PHISHING E SEUS RISCOS: UM ESTUDO SOBRE ROUBO DE DADOS EM REDES SOCIAIS NA POPULAÇÃO PERNAMBUCANA

PHISHING AND ITS RISKS: A STUDY ON DATA THEFT ON SOCIAL NETWORKS IN PERNAMBUCAN POPULATION

Guilherme Lins Ferreira[1]
Remo Alves Ferreira[2]

RESUMO

Este artigo propõe investigar o impacto do phishing no roubo de dados em redes sociais no estado de Pernambuco, com foco na atuação de cibercriminosos e os prejuízos resultantes para diversos estratos sociais. Inicialmente, realizaremos uma revisão bibliográfica abrangente sobre o tema de crimes cibernéticos, com destaque para o phishing, a fim de entender as diversas abordagens e perspectivas sobre esse assunto. Em seguida, conduzimos pesquisas em bases de dados online nacionais para identificarmos artigos científicos, monografias, teses e dissertações que abordam o phishing em redes sociais, aprofundando nossa compreensão sobre o tema. Além disso, analisaremos dados oficiais das autoridades competentes, nas esferas federal, estadual e municipal, a fim de coletar informações sobre a ocorrência desses crimes em Pernambuco. Posteriormente, apresentaremos os resultados encontrados, destacando as frequências, tipos, graus de prejuízos e graus de ameaças mais comuns enfrentados pelos pernambucanos, enfatizando o impacto do phishing nas redes sociais.

Palavras-Chave: Redes sociais, Crimes cibernéticos, Phishing, Cibercriminosos.

ABSTRACT

This article aims to investigate the impact of phishing on data theft on social networks in the state of Pernambuco, focusing on the actions of cybercriminals and the resulting losses for different social strata. Initially, we will carry out a comprehensive literature review on the topic of cybercrime, with emphasis on phishing, in order to understand the different approaches and perspectives on this subject. We will then conduct research in national online databases to identify scientific articles, monographs, theses and dissertations that address phishing on social networks, deepening our understanding of the topic. Furthermore, we will analyze official data from the competent authorities, at the federal, state and municipal levels, in order to collect information on the occurrence of these crimes in Pernambuco. Later, we will present the results found, highlighting the frequencies, types, degrees of damage and most common degrees of threats faced by people from Pernambuco, emphasizing the impact of phishing on social networks.

Keywords: Social networks, Cybercrime, Phishing, Cybercriminals.

[1] Acadêmico do Curso de Bacharelado em sistemas de informações da Associação Vitoriense de Educação, Ciência e Cultura, Centro Universitário FACOL - UNIFACOL; guilhermel.ferreira@unifacol.edu.br

[2] Professor Mestre e Orientador do Curso Bacharelado em Sistemas de Informações da Associação Vitoriense de Educação, Ciência e Cultura, centro Universitário FACOL - UNIFACOL; remo.ferreira@unifacol.edu.br

1 INTRODUÇÃO

As redes sociais se tornaram uma parte integral da vida de muitas pessoas em todo o mundo, transformando a maneira como nos relacionamos e compartilhamos informações, como destacado por Smith (2018). Elas proporcionam uma dinâmica social caracterizada por interações rápidas e a disseminação instantânea de notícias, conforme observado por Marinho (2017) e Recuero (2011). No entanto, à medida que essas plataformas desempenham um papel cada vez mais central em nossas vidas, também surgem ameaças significativas à segurança cibernética, sendo o phishing um dos principais vetores de ataque.

O phishing, segundo Moura (2020), é uma técnica amplamente utilizada por cibercriminosos para obter informações pessoais e sensíveis, como números de telefone, endereços, dados de cartão de crédito e senhas. Ainda segundo o autor, à medida que os usuários se tornam mais ativos nas redes sociais, eles se tornam alvos em potencial para esses ataques, que podem resultar em roubo de identidade, fraudes financeiras e invasões de privacidade.

De acordo com o relatório do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br), em 2021 houve um aumento significativo nos crimes cibernéticos, com um aumento de 7% em relação a 2020. O phishing, de acordo este relatório, foi uma das táticas mais prevalentes, com 847.376 reclamações de crimes pela internet e um prejuízo total de quase 7 bilhões de dólares, afetando um em cada 467 usuários, representando uma taxa de ataque de 0.4%.

