquer trabalho é feito on-line, e por isso, há alta probabilidade de que informações pessoais e credenciais sejam exploradas. Os atacantes escondem sua localização e executam sua ação. É considerado como um dos crimes mais bem organizados que utilizam técnicas de engenharia social.

2.2 Engenharia social

Para Leonov et al. (2021) engenharia social é a técnica utilizada por hackers baseada na coleta de informações sobre uma pessoa, empresa ou objeto por meio de uma conversa pessoal, ou usando e-mail, telefone celular e outros meios de comunicação, quando uma das partes involuntariamente divulga informações ou executa algum tipo de ação.

Ainda para Leonov et al.(2021), um dos elementos mais fracos na proteção de qualquer sistema são os usuários. O cérebro humano não funciona perfeitamente, e a culpa são das chamadas distorções cognitivas. Essas distorções, às vezes também conhecidas como "erros no pensamento humano", são usadas por atacantes em várias combinações para criar métodos de ataque. Hackers estudam as fraquezas e vulnerabilidades de uma pessoa ou um grupo de pessoas que têm acesso às informações necessárias. Desta forma, usando os "pontos fracos" descobertos, eles recebem os dados desejados ou as informações confidenciais. Isto é a base da engenharia social

De acordo com Baig et al. (2021) os golpes atraem uma variedade de fraquezas humanas, incluindo o desejo de ganhar recompensas rápidas, o desejo de ajudar os outros e o desejo de ser apreciado pelo scammer(golpista). Os autores sugerem que há estudos que dizem que algumas pessoas têm um "caráter de vítima", o que as torna mais suscetíveis a golpistas. Essas pessoas tendem a ser vítimas de fraudes regularmente. A falta de controle emocional é um aspecto que pode tornar algumas pessoas mais inclinadas a serem vítimas.

De acordo com HIJJI e GULZAR (2020) a engenharia social é dividida em quatro tipos: físico, social, técnico e socio-técnico. No físico os invasores executam algumas ações como busca por dados pessoais, manuais, memorandos e informações confidenciais em lixeiras. O objetivo principal do atacante é acumular informações sobre a vítima a partir de materiais físicos. No tipo social, que é o mais utilizado, os scammers usam técnicas

psicológicas para convencer o usuário-alvo visando construir um relacionamento. No técnico, utiliza-se em geral os sites de redes sociais que são fontes muito estimadas de informação. Os scammers frequentemente usam mecanismos de pesquisa para coletar informações relevantes sobre as vítimas. E por último a sociotécnica, ela é a mais poderosa técnica da engenharia social, combinando os tipos social e técnico. O engenheiro social considera certos fatores como a cultura social da vítima, o comportamento humano, as tecnologias utilizadas e a construção de infraestrutura, bem como metas e valores. A combinação de técnicas aumentam as chances de ataques cibernéticos de engenharia social bem-sucedidos.

2.3 Tipos de técnicas de ataques phishing

De acordo com ATHULYA e PRAVEEN (2020), os ataques de phishing dependem principalmente do canal de phishing, o mecanismo de phishing utilizado e o número de alvos, eles dividem o ataque phishing em 2 grupos: **Ataques de engenharia social e Ataques de subterfúgio técnico**. A classificação de tipos de phishing é mostrada conforme Figura 1.

Figura 1 – Classificação de tipos de phishing

Fonte: Adaptado de Athulya e Praveen (2020)

2.4 Ataques de engenharia social

1) SMS phishing: No SMS phishing o golpe se dá por meio de envio de mensagens de SMS fraudulentas. O phishing por SMS pode ter uma base incrivelmente ampla, uma vez que o phisher pode enviar grandes quantidades do mesmo texto a muitos números que podem conter ligações. O atacante frequentemente tenta enganar as pessoas a pensar que ganharam um concurso, oferecem prêmios de graça, ofertas, ofertas de desconto, ofertas de emprego ou detalhes de encomendas falsas com um link de cancelamento.

2) Vishing: Vishing ou VoIP (voz sobre IP) refere-se ao phishing que pode ser feito por meio de chamadas telefónicas. O atacante telefona a seu alvo e diz ser, por exemplo, representante bancário, e se oferece a resolver algum suposto problema na conta bancária, e muitas vezes consegue convencer à vítima a compartilhar dados da conta, e ainda progridem no golpe, induzindo a vítima a fornecer dados de acesso como PIN e senhas.

3) Phishing enganoso: Inclui envio de e-mails que imitam logótipos ou websites legítimos de instituições financeiras respeitáveis e outras entidades que fazem os usuários acreditarem e clicarem no link. Nestes tipos de ataques, os usuários podem ser enganados pela sintaxe do nome de domínio. Por exemplo, useraccount@mazon.com pode enganar um usuário.

4) Spear phishing e Whaling: São os famosos phishing direcionado e o caça à baleia, eles visam especificamente certas organizações ou pessoas. Os atacantes da Spear phishing visam vítimas específicas, obtendo o máximo de informação pessoal possível sobre eles e enviar e-mails que parecem legítimo. Os ataques a "baleias" ocorrem quando o phisher tem como alvo um usuário em um cargo executivo como CEO. A caça à baleia pode ter um resultado extremamente desastroso, porque as pessoas do alto escalão executivo têm

o acesso às informações mais confidenciais sobre a empresa.

5) Manipulações de links: Manipulações de links também conhecidas como ataques de phishing homográficos. Neste ataque os URLs podem parecer legítimos, e o conteúdo da página pode parecer o mesmo, mas o conteúdo difere do conteúdo original, pois é um website criado para roubar dados sensíveis da vítima ou para corromper o dispositivo do usuário. É possível através da utilização de códigos. O Código Puny, por exemplo, é uma forma de converter palavras que não podem ser escrito em ASCII, em letras unicode codificadas em ASCII. O atacante pode lançar um nome de domínio que substitui certos ASCII ,cartas com letras Unicode. O prefixo de codificação ASCII é utilizado por muitos navegadores web para sinalizar que o domínio utiliza código puny. Esta é uma precaução para proteger contra ataques de phishing da Homograph. Nem todos os navegadores exibem o prefixo do código puny, deixando os hackers aptos a explorar essa vulnerabilidade.

