CIBERSEGURANÇA: Ameaças de *phishing* relacionadas a *roubo de identidade*

Brendo Barbosa Soares[1]

César Fernandes Ribeiro Filho[2]

RESUMO

O presente artigo destaca a importância da cibersegurança devido à presença crescente da tecnologia digital na sociedade. Ele aborda as ameaças cibernéticas relacionadas a *phishing* para com o *roubo de identidade*, e explora medidas de proteção contra esses crimes. A pesquisa investiga as principais ameaças cibernéticas relacionadas ao *phishing*, como s*pear phishing, pharming, vishing e smishing* e como esses crimes são executados. O problema da pesquisa é buscar soluções contra esses crimes. Pois a falta de conhecimento e boas práticas de segurança de dados é identificada como uma hipótese para que essa prática tenha sucesso. A metodologia utilizada foi a revisão sistemática, onde houve uma análise sobre as ameaças de *phishing* nos trabalhos selecionados. A pesquisa envolveu a busca de artigos nos bancos de dados do Google Acadêmico e SciELO, com critérios de inclusão e exclusão específicos. Dos 60 artigos analisados, seis foram selecionados. Um levantamento revelou que 1.378 participantes estavam envolvidos em pesquisas relacionadas ao *roubo de identidade* por meio de *phishing*. Os resultados mostram que as medidas propostas respondem ao problema de pesquisa e enfatizam a necessidade de conhecimento e adoção de medidas de segurança para combater os crimes cibernéticos e proteger os dados pessoais. confirmando a hipótese da importância do conhecimento na prevenção desses crimes

Palavras-chave: Cibersegurança.*Roubo de identidade*.*Phishing*

1 INTRODUÇÃO

A segurança na internet tem se tornado cada vez mais importante nos dias de hoje, devido à crescente presença da tecnologia digital na sociedade. Com os avanços tecnológicos, é possível armazenar informações pessoais que precisam ser protegidas contra ameaças

[1]Aluno do curso de graduação em Bacharelado em Sistemas de Informação Centro Universitário do Sul de Minas. Email: brendo.soares@alunos.unis.edu.br

[2] Professor do Centro Universitário do Sul de Minas - UNIS, formado em ciência da computação e Administração com Mestrado em Administração. cesar.filho@professor.unis.edu.br

cibernéticas. A proteção desses dados é de grande importância, uma vez que informações pessoais são constantemente compartilhadas em plataformas digitais, e se esses dados caírem nas mãos de criminosos, poderão ocorrer danos irreparáveis, como *roubo de identidade*, invasão de privacidade e fraudes financeiras.

O problema de pesquisa se baseia na seguinte questão: Quais medidas podem ser adotadas contra crimes relacionados a *phishing* referente ao *roubo de identidade*? No cenário atual, é comum ler ou ver notícias que relatam golpes cibernéticos, sendo os exemplos mais comuns contas hackeadas em redes de mídias sociais, bancos, telefonia, entre outros. A maioria desses golpes ocorre por meio de gatilhos chamativos que despertam interesses, como oportunidades imperdíveis ou vantajosas.

O objetivo desta pesquisa consistiu em investigar de forma exploratória as principais ameaças cibernéticas relacionadas ao *phishing* e seus principais ataques, como *phishing, spear phishing, pharming, vishing e smishing*, que influenciam no *roubo de identidade* em ambientes digitais. A narrativa da pesquisa busca esclarecer como esses crimes cibernéticos são executados e por meio de quais ferramentas são aplicados.

A falta de conhecimento e boas práticas de segurança de dados é identificada como uma hipótese para que essa prática tenha sucesso. É importante abordar concepções importantes de medidas de segurança e iniciativas de prevenção dessas ameaças, uma vez que a falta de conhecimento e boas práticas de segurança de dados pode ser a maior aliada dessas ameaças. Segundo Rodrigues (2020), o avanço desenfreado da tecnologia tende a trazer diversas consequências na área do conhecimento humano. Portanto, este artigo se justifica em promover conhecimentos e informações sobre boas práticas para garantir a segurança dos dados contra esses golpes.

Esta pesquisa consistiu em uma busca bibliográfica descritiva e uma revisão sistemática da literatura sobre cibersegurança, *phishing e roubo de identidade*. Foram utilizados os bancos de dados do Google Acadêmico e SciELO para encontrar artigos publicados entre 2017 e 2022. Os critérios de inclusão envolveram a seleção de artigos em português e relacionados ao tema, enquanto os critérios de exclusão foram artigos incompletos ou sem análise de dados. Após a análise de 60 artigos, seis foram selecionados para esta pesquisa. A revisão sistemática possibilitou uma análise cuidadosa e imparcial das informações disponíveis, assegurando a confiabilidade e a validade dos resultados obtidos.