No contexto brasileiro, a ausência de regulamentação específica para crimes cibernéticos gera uma sensação de impunidade no ambiente digital, conforme ressaltado por Ferreira (2012). Embora leis como a Lei Carolina Dieckmann e o Marco Civil da Internet tenham sido introduzidas para lidar com essas questões, elas ainda apresentam limitações. É crucial, segundo Ferreira (2012), um esforço contínuo para atualizar e aprimorar a legislação, garantindo uma abordagem eficaz na proteção dos usuários e no combate aos crimes digitais.

Pernambuco acompanha a tendência global de crescimento no uso das redes sociais, conforme observado por Marinho, Jhemisson e Moura (2017). Nesse contexto, é essencial que os usuários pernambucanos adotem medidas de proteção e compreendam as boas práticas de cibersegurança. Isso inclui o uso de senhas fortes e exclusivas, a implementação da autenticação em dois fatores e a vigilância contra táticas de phishing

e engenharia social empregadas por cibercriminosos, conforme salientado por Moura (2020). Senhas fortes devem mesclar números, letras maiúsculas, letras minúsculas e caracteres especiais para garantir a segurança do usuário. A autenticação em dois fatores, por sua vez, acrescenta uma camada adicional de segurança ao exigir um segundo fator de confirmação.

Quando exploramos a problemática do phishing e seus riscos nas redes sociais, nos deparamos com a seguinte pergunta: quais medidas de segurança são as mais eficazes para os usuários se protegerem contra ataques de phishing em ambientes de redes sociais?

Com base nessa problemática, foi formulada a seguinte hipótese: o entendimento dos riscos associados a sites maliciosos capacita as pessoas a se prepararem de forma mais eficiente, reduzindo assim a probabilidade de se tornarem vítimas de tais sites. Portanto, o conhecimento desempenha um papel valioso na prevenção de problemas em sites maliciosos.

Este estudo tem como objetivo principal fornecer aos usuários orientações para aumentar a segurança de suas redes sociais por meio de um guia de boas práticas para comportamento na internet. Já aos objetivos específicos temos: mapear os casos de Phishing mais frequentes; entender os prejuízos que o Phishing pode causar a um usuário; desenvolver resolução de proteção para o Pishing.

2 A IMPORTÂNCIA DA COMUNICAÇÃO NA ERA DA INTERNET

Com o passar do tempo, conforme Fraga (2022) não só a linguagem passou por processos de evolução como também os meios de comunicação. Quem, há 50 anos atrás, diria que seria possível se comunicar com alguém do outro lado do mundo em tempo real? Hoje em dia, a chegada da internet revolucionou os meios de comunicação. Sendo assim, fica pré-estabelecida a importância crucial da comunicação para a sociedade, como destaca Fraga (2022).

A comunicação interpessoal, como informa Dante (2006), ocorre quando as pessoas sentem a necessidade de se informar, serem informadas ou buscarem conhecimento, utilizando diferentes formas de linguagem, como a fala, gestos e escrita. Além disso, Dante (2006) cita que se utilizam de meios variados, como a voz, o telefone, expressões corporais, cartas e livros, para se conectar e interagir com outras pessoas, promovendo a troca de informações e estabelecendo relacionamentos significativos.

A internet foi uma das responsáveis pela gigantesca evolução dos meios de comunicação, Fraga (2022) citava que ela possibilita até os dias de hoje a comunicação praticamente instantânea entre pessoas de países distintos. Sendo uma ferramenta totalmente popular atualmente, mas não se restringindo às camadas populares e sendo utilizada até mesmo pelas camadas mais altas da sociedade, como governos e vários órgãos internacionais, segundo Fraga (2022).

O surgimento da internet se deu nos Estados Unidos, por volta de 1969, inicialmente chamada de Arpanet, servia para interligar laboratórios de pesquisa. Por estar vivendo no auge da Guerra Fria, os Estados Unidos detinham o controle, ficando o Departamento de Defesa norte-americano responsável pelo controle de tal ferramenta, que era utilizada para a comunicação entre militares e cientistas, conforme Souza (2015). Foi então a partir de 1982 que o uso da Arpanet através do meio acadêmico, antes restrito aos Estados Unidos, foi se expandindo a outros países, como Holanda, Dinamarca e Suécia, a partir desse momento passou a ser chamada pelo nome de internet. Em 1987 a internet foi utilizada pela primeira vez para o uso comercial. (Souza et al, 2015).