6) Phishing de sessão: Outro tipo de phishing que abusa da confiança de um site legítimo na forma de um pop-up durante o meio da sessão. Mensagens pop-up como "tempo limite da sessão", "redefinir sua senha" ou "fazer login novamente" são exibidas. Como parece vir de um site confiável, o usuário envia suas informações, que enviarão as credenciais de login para os invasores em vez de servidores confiáveis.

2.5 Ataques com subterfúgio técnico

Segundo ATHULYA e PRAVEEN (2020), estes tipos de ataquem funcionam instalando algum software criminoso diretamente no dispositivo da vítima. Os objetivos são sempre os mesmos, roubar credenciais, enganar redes de tráfego locais e remotas para ludibriar os usuários para que acessem sites falsos via proxies controlados por phishers. Segue abaixo os tipos de phishing que se enquadram nessa categoria.

1) Phishing baseado em malware: O Malware pode ser enviado como um anexo de e-mail ou arquivo multimídia do site ou por exploração de falhas de segurança de aplicativos ou software desatualizados.

2) Key loggers e Screen loggers: Estes são variantes específicas de malware que monitoram a entrada do teclado e transmitem informações confidenciais pela Internet para o hacker. Pequenos programas utilitários incorporam-se aos navegadores do usuário que serão executados automaticamente quando o navegador for iniciado e entrará em arquivos de sistema, drivers de dispositivo, etc.

3) Sequestro de sessão: Sequestro de sessão é definido por um ataque no qual as ações do usuário são rastreadas até uma conta de destino ou a transação é interceptada e os invasores estabelecem a conexão com credenciais dos usuários. O software mal-intencionado controla ponto a ponto e pode executar um comportamento não autorizado, como a transferência de fundos, sem o conhecimento do usuário.

4) Cavalos de Tróia: Trojans são aplicações maliciosas instaladas nas máquinas das vítimas, e que são ativadas quando usuários tentam fazer login. Eles coletam credenciais do usuário e encaminham para o phisher.

5) Pharming: Este ataque funciona pelo meio de um envio de um código malicioso para o alvo através de e-mail ou links que modificam todo o sistema de dados do localhost. As URLs podem ser traduzidas para strings de números que são usadas pelo sistema para acessar páginas da web. Essa mudança causa o redirecionamento para o site mal-intencionado, mesmo que o URL digitada seja a correta. O pharming também pode ser feito por envenenamento de DNS. Nesse processo, os arquivos de host local da rede não são modificados, mas a tabela do nome de domínio do sistema é atualizada. Isso resulta no alvo sendo direcionado para sites maliciosos.

2.6 – Estrutura de ataque phishing

Para OEST et al. (2018) para se ter um impacto positivo na luta contra o phishing, deve-se primeiro familiarizar com a natureza do ataque de phishing, as ferramentas à disposição de phishers e também as defesas disponíveis na indústria. No mercado há diversas opções de kits que auxiliam a construção de um ataque. Um kit de phishing é uma coleção unificada de ferramentas usadas para implantar um site de phishing num servidor Web. Alguns kits de phishing são mantido em posse de seus criadores, enquanto outros são oferecidos como parte da economia da cibercriminalidade como serviço. Certos criminosos se especializam na criação e venda de kits de phishing e até mesmo aceitam pedidos personalizados para a criação de kits. Os componentes básicos de um kit de phishing incluem

um modelo que imita o design do site que está sendo personalizado, o código do lado do servidor para capturar e enviar dados enviados para o phisher, e, opcionalmente, codigo para filtrar o tráfego indesejado ou implementar outras contramedidas contra a comunidade anti-phishing. Tais contramedidas podem incluir encurtamento ou redirecionamento de URL, randomização de URL ou ofuscação de código.

De acordo com os autores Jain e Gupta(2021) os ataques phishing possuem um ciclo de vida, conforme pode-se ver na Figura 2.

Figura 2 – Ciclo de vida do ataque Phishing

Fonte: Jain e Gupta(2021)

Segue abaixo o detalhamento de cada passo do ciclo de vida do phishing evidenciado na Figura2.

Passo 1: Planejamento e configuração: O phisher identifica a organização alvo e prepara a estratégia técnica para adquirir informações secretas.

Passo 2: Construção de sites de phishing: O phisher cria um site de phishing que parece semelhante ao site oficial. Várias ferramentas on-line estão disponíveis que geram uma réplica de um site bem conhecido. Depois de construir o site, o phisher carrega esses arquivos para um servidor de hospedagem na web.

Passo 3: Propagação de phishing: O phisher escolhe a distribuição apropriada método para espalhar o link do site de phishing.

Passo 4: Instalação: O link falso redireciona o usuário para o site malicioso onde o usuário pode acabar fornecendo credenciais. O link falso pode instalar algum software malicioso no sistema do usuário.

Passo 5: Coleta de dados: Os phishers podem acessar os dados preenchidos pelo usuário da Internet. Além disso, o software malicioso também pode enviar as informações armazenadas no sistema do usuário.

Passo 6: Break-Out: Depois de receber as credenciais do usuário, os cibercriminosos excluem todos as evidências, ou seja, os sites de phishing, contas de e-mail e assim por diante. O atacante pode usar a credencial do usuário (por exemplo, detalhes do cartão de crédito, nome de usuário, senha, etc.) para fins ilícitos.