2 REVISÃO DA LITERATURA

2.1 Cibersegurança

Antes da globalização da rede de dados não havia uma certa preocupação em relação a segurança, pois era usada apenas para encaminhar e-mails e uso de impressoras compartilhadas em empresas, mas com o crescimento exponencial de usuários que utilizam as redes para realizar atividades comuns como operações bancárias, compras, compartilhar dados importantes entre outros, a segurança se tornou um grande problema (TANENBAUM, 2021).

A cibersegurança tem como objetivo evitar que usuários maliciosos tenham acesso a informações sigilosas de outros usuários, pois muitas dessas ações são para obter benefícios ou prejudicar pessoas. Impedindo o acesso remoto de serviços que os usuários não têm autorização para uso, lidando com ameaças e ataques cibernéticos e verificando se as informações são verdadeiras (TANENBAUM, 2021).

2.2 Roubo de identidade

O *roubo de identidade* ocorre com a exposição dos dados pessoais no ciberespaço, como: cpf, identidade, endereços, dados bancários e senhas na internet. Que se tornam dados valiosos para cibercriminosos usarem de formas indevidas. Dantas (2022, p.32), descreve que: “Existem vários graus de *roubo de identidade* que podem ocorrer. As instâncias comuns incluem o uso de suas informações para se inscrever em um cartão de crédito, fazer criar contas falsas, chantagear alguém que conhece ou aplicar o golpe de *phishing*”.

Em um levantamento feito pela Serasa Experian, no ano de 2022 constatou que 80% dos brasileiros se preocupam com o roubo de suas identidades e 61% dos entrevistados afirmou que já foram vítimas ou conhecem experiências de outras pessoas próximas.

Com as facilidades promovidas pela era digital é possível que dados pessoais sejam armazenados ou vinculados a uma única conta, e-mail e aplicativos bancários. Se essas informações não estiverem seguras o risco de roubo de dados cresce de forma significativa (PAULO, 2021).

2.3 Phishing

Phishing é uma crime que fisga dados pessoais, senhas, dados bancários, informações de organizações, empresas, entre outros. Pinheiro (2020, p. 16), define *phishing* como:

> consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um link falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios.

E-mail, sms ou ligações telefônicas são as principais meios para a disseminação de *phishing*, onde criminosos agem de forma sutil para atrair as vítimas com mensagens bem elaboradas com aspectos oficiais de uma instituição, instigando o interesse com ofertas tentadoras ou com caráter de urgência como assegurar de que à problemas com a conta bancária da vítima.

Segundo uma pesquisa da empresa cibernética PSAFE, no primeiro semestre de 2022 houve mais de 5 milhões tentativas de golpes caracterizados em *phishing* no setor bancário brasileiro, ocorrendo um aumento de 97% comparado ao mesmo período de 2021 (OLIVEIRA,2022).

Sendo uma prática mais comum de cibercrime, o *phishing* pode ser aplicado sem que haja alguma desconfiança da vítima, mesmo que seja um ataque simples, a falta de conhecimento e o comportamento emocional da vítima possibilita uma facilidade para o fornecimento de dados pessoais.

Para enfatizar o autor Teixeira (2022, p. 237), aborda que: “ A falta de conscientização da importância de prevenção, com a adoção de medidas de segurança, reflete outra fragilidade da internet. Ou melhor, muitos se utilizam da internet sem a preocupação do perigo de invasão ao computador”.

2.3.1 Spear Phishing

Spear phishing denomina em um ataque direcionado a um indivíduo ou organização específica via e-mail, onde os cibercriminosos se passam por pessoas conhecidas das vítimas e tentam ludibriar para obter informações, senhas e dados bancários. capaz de instalar um malware remoto a fim de ganhos financeiros (IBM, 2022).

2.3.2 Pharming

É um tipo de crime semelhante ao *phishing*, mas o ataque do *pharming* consiste em envenenar o DNS com a ajuda de softwares maliciosos funcionando da seguinte forma: o DNS tem a função de traduzir uma URL e converter em endereço de IP , quando o envenenamento acontece essa URL do site verdadeiro é redirecionada ao IP de um site falso com as mesmas finalidades do *phishing* (KASPERSKY, 2023).

2.3.3 Vishing

Diferente das outras formas de golpes citadas, o *vishing* é o ataque aplicado através de ligações telefônicas, voicemail e VoIP. No qual os criminosos se passam por representantes bancários, comerciais ou pessoas próximas, induzindo a vítima a fornecer informações pessoais, muitas vezes acontece a tentativa de extorsão pelo falso sequestro (AVAST, 2022).

2.3.4 Smishing

O *smishing* é aplicado especificamente por SMS com links maliciosos, mesmo que seja uma ferramenta de comunicação obsoleta que ainda traz grande vantagem aos cibercriminosos em utilizá-la, segundo um levantamento da PSAFE houve mais de 150 milhões de pessoas que caíram nesse golpe no ano de 2021. Na maioria dos casos são falsos alertas de bancos avisando operações em contas bancárias da vítima, instigando-a entrar nesses links que redirecionam para falsas centrais (MOURA, 2021).