A partir de 1992 foram surgindo novas empresas provedoras de acesso à internet, nesse mesmo ano Meneses (2022), fala que o Laboratório Europeu de Física de Partículas (Cern) criou o World Wide Web, o famoso “www” antes dos links, que significa Rede Mundial de Computadores, hoje em dia em alguns sites, não se faz mais necessário o seu uso. Meneses (2022) fala que atualmente a internet já está quase que totalmente difundida, sendo raras as exceções, todos os países a utilizam, possuindo mais de 3,9 bilhões de usuários que acessam diariamente a internet, equivalente a 51% da população mundial.

2.1 **REDES SOCIAIS COMO INSTRUMENTO DE COMUNICAÇÃO ENTRE PESSOAS**

Não é novidade para ninguém que a internet revolucionou o mundo em muitos aspectos. Certamente não seria diferente para os meios de comunicação e entretenimento. Foi nesse sentido, que a partir dos anos 2000, conforme Recuero (2011) com a popularização da internet de modo mais expressivo, foram disseminadas as redes sociais. Os primeiros serviços surgiram em 1969, com o intuito de socializar dados. (Recuero et al 2011).

No ano de 1985, como ressaltado por Recuero (2011) foi lançado o América Online, uma plataforma que oferece ferramentas para que as pessoas pudessem criar

perfis virtuais, descrever-se e formar comunidades para compartilhar informações e participar de discussões sobre uma ampla variedade de tópicos. Embora já tivéssemos visto avanços anteriores nessa área, foi durante a década de 1990 que testemunhamos um crescimento exponencial dos recursos de comunicação. Em 1994, um marco importante ocorreu com o surgimento das redes sociais, sendo o lançamento do GeoCities um dos primeiros sinais dessa revolução, conforme discutido por Recuero (2011).

Maximo (2014) dizia que o conceito desse serviço era fornecer recursos para que as pessoas pudessem criar suas próprias páginas na web, sendo categorizadas de acordo com a sua localização. Ele chegou a ter 38 milhões de usuários, foi adquirido pela Yahoo! cinco anos depois e foi fechado em 2009. Outros dois serviços foram anunciados em 1995, e segundo Maximo (2014) ambos com características mais claras de um foco voltado para a conectividade entre pessoas.

O homem é um ser social, é por isso que viramos praticamente dependente das redes sociais. Hoje não precisamos exatamente estar em algum lugar para se comunicar com outras pessoas, podemos fazer isso apenas pegando o celular e mandando mensagens por elas. O Brasil é o segundo no ranking mundial no acesso a redes sociais, necessitamos da comunicação a todo momento tanto para a parte acadêmica, tanto para a parte profissional, ou lazer mundial. (Correa et al, 2014).

Devido a comunicação muito interativa, Maximo (2014) reforça que faz com que as informações e conhecimentos se compartilhem mais rapidamente. No entanto, a rede social também tem seus contras, como por exemplo, a comunicação das pessoas na realidade está deixando de ser tão interessante para muitos. Segundo Maximo (2014) as pessoas preferem ficar em casa a sair com seus amigos, ficam mais ligados a tela dos smartphones do que com pessoas de verdade mundial.

Essa tal forma de comunicação tem afetado tanto as pessoas que as horas de acesso por mês de alguns anos para cá só vão aumentando, sendo em média 279 horas por mês. E Correa (2014) relata que a maior parte desse tempo é dedicada às redes sociais mais utilizadas, como o Instagram e o Facebook mundial. Nesse contexto, observa-se uma mudança significativa nos hábitos de consumo de mídia digital, indicando uma crescente dependência dessas plataformas para a interação social (Smith, 2018). Além disso, estudos recentes destacam a influência das redes sociais na construção da identidade online e na formação de relações interpessoais (Jones et al 2013).

O uso das redes sociais nos dias de hoje é quase totalmente indispensável, mais de 122 milhões ou 58% da população brasileira é usuário ativo, segundo o relatório do Digital in 2017, feito pela “We Are Social” em parceria com Hootsuite. Em um gráfico da Social Media Trends 2018, mostra o uso de várias redes sociais mais usadas no Brasil, com destaque para os 4 primeiros: Instagram, com 47,1% (cerca de 51 milhões de brasileiros); Facebook, com 29,6%; Youtube, com 8,3%; Twitter, com 7,7%.

Agora falando sobre as redes sociais mais utilizadas, conforme Correa (2014) o Facebook (25%), Instagram (44%) e Whatsapp (29%), outras (1%). O mais interessante fato observado é que as redes sociais como informado por Correa (2014), estão perdendo um pouco do seu viés de entretenimento e passando a ser utilizadas para a promoção de produtos e marketing.