Para Oest et al. (2021) os estágios de um cenário típico de phishing são ilustrados conforme a Figura 3. Primeiro, antes de envolver qualquer vítima, um atacante falsifica um site copiando sua aparência de tal forma que fique difícil para um usuário comum distinguir entre o site legítimo e o falso. Isso pode ser feito usando um kit de phishing. Em seguida, o atacante envia mensagens (como e-mails de spam) para o usuário, aproveitando engenharia social para insistir que uma ação é necessária e atrai o usuário para clicar em um link para o

site de phishing. Se a vítima é enganada com sucesso, então visita o site e começa a enviar as informações confidenciais, como credenciais de conta ou números de cartão de crédito. Muitas vezes, durante o processo serão mostradas as vítimas mensagens de confirmação para parecer ser algo legítimo, minimizando a suspeita do ataque após o fato. Por fim o site de phishing transmite as informações da vítima de volta para o phisher que tentará usá-lo fraudulentamente para ganho monetário diretamente ou indiretamente.

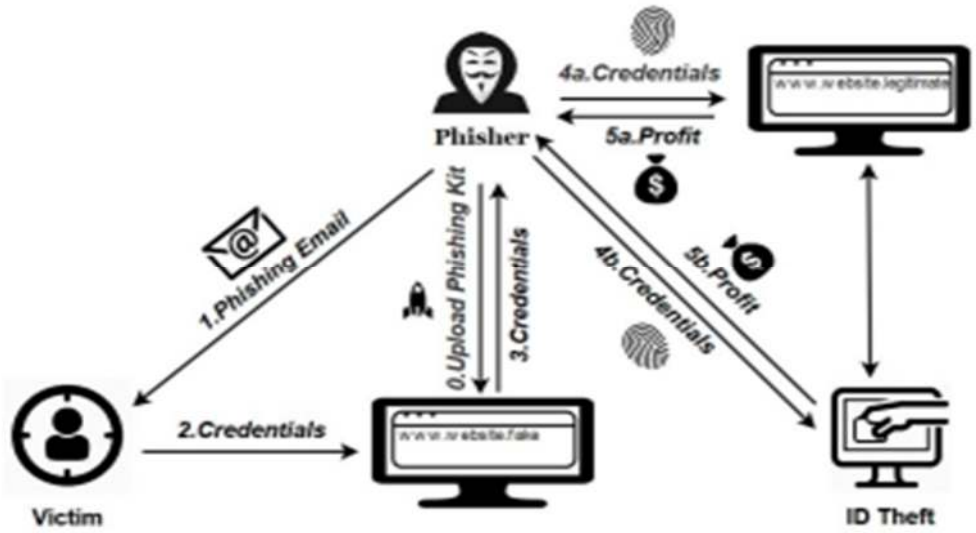

Figura 3 – Ataque de phishing clássico.

Fonte: Oest et al.(2018)

2.7 Soluções Anti-phishing

Os autores Athulya e Praveen (2020) propõe uma divisão no que diz respeito às soluções anti-phishing conforme Figura 4.

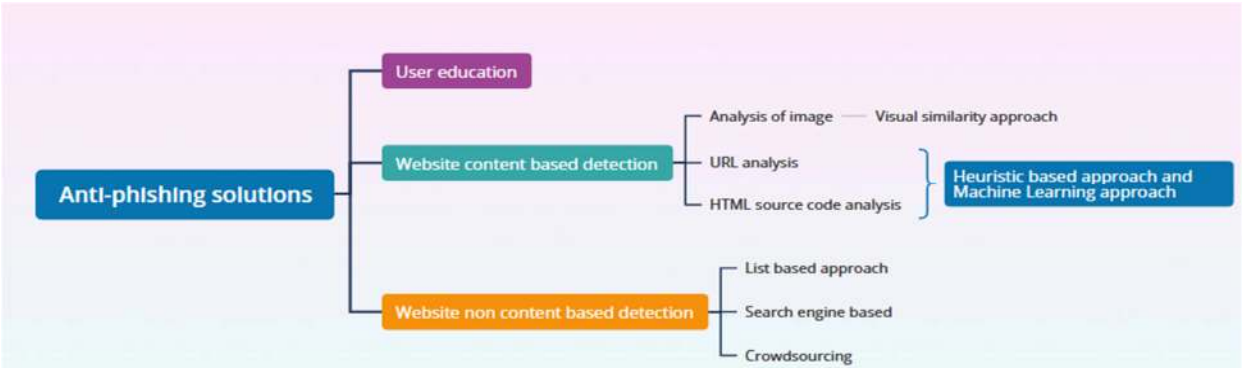

Figura 4 – Soluções anti-phishing

Fonte: Athulya e Praveen (2020)

A. Educação do Usuário – Programas de conscientização de usuários de internet, para que os mesmos possam aprender reconhecer as tentativas de phishing direcionadas. Athulya

e Praveen (2020)acreditam que esta não seja um boa solução pois a maioria das pessoas são novatas e não sabem testar a autencidade dos sites, verificação de SSL etc. Em contrapartida, para Sumner e Yuan(2019) estudos mostram a necessidade de melhorar a conscientização do usuário sobre ataques de engenharia social.
Segundo Beppler et al.(2021) algumas sugestões para educação do usuário com relação a cibersegurança são:

• Verificações de sites, contas de redes sociais e endereços de e-mail: ferramentas como Google Safe Browsing,Google Transparency Report, Alexa ranking.

• Educação do Usuário por meio de programas de conscientização frequentes.

Instalação/atualização de software de anti-vírus;

• Implantação e reforço nas política de segurança da empresa;

• Atualização de programas e sistemas;

• Conexão a rede segura e acesso de contas por meio da VPN;

• Arquivos de Backup e política de recuperação de desastres ;

• Uso de autenticação multi-fator.