3 MATERIAL E MÉTODOS

Essa pesquisa foi desenvolvida através de uma busca bibliográfica descritiva sobre os seguintes assuntos: cibersegurança, *phishing*, *spear phishing, pharming, vishing, smishing e roubo de identidade*. E uma revisão sistemática da literatura, da qual utilizou os seguintes bancos de dados: Google acadêmico e SciELO como fonte de busca de artigos públicos entre os anos de 2017 a 2022. Onde as palavras chaves de pesquisas foram “ Phishing”, “Ataques de phishing” e “ Cibersegurança”.

Os critérios de inclusão propostos foram: a busca por artigos publicados nos últimos cinco anos, a preferência de artigos na língua portuguesa e que tivessem relações com o tema da pesquisa, já os critérios de exclusão foram de artigos não disponibilizados na íntegra e que não houvesse resultados ou análise de dados na prática. Foram analisados 60 artigos através das palavras chaves de busca, porém seis artigos foram selecionados após cumprirem os critérios de inclusão e exclusão.

4 DISCUSSÃO E RESULTADOS

Após a revisão dos trabalhos selecionados foi feito uma tabela individual descrevendo alguns dados e um resumo de cada artigo, como pode ser observado logo abaixo:

Título: TÉCNICA PHISHING SIMPLES, MAS EFICAZ
Data: 2017 **Autores:** Faria
Resumo: Este artigo consiste em um estudo que aborda a técnica de *phishing*, a qual é empregada por indivíduos mal-intencionados com o intuito de obter informações pessoais e financeiras das vítimas. O objetivo principal deste estudo é analisar a relevância do fator humano no campo da Segurança da Informação, considerando a utilização da técnica de *phishing*. Para isso, foi conduzida uma pesquisa experimental envolvendo uma determinada população de usuários, na qual a técnica de *phishing* foi utilizada para coletar dados que posteriormente foram analisados. A partir dessa análise, foram identificadas as consequências do *phishing*, tais como a perda de informações pessoais e financeiras, e também foram apresentadas sugestões para se proteger contra essa ameaça. É fundamental estar ciente desse problema e manter-se vigilante ao realizar transações online, pois a melhor defesa contra essa ameaça é a conscientização.

Título: PHISHING E REDES SOCIAIS: UM ESTUDO DE CASO
Data: 2019 **Autores:** Pessoa
Resumo: É um estudo aprofundado sobre a utilização de *phishing* em redes sociais e as medidas de segurança que podem ser adotadas para evitar ataques, apresentando o conceito de *phishing*, suas características e como ele pode ser utilizado em redes sociais. No qual foi realizado um estudo de caso através de um formulário na ferramenta Google Forms e aplicado a uma amostra de usuários de uma rede social específica que haviam sido vítimas de ataque de phishing e propondo medidas de segurança que podem ser adotadas para evitar ataques.

Título: ENGENHARIA SOCIAL COMO AMEAÇA AO SETOR BANCÁRIO: USO DO PHISHING PARA COLETAR INFORMAÇÕES DOS CORRENTISTAS E A NECESSIDADE DE ESTRATÉGIAS DE SEGURANÇA.
Data: 2019 **Autores:** Silva
Resumo:O artigo faz uma análise detalhada abordando o conceito phishing, *spear phishing* e outras técnicas utilizadas pelos criminosos para obter informações dos correntistas. Com a realização de uma pesquisa com usuários de bancos convencionais e digitais. Por fim, algumas dicas são compartilhadas para que medidas sejam tomadas pelo usuário para evitar que esses ataques aconteçam.

Título: VITIMAÇÃO POR PHISHING: UM ESTUDO EMPÍRICO
Data: 2022 **Autores:** Alexandra
Resumo: Esse artigo faz uma análise de vítimas de ataques de *phishing*, no qual investiga as variáveis que aumentam a probabilidade de responder a ataques *phishing*, incluindo características sociodemográficas, traços de personalidade e o autocontrole. Além disso, o estudo procura entender se as variáveis contextuais, como exposição à internet ou medidas preventivas, são importantes para explicar a vitimação por *phishing*. Os resultados indicam que traços de personalidade, como impulsividade e baixo autocontrole, são fatores de risco para a vitimização, assim como a exposição à internet e a falta de medidas preventivas.