3 CRIMES DA INFORMÁTICA

Segundo Silvestre (2003) Crimes informáticos são todos os tipos de delitos criminosos em que se utiliza um computador ou uma rede de computadores como instrumento ou base de ataques. Ataques esses que possam atingir redes de computadores, internet ou qualquer outro sistema informático.

No contexto de Ferreira (2012), crimes cibernéticos são cometidos por indivíduos que possuem familiaridade com o uso regular de computadores em seu trabalho, mas isso não exclui a possibilidade de serem cometidos por pessoas com menos conhecimento, que apenas se aventuram na área. Esses criminosos eletrônicos, ou cyber delinquentes, já foram batizados pela comunidade cibernética de hackers ou crackers.

Silvestre (2003) relata que os crimes cibernéticos ocorrem de várias maneiras, incluindo a propagação de vírus e malware por meio de e-mails infectados, a fim de roubar informações sensíveis. Os criminosos também utilizam essas informações de forma indevida para realizar atividades ilegais, como distribuição de conteúdo pornográfico não autorizado, fraudes financeiras e violação de direitos autorais. Além disso, eles invadem sites para disseminar mensagens difamatórias e prejudicar a reputação de pessoas, empresas e instituições. É importante adotar medidas de segurança online para proteger-se contra esses crimes, como uso de antivírus, boas práticas de segurança cibernética e educação sobre os riscos da tecnologia digital. (Silvestre et al, 2003).

Os crimes cibernéticos são fenômenos que surgiram no fim do século XX e de acordo com Ferreira (2012), eles englobam diversas iniciativas ilegais realizadas por meio de computadores, estejam eles de certo modo vinculados a algo e em alguns casos sem precisar necessariamente se conectar. Essas atividades criminosas, ressaltadas por Ferreira (2012), vão desde a manipulação de caixas eletrônicos até a pirataria de programas de computador, incluindo também abusos nos sistemas de telecomunicação.

Essas ações evidenciam uma fragilidade que os responsáveis por esses sistemas não haviam antecipado, necessitando de uma proteção imediata. Isso requer não apenas o desenvolvimento de novas estratégias de segurança para sua implementação, mas também a criação de métodos atualizados de controle e punição. (Nunes et al, 2020).

Silvestre (2003) diz que os crimes cibernéticos possuem duas características importantes. A primeira é a sua natureza transnacional, o que dificulta as investigações e a obtenção de provas contra os suspeitos, uma vez que podem agir de diferentes países. A segunda característica está relacionada ao aumento do uso de computadores pessoais. Isso permite que qualquer pessoa, em qualquer lugar do mundo, possa cometer esses crimes contra qualquer indivíduo, sem precisar sair de casa.

A diferença é que como são aplicados a partir da internet, os responsáveis podem se utilizar de redes públicas, privadas ou domésticas, assim podem fazer tudo isso em anonimato. E é por isso que precisamos ter atenção e conhecer os crimes mais comuns. Como por exemplo: Difamar, que se trata de expor fatos ofensivos de alguém; injuria, que é ofender alguém a fim de sujar sua dignidade; Roubo de dados, que se trata de obter vantagens ilícitas alheias, induzindo ou mantendo alguém em erro, ou qualquer outro meio fraudulento. (FRAGA, C. 2022). Plagiar trata-se de uma cópia de informações veiculadas por terceiros sem a indicação da fonte sabendo disso é bom ficar atento e investir na segurança de seus dados para não ser vítima ou autor de nenhum deles. Isso pode trazer inúmeros transtornos e dores de cabeça. (Nunes et al, 2020).

Conforme Meneses (2022), todo software atualizado é de extrema importância para os sistemas operacionais e para as suítes de segurança na Internet. Os hackers provavelmente usarão explorações conhecidas no software para obter acesso ao seu sistema. A Meneses (2022) sempre diz que a aplicação de patches para essas explorações reduz significativamente a probabilidade de você se tornar uma vítima. Gerencie as suas configurações de mídias sociais para manter a maior parte das suas informações pessoais e privadas bloqueadas.

3.1 ROUBO DE DADOS NA REGIÃO PERNAMBUCANA

Segundo Severino (2023), o roubo de dados é um crime digital que tem se tornado cada vez mais frequente na região Pernambucana e preocupante na era da informação digitalizada. Este crime envolve a obtenção não autorizada e o subsequente uso indevido de informações pessoais, financeiras ou confidenciais de indivíduos ou organizações por parte de hackers, criminosos cibernéticos e até mesmo empresas mal-intencionadas. Severino (2023) fala que o objetivo principal por trás do roubo de dados geralmente é o ganho financeiro, o acesso a segredos comerciais ou industriais, a violação da privacidade das vítimas ou mesmo a divulgação de informações sensíveis para prejudicar a reputação das partes envolvidas.