B. Soluções não baseadas em conteúdo do site – Estas soluções são divididas em 3 tipos:

- Abordagem baseada em lista: A abordagem baseada em lista usada principalmente para verificar o status das páginas da Web, seja ela legítima ou de phishing. Há dois tipos de abordagem, a de blacklist e whitelist.
- Técnicas de Whitelist: Os métodos de whitelist incluem uma lista de URLs, estilos, domínios e certificados digitais legítimos para comparar com sites falsos. A semelhança entre o site legítimo e o site suspeito é verificada. O acesso é dado ao domínio suspeito se ele for encontrado nas URLs armazenadas. Caso contrário, ele é bloqueado. A principal desvantagem dessa abordagem de lista é no caso de sites legítimos impopulares ou sites recém-registrados que não estão na lista branca podem ser classificados incorretamente como sites falsos, o que resulta em altos falsos positivos
- Técnicas de Blacklist: Os métodos de blacklist armazenam URLs de phishing, tags, domínios e outras informações necessárias. Os URLs de spam são atualizados nesta blacklist. A blacklist não tem um URL de phishing recém-criado. A técnica da blacklist geralmente definida como um plug-in ou barra de ferramentas do navegador em navegadores da Web. Algumas das ferramentas que implementam essa abordagem de blacklist são a navegação segura (GSB) do Google, o Microsoft Smart Screen, o Opera e o PhishTank.

1- Técnicas baseadas em motores de busca: Este método recupera informações de identidade de sites e os mecanismos de pesquisa são usados para determinar a autenticidade dos sites que estão sendo consultados. Essas técnicas têm alto tempo de resposta e podem detectar um ataque de phishing de zero hora. A

técnica baseada em mecanismo de pesquisa forma uma cadeia de caracteres de consulta que é gerada com as palavras-chave de identidade de página da Web suspeita ou título concatenado com o nome de domínio ou uma imagem. Quando uma consulta é dada como entrada para o mecanismo de pesquisa, ela produz resultados de acordo com a consulta. Aqui, o desenvolvedor assume que, se for uma página da Web legítima, ela pode aparecer nos principais resultados 'n'. A detecção de páginas da Web de phishing é rápida e confiável nessa técnica.

2- Crowdsourcing: A web of trust (WOT) é uma extensão do navegador focada em crowdsourcing, que se baseia na classificação do site dada pelos usuários. WOT é um programa proprietário, onde o comportamento do usuário é monitorado, valida o ranking e avaliado periodicamente. Ele exibe reputações de nomes de domínio como semáforos próximos aos resultados de pesquisa ao usar o Google, o Yahoo e outros sites de rede, como Facebook, Twitter e Gmail.

C- Soluções baseadas em conteúdo do site – Nesta técnica haverá a extração principalmente de recursos da página da Web para detectar páginas phishing. Essa técnica se divide em: detecção de phishing baseada em similaridade visual, abordagem heurística e abordagem com uso de aprendizado de máquina.

1- Técnica baseada em similaridade visual: Nesta técnica, os sites de phishing são detectados usando semelhanças visuais, como layouts de página, conteúdo, imagens, layout de fonte, tamanho e cor entre phishing e páginas da Web legítimas. Para escapar da técnica de detecção de phishing, os invasores normalmente inserem imagens, Flash e Java Applet em vez de texto HTML. Essa técnica identifica facilmente esses artefatos incorporados presentes nos sites de phishing usando uma relação assinatura/semelhança.

2- Abordagem de aprendizado de máquina: Hoje em dia, essa técnica é amplamente utilizada. Os algoritmos de aprendizado de máquina são aplicados aos recursos derivados dos sites para detectar ataques de phishing. Tais abordagens são uma mistura de métodos heurísticos e algoritmos de aprendizado de máquina, ou seja, através da abordagem heurística, o conjunto de dados é criado. Em seguida, alguns dos algoritmos de aprendizado de máquina como Random Forest (RF), otimização mínima sequencial (SMO), árvore J48, perceptron multicamada (MLP), máquina vetorial de suporte (SVM), AdaBoostM1, regressão logística (LR) e rede bayesiana (BN) são aplicados com base em sua eficiência. Eles podem identificar os ataques de phishing de dia zero e trabalhar relativamente em um grande conjunto de dados. Como esse método envolve a extração de tantos recursos, seu tempo de resposta é lento. A eficiência dessa abordagem depende do tamanho do conjunto de dados, da seleção de recursos e do tipo de classificadores de aprendizado de máquina.

3- Abordagem baseada em heurística: técnicas baseadas em heurística extraem as propriedades mais comuns, como URL e hiperlinks, de sites falsos existentes para encontrar novos sites de phishing. Essas propriedades podem não aparecer em todas as páginas da Web, o que trará baixas taxas de detecção. Uma vez que um invasor descobre o algoritmo ou os recursos usados na detecção processo eles podem substituir as características heurísticas, assim, alcançar o objetivo de roubar informações confidenciais.

3. MÉTODO

Este estudo foi realizado com base na metodologia de Revisão Sistemática da Literatura (SLR). Revisão sistemática de literatura apresenta-se como uma forma de estudo secundário que utiliza uma metodologia bem definida para identificar, analisar e interpretar todas as evidências disponíveis a respeito de uma questão de pesquisa particular de maneira imparcial e repetível(KITCHENHAM E CHARTERS, 2007). A metodologia aplicada por este artigo foi baseada no estudo de Weidt e Silva (2016) na qual divide o trabalho de Revisão Sistemática da Literatura em três fases: fases de planejamento, condução e síntese.

Para o gerenciamento de referências bibliográfica foi utilizado o Mendeley, para gerenciamento de protocolo de revisão sistemática da literatura foi utilizado o Parsifal (https://parsif.al/). Para geração de planilhas referente à documentação da revisão sistemática foi utilizado o Microsoft Excel (https://www.microsoft.com/pt-br/microsoft-365/excel).

3.1 Planejamento da Revisão Sistemática da Literatura

A fase de planejamento foi dividida em etapas, iniciando pelo objetivo da pesquisa até as estratégias de análise utilizadas para publicação dos dados. Seguem abaixo as etapas:

3.2 Objetivo da Pesquisa:

Construir uma revisão sistemática de literatura que apresente o que há de mais atual em termos de fraudes cibernéticas ocasionadas por phishing que utilizam como principal técnica a engenharia social , realizando assim um mapeamento dos de alguns tipos de phishing e as principais técnicas de detecção e combate aos ataques.

3.2 Questão de Pesquisa:

Quais são as tipos e técnicas mais recentes de phishing e quais são as principais técnicas e métodos e detecção e combate mais utilizadas para cada caso?