Título: ANÁLISE PRÁTICA E MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NA ERA DIGITAL
Data: 2022 **Autores:** Rannyson
Resumo: Este estudo aborda a Engenharia Social com relação ao *phishing*, revelando as técnicas utilizadas por invasores para obter informações confidenciais de indivíduos e empresas. O trabalho apresenta uma análise prática desde a coleta de informações de um alvo até o uso de ferramentas de testes de invasão. O objetivo do estudo é alertar os usuários e empresas sobre os perigos expostos na internet e ajudá-los a proteger seus dados. O artigo destaca a importância de se conhecer as principais técnicas utilizadas por invasores e como se proteger contra elas.

Título: CIBERSEGURANÇA NO NOVO MUNDO DIGITAL: COMO ALERTAR OS IDOSOS SOBRE OS RISCOS CIBERNÉTICOS DESCENDENTE DO PHISHING NA UTILIZAÇÃO DOS SMARTPHONES
Data: 2022 **Autores:** Henrique
Resumo: O foco desta pesquisa foi de como alertar os idosos sobre os riscos cibernéticos descendentes do *phishing* na utilização dos smartphones, que tem como objetivo discutir os principais riscos cibernéticos aos quais os idosos estão expostos ao utilizar smartphones e como eles podem se proteger contra esses ataques. A parte prática consistiu em uma pesquisa aplicada com abordagem exploratória, o estudo foi realizado por

meio de um questionário para a coleta de dados. O trabalho oferece sugestões práticas para que os idosos possam se proteger contra os ataques cibernéticos.

4.1 Dados coletados

Após analisar os trabalhos selecionados houve um levantamento que constatou um total de 1.378 participantes de pesquisas relacionadas à *phishing*, *spear phishing, pharming, vishing, smishing* para com o roubo de dados pessoais. houve estudo que a coleta de dados foi por meio de experiência prática e outros por meio de questionários, onde as coletas por meio de questionários submeteram 95,6% do total de participantes.

Dos trabalhos selecionados o do Faria, 2017 se diferencia, pois foi o único que realizou uma experiência com os participantes. Que se sucedeu da seguinte maneira: foi um experimento por meio de uma isca de *phishing*, na qual foi criada uma página idêntica de login do pacote office 365 da Microsoft com um protocolo de HTTPS diferente do original.

Logo em seguida foi mandado um e-mail para os participantes com critério de emergência com o link da conta falsa para fazer o login, se caso o participante fizesse o login através do link, suas informações seriam armazenadas em um arquivo de texto e o usuário seria direcionado a página oficial. Dos 60 participantes 51% foram vítimas do experimento, pois alegaram que agiram por fatores emocionais ou foram desatentos.

Os demais trabalhos analisados utilizaram uma abordagem quantitativa, e os instrumentos utilizados para a coleta de dados foram questionários ou formulários. A seguir o destrinchamento de partes importantes de cada um servirá como base para os resultados deste artigo:

No trabalho de Pessoa, 2019 foi realizado um estudo de caso de ataques de *phishing* em redes sociais, a coleta de dados consistiu em um formulário com perguntas objetivas, onde foi executado através do google forms, no que resultou em um total de 153 participantes .Alguma das perguntas feitas com relação ao tema era direcionada a saber se o participante tinha algum conhecimento sobre o assunto, sendo que 93,5% sabia da possibilidade de ter dados roubados no mundo virtual, mas 68% não conheciam o termo *phishing*.

Já outras perguntas eram voltadas à auto reflexão para o participante refletir e opinar se em algum momento já chegou a pensar o quanto expunha suas informações através da internet, no qual a resposta foi que 77,1% responderam que já refletiram sobre o assunto.

Em uma pergunta relacionada a cadastros e compras em e-commerce foi questionado se o participante verificava se a página ou navegação era segura antes de inserir informações pessoais ou bancárias. De acordo com os resultados obtidos, 84,3% diziam ter essa preocupação e 15,7% não se preocupava ou achava irrelevante.

E por fim uma pergunta que fez um levantamento de vitimização por meio de *phishing* na qual o interesse era saber se o participante ou algum conhecido já foram vítimas desse tipo de ataque. Onde grande maioria respondeu que já foi vítima ou conhece quem teria sido, representando 67,5% do total de participantes.

Já no trabalho de Silva, 2019, realizou-se um estudo com 15 vítimas que sofreram com algum tipo de ataque relacionado a *phishing* no setor bancário, por meio de um questionário,com o objetivo principal de identificar possíveis características em comuns entre as vítimas.

Uma das perguntas do questionário era se a vítima costumava a usar com que frequência semanalmente o app ou canal web para realizar transações bancárias, dos entrevistados 33,7% responderam que sete ou mais vezes por semana, outros 46% até tres vezes por semana.

Noutra pergunta a questão levantada foi entender qual foi o motivo dos entrevistados fornecerem suas informações bancárias em páginas falsas ou manipuladas por algum tipo de *phishing*. Destes, 53,3% acharam que estivesse ganhando alguma premiação ofertada pelo suposto site, já outros 33,3% acreditaram que estariam compartilhando com a página oficial do banco.