Em Pernambuco no ano de 2022 diante as informações do g1.globo.com foi constado um aumento gigantesco em relação a roubo de dados de cerca de 237% através de crimes cibernéticos no estado Pernambucano, sendo utilizado em números mais específicos, são cerca de 280 ocorrências no ano de 2021 e no ano seguinte teve um aumento três vezes mais que o ano anterior, com cerca de 944 ocorrências, cerca de 664 ataques a mais que o ano de 2021. Foi passado informações e dicas para essas pessoas que sofreram os ataques e para pessoas também se prevenirem, usando palavras como “É essencial ter cuidado com as informações no telefone, verificar sua veracidade, e nunca pagar antecipadamente por serviços ou empregos. Fique sempre alerta a possíveis golpes.”, palavras ditas por Meneses (2022).

Com base em informações recorrentes através do G1, Globo.com, mostrando no ano de 2022, com o gigantesco aumento de roubos de dados no ano em questão. Diante todos esses roubos de dados existiu uma quadrilha que trabalhava roubando dados em redes sociais da população, que inicialmente eles agiam no Rio Grande do Norte, Natal. Com o passar do tempo eles foram mudando de estado, percebendo que talvez fossem pegos ou tinham dificuldades em fazer seus atos criminosos acabaram se mudando para outro estado, assim tendo seu fim na capital Pernambucana.

Essa quadrilha trabalhava fazendo fraudes no seguinte modo, roubam dados de pessoas através do phishing, pegando dados pessoais como e-mail, senhas dos indivíduos, assim utilizando disso para ter acesso ao RG, CPF, número de telefone, redes sociais contas em sites de compras e muitos outros, a quadrilha atuava utilizando cartões roubados de pessoas, junto com identificações de outros usuários e faziam os pedidos e compras para ser pegos em lojas, foram pegos após uma das vítimas sabendo

a localização da compra e em qual loja seria através do e-mail, assim a contatou a polícia sobre a possível localização, assim os agentes atuaram e pegaram dois homens em flagrante assim que fizeram a retirada da loja, foram pegos com vários eletrônicos, joias, além de cédulas falsas de identidade e máquina de plastificar documentos.

4 METODOLOGIA

Este estudo empregou uma abordagem qualitativa e quantitativa para investigar o fenômeno dos ataques de Phishing, com foco no roubo de dados em redes sociais na população de Pernambuco.

Para atingir os objetivos, será realizada uma pesquisa bibliográfica em fontes acadêmicas, publicações, relatórios e artigos relacionados a crimes cibernéticos, segurança digital e redes sociais. As bases de dados pesquisadas serão: Cert.br, Scielo, Google Acadêmico e BDTD (Biblioteca Digital Brasileira de Teses e Dissertações), onde serão consultadas para encontrar literatura relevante.

Como critérios de inclusão, temos os artigos em língua portuguesa que tratam de crimes cibernéticos, em especial no estado de Pernambuco. Como critérios de exclusão, temos aqueles artigos em línguas estrangeiras que não apresentam relevância significativa para esta pesquisa.

O estudo pode apresentar algumas limitações, como a possibilidade de subnotificação de casos de crimes cibernéticos, uma vez que muitas vítimas podem não relatar incidentes por medo ou falta de conhecimento. Além disso, a amostra pode não representar completamente a diversidade da população de Pernambuco.

Espera-se que este estudo contribua para uma compreensão mais profunda dos crimes de roubo de dados em redes sociais na população pernambucana. Os resultados podem ser úteis para a conscientização pública, políticas de segurança digital e ações preventivas em nível regional. Esta metodologia servirá como base para conduzir a pesquisa de forma sistemática, buscando obter insights e dados relevantes sobre o tema proposto. Qualquer ajuste adicional necessário pode ser feito durante a condução da pesquisa para garantir a qualidade e a eficácia do estudo.

5 PHISHING E SEUS RISCOS EM REDES SOCIAIS.

As redes sociais desempenham um papel fundamental em nossas vidas online, permitindo-nos compartilhar momentos, interagir com amigos e até mesmo estabelecer

novas conexões. No entanto, essa plataforma de interação social não está imune a ataques, especialmente o phishing. Neste capítulo, exploraremos os tipos de phishing comuns nas redes sociais e oferecemos um guia prático para manter sua segurança e privacidade.