A estruturação da pergunta de pesquisa foi feita através da estratégia PICO de Petticrew e Roberts (2005). PICO representa um acrônimo para Population, Intervention, Comparison e Outcome.

População (P): Usuários de internet em geral;

Intervenção (I): Técnicas e métodos de campanhas phishing e estratégias de detecção e combate aos ataques;

Controle (C): lista de referências obtida por meio de pesquisa exploratória do tema, servindo de base para a escolha das palavras chaves e fontes:

Resultados (O): Apresentação do que há de mais atual em campanhas phishing e propostas de técnicas de detecção aos ataques.

3.3 Critérios de Seleção das Bases de Busca:

As bases utilizadas foram escolhidas devido ao seu reconhecimento mundial e por incluírem os principais artigos, revistas e eventos científicos em computação quântica e inteligência artificial, conforme Quadro 1.

Lista das Bases de Busca:

Fonte de Busca	Endereço Online
ACM *Digital Library*	https://dl.acm.org/
IEEE *Xplore*	https://ieeexplore.ieee.org/xplore/
ISI Web of Science	http://www.webofscience.com/

Quadro 1 – Motores de busca utilizadas na RSL.

Fonte: Elaborado pelos autores.

3.4 Strings de Busca:

A busca nas bases durante esta etapa ocorreu em novembro de 2022. O objetivo do estudo era bem específico com relação a somente a técnicas de ataques de phishing, a string procurou abranger o maior número de artigos possíveis, sendo definida por:

IEEE, Web of Science: (“phishing” OR “attack*”) AND (“social engineering” OR “techniques”)

ACM: (“phishing” OR “attack”) AND (“social engineering” OR “techniques”)

3.5 Critérios de Inclusão de Estudos:

I1) O estudo fala de algum tipo de ataque phishing e métodos de prevenção e combate.

I2) O estudo fala sobre engenharia social aplicada a fraudes.

3.6 Critérios de Exclusão de Estudos:

E1) O estudo não se encontra na língua inglesa;

E2) O estudo é duplicado;

E3) O estudo não é focado em ataques phishing;

E4) O estudo não fala sobre engenharia social.

3.7 Estratégia de busca para a identificação dos artigos:

A aplicação da string nas bases de dados escolhidas ocorreu por método de pesquisa automática para abstract, sendo selecionado o período de publicação entre 2019-2022.

3.8 Estratégia para seleção dos trabalhos:

Os metadados (título, resumo e palavras-chaves) de todos os trabalhos obtidos foram importados para o Mendeley, visando à organização e a documentação em planilhas específicas para cada fonte de busca na ferramenta Excel. Após a exportação dos metadados em arquivo de formato BibTeX, foram realizadas sucessivas avaliações de todos os trabalhos. As avaliações foram realizadas em 3 fases com o uso das ferramentas Parsifal e Microsoft Excel.

1ª Fase: Leitura dos títulos e resumos dos artigos identificados na busca inicial das bases selecionadas. Foi feita a filtragem dos arquivos retirando os duplicados e foram aplicados os critérios de inclusão e exclusão em cada estudo. Foram documentados os arquivos selecionados em uma planilha do Excel para próxima fase.

2ª Fase: Leitura da introdução e da conclusão dos artigos que foram incluídos na 1ª fase. Foi gerada uma nova planilha, foram aplicados os critérios de inclusão e exclusão e depois documentados os arquivos que iriam para a terceira fase de avaliação.

3ª Fase: Leitura completa dos artigos incluídos na 2ª Fase, uma planilha final foi gerada com os artigos incluídos que farão parte da Síntese da Revisão Sistemática de Literatura.

3.9 Estratégia de extração e síntese dos dados:

a) Descrição do tipo de ataque phishing apresentado;
b) Descrição do método, técnica ou framework utilizado para detecção e combate.

Estratégia de análise dos dados para publicação dos resultados:

a) Resumo comparativo entre os tipos de phishing e as técnicas detecção e combate apresentadas nos estudos;
b) Como os dados obtidos ajudam a responder à pergunta de pesquisa.

4. RESULTADOS

4.1 Resumo da Condução da Revisão Sistemática

Conforme pode-se visualizar na Figura 5, a condução da revisão sistemática da literatura foi executada da seguinte forma:

Em primeiro lugar houve a identificação dos artigos através dos motores de busca, ACM com 62 artigos, IEEE com 42 artigos e Web of Science com 48 artigos.

Em segundo lugar, partiu-se para a seleção dos artigos, que se dividiu em 3 fases:

Fase 1- Em primeiro lugar foi feita a avaliação dos artigos a partir da leitura do título e resumo, e com isso se chegou a 26 artigos selecionados;

Fase 2- Foi feita a avaliação dos artigos a partir da leitura da introdução e conclusão dos artigos, chegando a 18 artigos selecionados;

Fase 3- Por fim, após a leitura completa dos 18 artigos, chegou-se ao total de 10 artigos selecionados.