Em quesito de segurança foi questionado se os entrevistados já teriam buscado se informar quanto a quais medidas de segurança poderiam ser adotadas para o cuidado de suas informações sigilosas. A pesquisa identificou que 73,3% dessas pessoas em momento nenhum buscou esse tipo de informação antes de cair no golpe.

Para finalizar o questionamento o autor fez uma pergunta interessante sobre o posicionamento dos entrevistados no contexto de que se repetisse novamente a tentativa de golpe, os mesmos caíram novamente. E a grande maioria afirmou que cairia novamente ou poderiam ser enganados de outras formas, o que representa 80% dos entrevistados.

O estudo de Alexandra, 2022 relata um estudo empírico sobre a vitimização de *phishing* por meio de um questionário com a participação de 1002 indivíduos. Referente ao conhecimento sobre o assunto, a amostra indica que cerca de 18,3% têm conhecimento a

respeito, logo 81,7% demonstraram não ter conhecimento sobre o assunto, o que é no caso um resultado insatisfatório em relação ao tamanho total dos participantes.

Das perguntas relacionadas a tentativas de ataques ou ataques efetivos, os resultados demonstraram que 74,5% dos participantes afirmaram que já teriam sofrido em algum momento algum tipo de tentativa relacionado a *phishing*, já os outros 25,5% afirmaram ter caído em golpes nesse sentido.

Em questão a que meio de comunicação receberam os ataques, a amostra resultou em que a maioria dos participantes receberam uma tentativa de *phishing* via email, no caso 55.6%. Outros 43,5% relataram ter recebido tentativa de smishing via SMS, o restante sofreu tentativas vishing por meio de chamadas telefônicas.

A exposição foi outro ponto interrogativo, ao avaliar o quanto que os indivíduos se expunham na internet e tinham suas preocupações, com referência a isso resultou que uma parte de 35,6% ficavam mais expostos que o restante na internet, logo ficavam mais suscetíveis a sofrerem algum tipo de ataques relacionados a *phishing*.

Rannyson, 2022 em seu trabalho, aplicou um formulário pelo Google Forms com o objetivo de saber o grau de conhecimento das pessoas sobre a temática de engenharia social com relação a *phishing*, a pesquisa obteve 114 respostas com perguntas objetivas. A questão inicial era saber se o público pesquisado tinha algum conhecimento sobre o tema discutido anteriormente, os resultados mostraram que cerca de 49,1% não tinha conhecimento algum sobre o assunto.

Quanto ao questionamento sobre a preocupação dos questionados com sua exposição pessoal através da internet, o resultado demonstrou que cerca 95,6% tem preocupação com a exposição de seus dados pessoais, o que é de certa forma um resultado satisfatório para o pesquisador.

Com relação à vitimização por *phishing*, o questionamento era se os participantes já tinham sofrido ou conheciam alguém que foi alvo desse cibercrime. O resultado demonstrou que 34,2% declarou que conhece alguém ou ele próprio já foi lesado, outros 36,8% apenas sofreram tentativas. Já 28,9% não responderam.

Para finalizar, Henrique, 2022 realizou em seu estudo com um grupo de 34 pessoas a fim de medir o conhecimento dos participantes a ataques cibernéticos para com *phishing* e navegação com segurança pela internet. Na questão de usabilidade 79,4% tem receio de navegar ou compartilhar suas informações.

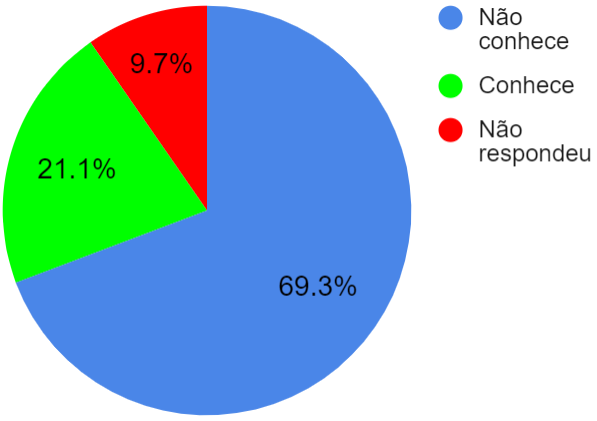
Já o conhecimento sobre o assunto de *phishing*, nota-se que 94,1% dos entrevistados não têm conhecimento algum sobre o tema. Em contrapartida 88,2% afirmaram que em algum momento já sofreram tentativas de golpes através de *vishing* ou *smishing* em algum momento da vida.

4.2 Revisão dos dados coletados

As questões explanadas foram o ponto de partida para chegar a possíveis resultados neste artigo. mesmo que cada trabalho citado tenham diferentes temáticas nesta área do saber, todas acabam se relacionando quando o assunto é ataques através de phishing, spear phishing, pharming, vishing, smishing.