Hoje, o crime cibernético, como o roubo de dados em redes sociais, não parece mais distante. Embora Fraga (2022) diz que possa parecer que estamos mais preparados para lidar com essas ameaças, os criminosos também estão se tornando mais habilidosos, usando táticas cada vez mais sofisticadas. Moura e Bomfim (2020), relatam que o roubo de dados na internet é uma forma de crime cibernético que ocorre em computadores, redes e dispositivos conectados. Antigamente, era algo distante, mas agora é uma ocorrência comum em nossas vidas cotidianas.

De acordo com Khonji, Iraqi & Jones (2013), o phishing é uma ameaça cibernética comum e enganosa, onde os atacantes criam mensagens falsas que parecem ser legítimas, muitas vezes imitando empresas ou instituições confiáveis, com o objetivo de induzir as vítimas a revelar informações sensíveis, como senhas e informações financeiras e envolvem a criação de mensagens de e-mail, mensagens de texto ou outras comunicações eletrônicas cuidadosamente projetadas para parecerem autênticas. Segundo Khonji (2013) Os atacantes frequentemente utilizam logotipos e marcas registradas conhecidas para tornar suas mensagens mais convincentes, fazendo com que as vítimas acreditem que estão interagindo com fontes confiáveis. Esses ataques exploram a vulnerabilidade humana e geralmente usam táticas psicológicas para enganar as pessoas e fazê-las agir rapidamente.

O phishing tradicional é uma tática de cibercrime na qual os criminosos enviam mensagens de e-mail em massa ou criam sites falsos que imitam entidades legítimas, com o objetivo de enganar as vítimas e induzi-las a revelar informações confidenciais, como senhas, informações bancárias e outras informações pessoais. Os quatro principais tipos de phishing são: Whaling: É uma forma de spear phishing que tem como alvo executivos de alto escalão e profissionais renomados. Os atacantes buscam informações privilegiadas ou dados corporativos confidenciais; Pharming: Envolve a manipulação maliciosa do sistema DNS (Domain Name System) para redirecionar o tráfego da web para sites falsos que se assemelham a sites legítimos. As vítimas são direcionadas a inserir informações confidenciais nesses sites; Vishing: É uma variação do phishing que utiliza chamadas telefônicas. Os criminosos solicitam informações pessoais por telefone, muitas vezes ameaçando consequências caso as vítimas não cooperem;

Smishing: Semelhante ao phishing tradicional, é realizado por meio de mensagens de texto. As vítimas recebem mensagens falsas que solicitam informações pessoais.

Em uma sociedade cada vez mais conectada a internet, este estudo identifica que as redes sociais desempenham um papel fundamental em nossas vidas. No entanto, com o aumento da presença online, o phishing nas redes sociais também está em ascensão. Geraldes (2017) afirma que criminosos desenvolveram técnicas cada vez mais sofisticadas para sequestrar informações pessoais e financeiras. Que variam de várias maneiras como por exemplo: Mensagens falsas são um engano pessoal comum: criminosos se passam por amigos ou conhecidos, buscando informações pessoais. Eles exploram a confiança que você tem em seus contatos para obter dados sensíveis, então é vital estar atento e examinar detalhadamente essas mensagens. Pedidos de senhas, dados pessoais ou ofertas de negócios suspeitas são alguns exemplos comuns; Links suspeitos também são uma cilada cibernética frequente. Criminosos compartilham URLs que parecem legítimos, mas levam a sites maliciosos. Relatos também ditos por Geraldes (2017), fala que esses cibercriminosos usam técnicas persuasivas, como mensagens convincentes ou exploram eventos atuais para aumentar a credibilidade desses links; Concursos ou promoções falsas nas redes sociais são outro perigo. Eles pedem informações pessoais em troca de prêmios fictícios. Indícios incluem requisitos para dados confidenciais, falta de informações claras sobre a empresa e prêmios excessivamente generosos; perfis falsos nas redes sociais são criados por criminosos para se passarem por pessoas reais. Eles usam identidades falsas e tentam infiltrar-se em suas conexões. Identificar perfis falsos requer atenção: verificar fotos de perfil, avaliar atividades recentes e analisar históricos e listas de amigos podem revelar padrões suspeitos.