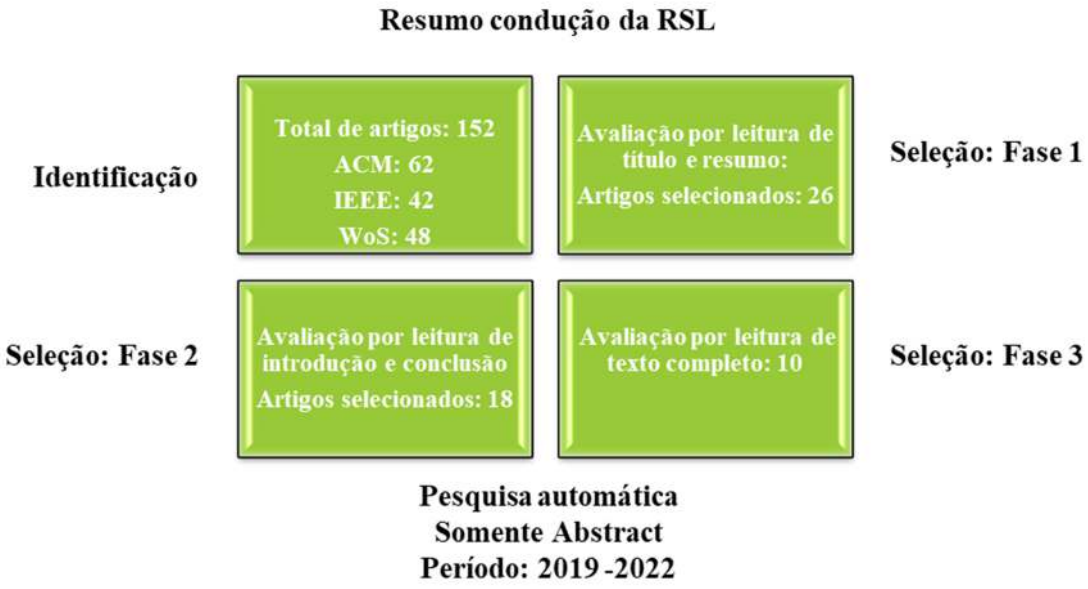

Figura 5 – Resumo da condução da RSL.

Fonte: Elaborado pelos autores.

4.2 Seleção final dos artigos da revisão sistemática da literatura

Na terceira fase da seleção dos artigos, foram escolhidos 10 artigos onde foi efetuada a leitura integral, segue abaixo a seleção elencada no Quadro 2.

N	Artigo	Ano	Autor	DOI
1	**Towards the Detection of Phishing Attacks**	**2020**	Athulya, A. A. Praveen, K.	10.1109/ICOEI48184.2020.9142967
2	**A comprehensive survey of AI-enabled phishing attacks detection techniques**	**2020**	Basit, Abdul, Zafar, Maham, Liu, Xuan Javed, Abdul Rehman Jalil, Zunera Kifayat, Kashif	10.1007/s11235-020-00733-2
3	**Inside a Phisher's Mind: Understanding the Anti-phishing Ecosystem Through Phishing Kit Analysis**	**2018**	Oest, Adam Safei, Yeganeh Doupe, Adam Ahn, Gail Joon Wardman, Brad Warner, Gary	10.1109/ECRIME.2018.8376206
4	**Phishing Detection Techniques: A Comparative Study**	**2021**	Srivastava, Sangeeta Gupta, Sudhir Kumar	10.1109/ICRITO51393.2021.9596093
5	**Real-Time Threat Intelligence-Block Phising Attacks**	**2021**	Swarnalatha, K. S. Ramchandra, K. C. Ansari, Kaushar Ojha, Love Sharma, Sanjok Subedi	10.1109/CSITSS54238.2021.9683237
6	**Preventive Techniques of Phishing Attacks in Networks**	**2021**	Adil, Muhammad, Khan, Rahim, Nawaz Ul Ghani, M. Ahmad	10.1109/ICACS47775.2020.9055943
7	**Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted**	**2021**	Baig, Muhammad Sawood, Ahmed, Faisal, Memon, Ali Mobin	10.1109/ICCIS54243.2021.9676394
8	**Detecting Telephone-based Social Engineering Attacks using Scam Signatures**	**2021**	Derakhshan, Ali Harris, Ian G Behzadi, Mitra	10.1145/3445970.3451152
9	**Mitigating Phishing Attacks: An Overview**	**2019**	Sumner, Alex Yuan, Xiaohong	10.1145/3299815.3314437
10	**Detection of Phishing Emails using Machine Learning and Deep Learning**	**2022**	Shalini, Lingampally, Manvi, Sunilkumar S., Gowda, Naveen Chandra, Manasa, K. N.	10.1109/ICCES54183.2022.9835846

Quadro 2 – Trabalhos Selecionados na Síntese da Revisão Sistemática
Fonte: Elaborado pelos autores.

4.3 Síntese da Revisão Sistemática

N	Artigo	Ano	Autor	Tipos de ataque phishing	Técnica de detecção e prevenção proposta
1	**Towards the Detection of Phishing Attacks**	**2020**	Athulya, A. A. Praveen, K.	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Abordagem baseadas em listas, motores de busca e crowdsourcing;
2	**A comprehensive survey of AI-enabled phishing attacks detection techniques**	**2020**	Basit, Abdul, Zafar, Maham, Liu, Xuan Javed, Abdul Rehman Jalil, Zunera Kifayat, Kashif	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Soluções baseadas no conteúdo do website(Deep Learning, machine learning, eurística);
3	**Inside a Phisher's Mind: Understanding the Anti-phishing Ecosystem Through Phishing Kit Analysis**	**2018**	Oest, Adam Safei, Yeganeh Doupe, Adam Ahn, Gail Joon Wardman, Brad Warner, Gary	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Website(Abordagem baseadas em listas, motores de busca e crowdsourcing;
4	**Phishing Detection Techniques: A Comparative Study**	**2021**	Srivastava, Sangeeta Gupta, Sudhir Kumar	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Soluções baseadas no conteúdo do website(Deep Learning, machine learning, eurística);
5	**Real-Time Threat Intelligence-Block Phising Attacks**	**2021**	Swarnalatha, K. S. Ramchandra, K. C. Ansari, Kaushar Ojha, Love Sharma, Sanjok Subedi	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Soluções baseadas no conteúdo do website(Deep Learning, machine learning, eurística);
6	**Preventive Techniques of Phishing Attacks in Networks**	**2021**	Adil, Muhammad, Khan, Rahim, Nawaz Ul Ghani, M. Ahmad	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Educação do usuário , Abordagem baseadas em listas, motores de busca, método passivo
7	**Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted**	**2021**	Baig, Muhammad Sawood, Ahmed, Faisal, Memon, Ali Mobin	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Educação do usuário e técnica de data mining
8	**Detecting Telephone-based Social Engineering Attacks using Scam Signatures**	**2021**	Derakhshan, Ali Harris, Ian G Behzadi, Mitra	1- Ataques baseados em engenharia social. 2- Ataques baseados em	Solução baseadas em machine learning, scan signature.
9	**Mitigating Phishing Attacks: An Overview**	**2019**	Sumner, Alex Yuan, Xiaohong	1- Ataques baseados em engenharia social. 2- Ataques baseados em	Educação do usuário, esquemas automatizados de detecçao.
10	**Detection of Phishing Emails using Machine Learning and Deep Learning**	**2022**	Shalini, Lingampally, Manvi, Sunilkumar S., Gowda, Naveen Chandra, Manasa, K. N.	1- Ataques baseados em engenharia social. 2- Ataques baseados em subterfúrgios técnicos.	Soluções baseadas no conteúdo do website(Deep Learning, machine learning, eurística);

Quadro 3 – Síntese da revisão sistemática
Fonte: Elaborado pelos autores.