Como citado anteriormente, ao reunir todas essas pesquisas a amostra total resulta em 1.378 participantes. Ao fazer o levantamento sobre o conhecimento do assunto em pesquisa, cerca de 964 participantes não têm nenhum conhecimento, já 290 relataram que têm algum conhecimento e os outros 133 não responderam. Como mostra o percentual no gráfico da figura 1:

Figura 1 – Dados sobre conhecimento relacionado a *phishing*



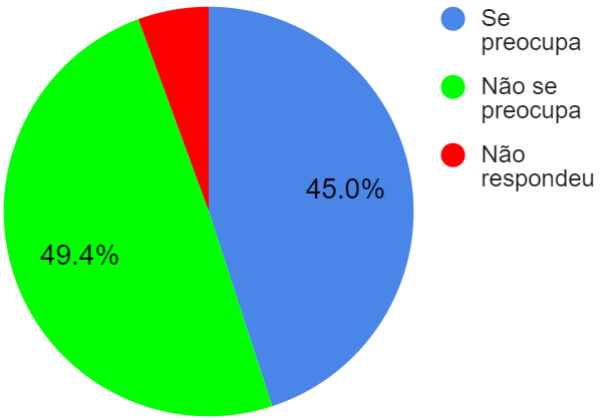
Fonte: Elaborado pelo autor – com base nas pesquisas relacionadas

Embora as práticas de cibercrimes através de *phishing* sejam comuns no cotidiano, a grande maioria não sabe seus fundamentos. Isso significa que as pessoas têm o conhecimento de que suas informações podem ser roubadas, mas não conhece as técnicas e ferramentas

empregadas por cibercriminosos para o ataque, logo ficam mais vulneráveis e suscetíveis a caírem em golpes.

Mesmo não tendo o conhecimento, a maioria dos participantes demonstraram que não se preocupam com a exposição de suas informações pessoais no ciberespaço, isso representa 681 participantes. Outros 620 dizem se preocupar com sua exposição e os 77 restantes não responderam, como mostra o percentual no gráfico na figura 2:

Figura 2 – Preocupação dos participantes com seus dados pessoais

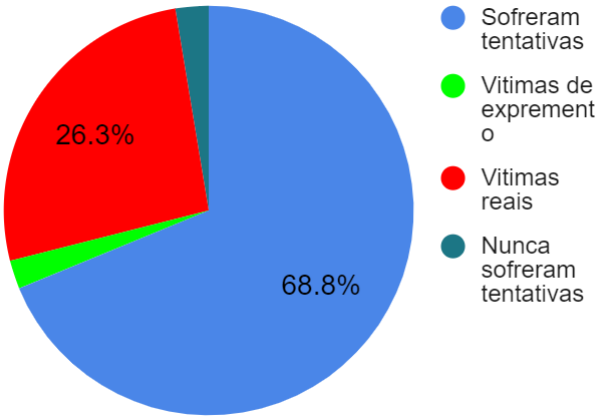


Fonte: Elaborado pelo autor – com base nas pesquisas relacionadas

Esses dados reafirmam que a falta de conhecimento gera o desinteresse das pessoas pelo cuidado com os seus dados pessoais gerando muitas vezes uma exposição desnecessária, desta maneira acaba facilitando a ação de cibercriminosos em "fisgar" essas informações expostas para obter vantagens. Por esses motivos, os ataques através de *phishing* são tão vividos no nosso cotidiano.

Embora essa prática não seja novidade em termos científicos, ela é usada a todo instante para tentar fazer vítimas. Ao relacionar os dados obtidos dos total de participantes 948 já sofreram no decorrer da vida alguma tentativa de *phishing*, *spear phishing, pharming, vishing* ou *smishing*. Outros 31 participantes foram vítimas do experimento realizado no trabalho do Faria, 2017, por outro lado 363 pessoas foram vítimas reais que perderam dados pessoais ou aquisições financeiras e uma minúscula parte de 36 participantes relataram não ter sofrido esse tipo de ataque, como mostra o percentual no gráfico na figura 3:

Figura 3 – Vitimização com ataques de *phishing*



Fonte: Elaborado pelo autor – – com base nas pesquisas relacionadas

Ao analisar a quantidade de vítimas reais nesta amostra pode-se considerar que seja uma quantidade baixa, mas no cotidiano esses valores chegam a ser alarmantes. para se ter uma ideia ao somar as tentativas com os casos reais da amostra deste estudo teremos 95,1% de participantes que já ficaram na "mira" desses ataques, agora imagine essas estatísticas em uma uma amostra maior de participantes.