Nos depararmos com um ambiente digital cada vez mais integrado à nossa vida cotidiana, é crucial reconhecer as crescentes ameaças, como o phishing, que evoluem rapidamente no espaço das redes sociais. Desde mensagens falsas até perfis fraudulentos, o mundo online está repleto de artimanhas para obter nossos dados pessoais. Este capítulo explorou os tipos comuns de phishing nas redes sociais, oferecendo insights e estratégias para proteger nossas informações. A vigilância constante, a verificação cuidadosa e o conhecimento das táticas empregadas pelos criminosos são armas poderosas na defesa de nossa segurança e privacidade online.

6 RECOMENDAÇÕES E BOAS PRÁTICAS CONTRA PHISHING

Após uma extensa investigação, ficou claro que o phishing, apesar de explorar falhas nas redes sociais dos usuários, pode ser prevenido e combatido. Serão fornecidas recomendações de boas práticas para proteger-se contra esses ataques, visando trazer uma sensação de segurança e eliminar preocupações sobre possíveis impactos causados por hackers que utilizam o phishing para ações maliciosas.

Os ataques de phishing evoluíram ao longo dos anos, diversificando-se em vários tipos enganosos, cada um projetado para atingir alvos específicos de maneira cada vez mais sofisticada. E conforme Bruna (2021) relata que embora todos os tipos de phishing compartilhem o objetivo comum de explorar a confiança e a falta de conhecimento das vítimas, suas abordagens variam de acordo com o método, o público-alvo e a finalidade do ataque. A compreensão desses diferentes tipos de phishing e como preveni-los é essencial para que as pessoas possam se defender e proteger suas redes sociais adequadamente contra essas ameaças.

A prevenção do phishing depende em grande parte da conscientização e educação das pessoas, com isso Severino (2023) diz que os usuários devem ser treinados para identificar sinais de phishing, como erros gramaticais, endereços de e-mail suspeitos e solicitações de informações confidenciais. Além disso, é essencial verificar a autenticidade dos sites antes de inserir informações pessoais.

De acordo com Bruna (2021) pressão por ações imediatas em mensagens via WhatsApp, Instagram ou até mesmo Facebook, quando alguém se passa por outra pessoa (muitas vezes alguém que seja conhecido) e solicita acesso a um link ou faz propostas suspeitas, pode ser evitada com medidas simples. Bruna (2021) também fala que, em primeiro lugar, evite continuar a conversa e exija autenticação para garantir a identidade da pessoa. Além disso, é fundamental não clicar em nenhum link enviado por essa pessoa. Agir com cautela nestas situações pode prevenir potenciais problemas e proteger suas informações pessoais.

E interessante as medidas adotadas por Khonji e Iraqi (2013) de boas maneiras para proteger dos problemas como por exemplo, as falsas mensagens, a estratégia seria verifique a origem das mensagens antes de responder e proteja suas informações sensíveis e incremente a segurança com autenticação em duas etapas, também implementar ferramentas de segurança, como filtros de e-mail e sistemas de detecção de ameaças, para ajudar a identificar e bloquear mensagens de phishing. A conscientização, a educação e a implementação de medidas de segurança são fundamentais para proteger

indivíduos e organizações contra ataques de phishing, que continuam sendo uma ameaça persistente no cenário da cibersegurança. (SEVERINO et al, 2023)

Ao realizarmos a atualização dos nossos aparelhos e softwares, que de acordo com Prado (2003), frequentemente nos deparamos com a possibilidade de comprometer nossa privacidade e segurança. Portanto Geraldes (2017) diz que é crucial adotarmos precauções simples para resguardar-nos dos delitos cibernéticos. Uma das medidas fundamentais consiste em utilizar uma suíte abrangente de segurança para a rede mundial, proporcionando-nos proteção contra vírus e outras ameaças virtuais. Dessa maneira, conforme Prado (2003) asseguramos uma experiência online mais segura e resguardada contra os riscos presentes na internet.

Uma medida eficaz para garantir a segurança dos seus dados é utilizar uma senha de criptografia robusta. Além disso, em conformidade Nunes (2020) recomenda-se fazer uso de uma VPN (Rede Privada Virtual) e de uma Proxy, que ajudam a criptografar todo o tráfego de dados que sai dos seus dispositivos até chegar ao seu destino. Segundo Geraldes (2017), mesmo que um hacker consiga acessar a sua linha de comunicação, não será capaz de interceptar informações, uma vez que todo o tráfego está protegido por criptografia. Essas medidas adicionais de segurança, de acordo com Nunes (2020), proporcionam uma camada adicional de proteção para a sua privacidade e garantem que suas informações permaneçam confidenciais durante a transmissão.