O quadro 3 apresenta uma síntese do que cada artigo selecionado mencionou com relação aos tipos de ataques phishing mais atuais, sendo separado por 2 grandes grupos: Ataques baseados em engenharia social e ataques baseados em subterfúgios técnicos. O ainda apresenta os tipos de ataques phishing que praticamente se repete em todos os trabalhos. Com relação às técnicas que detecção, os autores apresentam em seus trabalhos técnicas diferentes, que acreditam serem mais eficazes para a detecção e prevenção de ataques.

As técnicas de prevenção e detecção mais citadas pelos autores foram:

- Educação do usuário;

- Abordagem baseadas em listas(whitelist e blacklist);
- Abordagens baseadas em machine learning e deep learning;
- Abordagem baseadas em técnicas híbridas;
- Abordagens baseadas em motores de busca.

4.4 Análise dos resultados

Após a leitura minuciosa e completa dos trabalhos incluídos após a terceira avaliação, foi elaborado, na síntese da revisão sistemática, um resumo dos sistemas de detecção de phishing apresentados em cada estudo, conforme pode ser visto no Quadro 3, os dados reunidos neste estudo foram organizados para responder à questão de pesquisa.

Ao analisar os 10 artigos pode-se dizer que diversos estudos fazem a utilização de algoritmos de aprendizado de máquina para a identificar onde há páginas maliciosas. Grande parte desses algoritmos são classificadores. Exemplos de algoritmos mais citados nos trabalhos são o Random Forest e o Árvore de Decisão. Os autores também mencionam a mudança de configuração de tais algoritmos com objetivo de melhorar a eficácia dos mesmo e propõem novos atributos (features) para fornecer aos algoritmos de aprendizado de máquina mais informações sobre páginas maliciosas.

Athulia et al.(2020) propõe uma arquitetura para detectar a página Web phishing no navegador do lado do cliente. Os principais componentes da arquitetura são utilização de whitelist, blacklist e motores de busca.

Srivastava e Gupta(2021) citam que muitas abordagens de detecção foram tomadas a partir das técnicas baseadas em regras, onde os algoritmos têm dados suficientes para identificar mensagens de phishing e site, com algoritmos totalmente automatizados baseados em deep learning, onde o aplicativo será capaz de bifurcar phishing e sites genuínos sem envolvimento humano ou pouco envolvimento.

Alguns autores como Derakhshan et al.(2021) construíram bases de dados para treinamento de modelos para identificação de páginas de phishing juntando uma base de páginas de phishing com uma base de páginas legítimas. Os autores também concordam que o conjunto de páginas que compõe uma base de dados bem como o conjunto de atributos extraídos das páginas são fatores determinantes acurácia dos modelos treinados.

Para Basit et al.(2021) estratégias de como heurística, aprendizado de máquina e algoritmos de deep learning possuem altos custos computacionais. Os métodos heurísticos e de mineração de dados têm altas taxas de FP, no entanto, são melhores em distinguir ataques de phishing. Os procedimentos de aprendizado de máquina fornecem os melhores resultados quando contrastados com diferentes estratégias. Uma parte dos procedimentos de aprendizado de máquina pode identificar até 99%. Hoje em dia, os métodos de aprendizagem profunda e de aprendizagem automática são usados para detectar um ataque de phishing. métodos de classificação como Random Forest, Suport Vector Machine e Decision Tree também são comuns. Esses métodos são mais úteis e eficazes para detectar o ataque de phishing.

Para Younis e Musbah(2020) a utilização de algoritmos de aprendizado de máquina e filtros de phishing parece ser a primeira linha de defesa, mas os métodos de conscientização e as ferramentas de detecção dos usuários não devem ser negligenciados.

Oest et al.(2018) em seu trabalho mostraram como funciona o ecossistema anti phishing como um todo. Os autores explicam que com a combinação do esquema de classificação de URL e analisando a idade do domínio, pode-se traçar o perfil não só onde um ataque de phishing provavelmente originado em termos de infraestrutura, mas também porque essa URL foi escolhida. Os autores indicam que as abordagens de ML são populares para a detecção de sites de phishing e se tornam um problema de classificação simples. Eles explicam que para treinar um modelo de aprendizado de máquina para um sistema de detecção baseado em aprendizado, os dados em questão devem ter recursos relacionados a phishing e classes legítimas de sites e ainda que diferentes classificadores são usados para detectar um ataque de phishing.

Swarnalatha et al.(2021) em seu trabalho relatam que detectar e prevenir o ataque de phishing já era tão importante e ainda continuará sendo no futuro. Eles acreditam que em todos os sites maliciosos, para um melhor resultado de detecção deve-se fornecer a classificação precisa com base no modelo de treinamento, usando o melhor algoritmo de aprendizado de máquina .

Adil et al.(2020) acredita que além da educação do usuário, detecção e prevenção de ataques de phishing através de IDS e IPS, servidor antiphishing, barra de ferramentas de segurança do servidor web e honey pots são as melhores opções para os ataques phishing.