Agora entrando no contexto do uso de ferramentas para a prevenção de ataques, os estudos não ofereceram dados redundantes para uma metanálise, o que se torna um ponto negativo, em contrapartida todos trabalhos destacam que o conhecimento adequado é o principal meio de prevenção no *roubo de identidade*. Claro que existem ferramentas e medidas que auxiliam na prevenção, como:

- Usar senhas fortes para garantir que as informações pessoais estejam a salvas, além de atualizá-las com frequência;
- Ativar autenticação de dois fatores é uma segurança extra que impede de criminosos terem acesso ao dados;
- Manter o software e sistemas atualizados, geralmente quando há atualizações os parâmetros de segurança são melhorados;
- Evitar compartilhar informações pessoais online, se compartilhar verifique se realmente é um site legítimo;
- Usar uma VPN é essencial para mascarar o IP e criptografar os dados;
- Fazer backups regulares de dados, a fim de evitar o corrompimento dos dados;
- Utilizar software antivírus/firewall;

Houve dois trabalhos que se diferenciam, o de Pessoa, 2019, onde ele faz referência ao site virustotal.com que faz análises de arquivos ou URLS suspeitas, mesmo que não seja popular è uma boa ferramenta para auxiliar na prevenção, porém o autor não dispensa a utilização de antivírus.Já o outro trabalho que se destacou foi o do Henrique, 2022, o mesmo criou uma cartilha de conscientização de boas práticas de segurança para o enfrentamento de ataques relacionados a *phishing*.

5 CONSIDERAÇÕES FINAIS

Esse estudo teve como objetivo investigar as principais ameaças relacionadas a *phishing* para com o *roubo de identidade* e buscar possíveis soluções de prevenção. Após os resultados obtidos dos trabalhos submetidos a revisão sistemática, pode se dizer que respostas obtidas respondem ao problema de pesquisa que indagava quais medidas poderiam ser adotadas contra esses crimes.

A busca pelo conhecimento sobre o assunto é a primeira medida a ser adotada, ficou claro que a falta do conhecimento de como esses ataques são empregados é o trunfo dos cibercriminosos o que confirma a hipótese levantada anteriormente. logo alguns indivíduos não tem aquela preocupação pelo desconhecido como foi analisado no resultado da amostra estudada. Abrindo brechas para que essas tentativas criminosas continuem a manipular e fazer vítimas constantemente.

A Partir do interesse pelo saber, acreditasse que esse cenário pode trazer mudanças significativas com o cuidado dos dados pessoais no ciberespaço e as prevenções abordadas e discutidas anteriormente venham ser praticadas com êxito no enfrentamento desses crimes cibernéticos.

Conclui que os objetivos deste trabalho foram alcançados de certo modo, mas há lacunas que ainda podem ser investigadas de forma mais minuciosa. Então as sugestões para trabalhos futuros são:

- Se as ferramentas de proteção proposta são realmente eficazes;
- Uma pesquisa do emprego de novas tecnologias emergentes que podem empregadas com *phishing* para fins maliciosos;
- funcionamento de extensões anti-*phishing* na navegação web;
- Tendências futuras no campo das ameaças de *phishing* e *roubo de identidade*;

CYBERSECURITY: Phishing threats related to identity theft

ABSTRACT

This article highlights the importance of cybersecurity due to the growing presence of digital technology in society. It addresses cyber threats related to phishing for identity theft, and explores protection measures against these crimes. The research investigates the main phishing-related cyber threats, such as spear phishing, pharming, vishing and smishing, and how these crimes are executed. The research problem is to find solutions against these crimes. Because the lack of knowledge and good data security practices is identified as a hypothesis for this practice to be successful. The methodology used was a systematic review, where there was an analysis of phishing threats in the selected works. The research involved searching for articles in the Google Scholar and SciELO databases, with specific inclusion and exclusion criteria. Of the 60 articles analyzed, six were selected. A survey revealed that 1,378 participants were involved in research related to identity theft through phishing. The results show that the proposed measures respond to the research problem and emphasize the need for knowledge and the adoption of security measures to combat cybercrime and protect personal data, confirming the hypothesis of the importance of knowledge in preventing these crimes.

Keywords: Cybersecurity.Identity theft.Phishing

REFERÊNCIAS

ALEXANDRA, Raquel C. Neves. **SEGUNDO CICLO DE ESTUDOS CRIMINOLOGIA.** [s.l: s.n.]. Disponível em: <https://repositorio-aberto.up.pt/bitstream/10216/145534/2/592184.pdf>. Acesso em: 05 out. 2023.

AVAST. **O que é vishing e como posso me proteger contra ele?** Disponível em: <https://blog.avast.com/pt-br/stay-protected-vishing-scams>. Acesso em: 13 set. 2023.

DANTAS, Luizmar Peixoto. **A segurança da informação como ferramenta prática de proteção dos dados pessoais e a Lei Geral de Proteção de Dados (LGPD)**. Bc.ufg.br,

2018. Disponível em: <https://repositorio.bc.ufg.br/handle/ri/20926>. Acesso em: 10 set. 2023.

FARIA, T. **FACULDADE DE TECNOLOGIA DE AMERICANA Curso Superior de Tecnologia em Segurança da Informação**. [s.l: s.n.]. Disponível em: <http://ric.cps.sp.gov.br/bitstream/123456789/773/1/20171S_FARIAThiagoStefanini_OD0207.pdf>. Acesso em: 05 out. 2023

HENRIQUE, Pedro ; SILVA, D. UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO. **CIBERSEGURANÇA NO NOVO MUNDO DIGITAL: COMO ALERTAR OS IDOSOS SOBRE OS RISCOS CIBERNÉTICOS DESCENDENTE DO PHISHING NA UTILIZAÇÃO DOS SMARTPHONES.** Disponível em: <https://repositorio.ufersa.edu.br/server/api/core/bitstreams/c5647df0-1a44-460c-88bd-a0721894117f/content>. Acesso em: 05 nov. 2023.

MOURA. BIANCA **O que é smishing? Saiba tudo!** Disponível em: <https://www.psafe.com/blog/o-que-e-smishing-saiba-tudo/>. Acesso em: 13 set. 2023.

OLIVEIRA, Bruno, **Golpes bancários quase dobram em um ano, aponta levantamento**, CNN Brasil, disponível em: <https://www.cnnbrasil.com.br/economia/golpes-bancarios-quase-dobram-em-um-ano-aponta-levantamento/>. acesso em: 10 set. 2023.

O que é spear phishing? | IBM. Disponível em: <https://www.ibm.com/br-pt/topics/spear-phishing>. Acesso em: 10 set. 2023.

PAULO, S. UNIVERSIDADE PRESBITERIANA MACKENZIE ALESSANDRA PIVOVAR DE CAMARGO ROSA **FURTO DE IDENTIDADE DIGITAL**. [s.l: s.n.]. Disponível em: <https://adelpha-api.mackenzie.br/server/api/core/bitstreams/e42d48f2-1c73-4f97-a274-957ee57b816e/content>. Acesso em: 10 set. 2023.

PESSOA, M.; QUEIROZ, D.; AMERICANA, S. FACULDADE DE TECNOLOGIA DE AMERICANA Curso Superior de Tecnologia em Segurança da Informação **PHISHING E REDES SOCIAIS: UM ESTUDO DE CASO**. [s.l: s.n.]. Disponível em: <http://ric.cps.sp.gov.br/bitstream/123456789/3780/1/20191S_QUEIROZMarianaPessoade_OD0669.pdf>. Acesso em: 10 set. 2023.

PINHEIRO, Patricia P. **Segurança Digital - Proteção de Dados nas Empresas.** 1ª edição. São Paulo, SP: Grupo GEN, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 09 set. 2023.

RANNYSON, Francisco C. Silva. INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ CAMPUS PEDRO II **ANÁLISE PRÁTICA E MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NA ERA DIGITAL** . Disponível em: <http://bia.ifpi.edu.br:8080/jspui/bitstream/123456789/1781/1/2023_tcc_frcsilva.pdf>. Acesso em: 05 out. 2023.

RODRIGUES, Horácio Wanderlei; BECHARA, Gabriela Natacha; GRUBBA, Leilane Serratine. **Era digital e controle da informação.** Revista Em Tempo, v. 20, n. 1, 2020.

SERASA EXPERIAN. **Roubo de identidade preocupa 8 em cada 10 brasileiros; saiba como ocorre este tipo de fraude.** Disponível em: <https://www.serasaexperian.com.br/conteudos/prevencao-a-fraude/como-se-proteger-contra-roubo-de-identidade/#:~:text=Estat%C3%ADsticas%20de%20roubo%20de%20identidade,Noruega%20e%20%C3%81frica%20do%20Sul.>. Acesso em: 16 set. 2023.

SILVA, Yuri P. UNIVERSIDADE FEDERAL DO CEARÁ CAMPUS QUIXADÁ. **ENGENHARIA SOCIAL COMO AMEAÇA AO SETOR BANCÁRIO: USO DO PHISHING PARA COLETAR INFORMAÇÕES DOS CORRENTISTAS E A NECESSIDADE DE ESTRATÉGIAS DE SEGURANÇA**. QUIXADÁ. [s.l: s.n.]. Disponível em: <https://repositorio.ufc.br/bitstream/riufc/49703/1/2019_tcc_ipsilva.pdf>. Acesso em: 05 out. 2023.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. **Redes de computadores.** 6. ed. São Paulo: Grupo A, 2021. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 09 set. 2023.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 6ª edição. São Paulo, SP: Editora Saraiva, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596946/. Acesso em: 05 out. 2023

KASPERSKY. **O que é pharming e como evitá-lo?** Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/pharming>. Acesso em: 11 set. 2023.