Baig et al.(2021) em seu trabalho menciona que deve-se aumentar a conscientização, além disso menciona que ferramentas, cuidados com spams, não clicar em links suspeitos e não compartilhar dados pessoais são algumas formas de se prevenir do phishing. O trabalho também menciona a técnica de data mining como forma de deteção.

Derakhshan et al.(2021) apresenta em seu trabalho uma técnica de detecção que utiliza uma assinatura fraudulenta para identificar uma classe de ataques de engenharia social de forma única, da mesma forma que as assinaturas de malware são usadas para identificar malware, as assinaturas são baseadas no conteúdo da conversa.

Sumner et al.(2019) apesar de mencionar a importância de métodos automatizados de detecção de phishing, em seu trabalho focou na educação do usuário como método de prevenção e detecção de phishing.

Shalini et al.(2022) em seu trabalho desenvolveu um modelo a partir de machine learning e deep learning que detecta e-mails de entrada de usuários, sendo eles genuínos ou fraudulentos. Os autores acreditam que a detecção de e-mails desempenha um papel muito importante em cenários em tempo real

5. Conclusão

Em primeiro lugar, neste trabalho foram apresentados os conceitos e teorias dos principais temas que levam resposta à questão de pesquisa:

Quais são as tipos de técnicas mais recentes de phishing e quais são as técnicas de detecção e combate mais utilizadas para cada caso?

A resposta foi obtida através da revisão sistemática da literatura conduzida neste trabalho.

Em um segundo momento, foram apresentados os principais conceitos, objetivos e importância da revisão sistemática da literatura em um projeto de pesquisa. Nesta etapa forma apresentadas a fase de planejamento com o protocolo da pesquisa, a síntese final com os artigos encontrados e selecionados e por fim a análise e conclusão dos resultados obtidos no trabalho de pesquisa.

A revisão sistemática da literatura evidenciou que phishing é uma das técnicas de ataque mais utilizadas e por esse motivo diversos autores desenvolvem trabalhos com objetivo de apresentarem técnicas, modelos, frameworks para a identificação dos tipos de phishing existentes. A diversidade de tipos de ataques phishing requerem técnicas especificam para sua detecção e combate. Embora alguns autores citem a importância da educação do usuário para evitar que se torne uma vítima do golpe, a grande maioria dos trabalhos citam que técnicas que utilizam de subterfúgios técnicos são mais eficazes para a deteção e combate. Dentre as técnicas que utilizam o subterfúgio técnico, é notória a preferência entre os autores na utilização de modelos de treinamentos baseados em machine learning e deep learning para a classificação e identificação de páginas phishing.

REFERÊNCIA BIBLIOGRÁFICA

BASIT, A. et al. A Comprehensive Survey of AI-Enabled Phishing Attacks Detection Techniques. **Telecommun. Syst.**, v. 76, n. 1, p. 139–154, jan. 2021.

BAIG, M. S.; AHMED, F.; MEMON, A. M. **Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted**. 2021 4th International Conference on Computing & Information Sciences (ICCIS). **Anais**...IEEE, 2021. Disponível em: <https://ieeexplore-ieee-org.ez67.periodicos.capes.gov.br/document/9676394/>. Acesso em: 3 nov. 2022.

BEPPLER, T. et al. **Notícias Falsas, Dano Real: Levantamento, Análise e Discussão de Phishing, Malware e Fake News sobre COVID-19**. [s.l.] Association for Computing Machinery, 2021. v. 1

HIJJI, M.; ALAM, G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. **IEEE ACCESS**, v. 9, p. 7152–7169, 2021.

LEE, J. et al. Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. **IEEE ACCESS**, v. 9, p. 80866–80872, 2021.

LEONOV, P. Y. et al. The main social engineering techniques aimed at hacking information systems. **Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021**, p. 471–473, 2021.

Nakagawa, E. Y., Scannavino, K. R. F., Fabbri, S. C. P. F., & Ferrari, F. C. (2017). *Revisão sistemática da literatura em engenharia de software: teoria e prática*. Elsevier Brasil.

MORGAN, Steve (ed.). **Cybercrime to cost the world $10.5 Trillion annually by 2025**. 2020. Pesquisa elaborada por Cybersecurity Ventures. Disponível em: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. Acesso em: 10 nov. 2022.

OEST, A. et al. Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. eCrime Researchers Summit, eCrime, v. 2018- May, p. 1–12, 2018.

SRIVASTAVA, S.; GUPTA, S. K. Phishing Detection Techniques: A Comparative Study. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021, p. 1–6, 2021.

SUMNER, A.; YUAN, X. Mitigating Phishing Attacks: An Overview. Proceedings of the 2019 ACM Southeast Conference. Anais...: ACM SE '19.New York, NY, USA: Association for Computing Machinery, 2019

SWARNALATHA, K. S. et al. Real-Time Threat Intelligence-Block Phising Attacks. **CSITSS 2021 - 2021 5th International Conference on Computational Systems and Information Technology for Sustainable Solutions, Proceedings**, 2021.

YANG, Z. et al. Phishing Email Detection Based on Hybrid Features. 2018 4TH INTERNATIONAL CONFERENCE ON ENVIRONMENTAL SCIENCE AND MATERIAL APPLICATION. Anais...: IOP Conference Series-Earth and Environmental Science.DIRAC HOUSE, TEMPLE BACK, BRISTOL BS1 6BE, ENGLAND: IOP PUBLISHING LTD, 2019.

YOUNIS, Y. A.; MUSBAH, M. A Framework to Protect Against Phishing Attacks. Proceedings of the 6th International Conference on Engineering & MIS 2020. Anais...: ICEMIS'20.New York, NY, USA: Association for Computing Machinery, 2020.

https://www.ibm.com/downloads/cas/RKV2BV2Z

https://www.kaspersky.com.br/about/press-releases/2021_no-brasil-e-mais-comum-vazar-dados-pessoais-de-funcionarios-do-que-de-clientes-aponto-estudo-da-kasperksy

https://www.nic.br/noticia/na-midia/cyber-cultura-o-impacto-da-pandemia-no-uso-da-internet/