De fato, o phishing é uma grande ameaça nas redes sociais, e por conta disso aqui vai também mais algumas indicações de como proteger suas redes sociais contra o phising, por exemplo: Verificar a origem das mensagens, sempre bom confirmar a identidade do remetente antes de responder ou clicar em links e sempre desconfie de mensagens não solicitadas que solicitem informações pessoais. A prevenção do phishing depende em grande parte da conscientização e educação das pessoas. Com isso já pode seguir com os links suspeitos que geralmente são identificados pelo endereço do site, os usuários devem ser treinados para identificar sinais de phishing, como erros gramaticais nos links, erros ortográficos além disso, é essencial verificar a autenticidade dos sites antes de inserir informações pessoais e sempre ficar atento aos detalhes simples como verificar a segurança do site com um simples cadeado ao lado do endereçamento da url.

Com esse estudo, é possível identificar que, mesmo com precauções tomadas, até mesmo o simples ato de se conectar a uma rede Wi-Fi pode ser um ponto vulnerável.

Evite, sempre que possível, redes públicas suspeitas, especialmente aquelas de acesso aberto em locais públicos. É fundamental estar ciente das limitações e tomar medidas para evitar possíveis riscos. Manter suas senhas de redes sociais seguras é crucial para proteger suas informações. Uma boa prática é criar senhas robustas, combinando letras maiúsculas e minúsculas, números e caracteres especiais (! @ # $ %), garantindo uma senha mais forte e segura.

E como um meio de segurança muito importante, como descrito por Mello (2017) diz como autenticador de dois fatores (2FA), ele é um método de segurança que requer além da senha um segundo fator de verificação para acessar contas online. Esse segundo fator pode ser um código enviado por mensagem ou gerado por um aplicativo. Ele adiciona uma camada extra de proteção, dificultando o acesso não autorizado à conta, mesmo se a senha for comprometida. De Acordo com Mello (2017), uma forma mais direta funcionaria da seguinte maneira: primeiro fator seria a senha, e o segundo fator seria após inserir a senha, ser solicitado um segundo método de autenticação como um aplicativo de autenticador, uma impressão digital ou até mesmo um token físico, algo que sirva realmente como uma prova adicional que a conta é sua.

Manter-se atualizado é crucial para a segurança e o crescimento pessoal, mesmo em ambientes digitais, é fundamental acompanhar as atualizações, termos e medidas de segurança em suas redes sociais e sempre evitar compartilhar informações sensíveis como as ditas anteriormente por Khonji (2013). Entender os variados tipos de phishing e suas estratégias é essencial. Investir em educação contínua e conhecimento constante é valioso para todos. Além de que vale reforçar a importância de uma limitação de dados pessoais, como restringir informações nas redes sociais. Conhecer profundamente suas redes sociais e como protegê-las é imprescindível para garantir sua segurança online.

Esse estudo mostra que caso tenha sido vítima de um caso suspeito em que suas credenciais foram comprometidas, agir rapidamente é crucial. Comece mudando imediatamente suas senhas e fique atento a qualquer atividade suspeita em suas contas. É importante também informar seus contatos sobre a possibilidade de sua conta ter sido comprometida, mantendo-os alertas quanto a possíveis mensagens ou atividades suspeitas provenientes de sua conta. Além disso, notifique as autoridades competentes ou a plataforma em uso sobre a situação para tomar as medidas adequadas e ajudar na resolução do problema. Essas ações imediatas podem ajudar a conter danos e impedir o acesso não autorizado às suas informações.

Por fim, devemos destacar que manter a segurança nas redes sociais é fundamental para preservar sua identidade digital e proteger informações pessoais. Adotando essas diretrizes e práticas, você estará mais bem preparado para desfrutar de suas redes sociais sem colocar em risco sua segurança. Mantenha-se vigilante, proteja-se e desfrute de uma experiência online segura. Suas redes sociais podem ser uma fonte de alegria e conexão, desde que você esteja ciente dos riscos e saiba como se proteger. O conhecimento e as práticas de segurança são as melhores armas contra o phishing nas redes sociais.

7 CONSIDERAÇÕES FINAIS

Neste estudo, exploramos a crescente ameaça dos crimes cibernéticos, com foco no roubo de dados em redes sociais, na região de Pernambuco. O crescente uso de redes sociais e a digitalização da informação têm criado um ambiente propício para o aumento do roubo de dados e ataques de phishing. Os criminosos cibernéticos estão se tornando mais sofisticados em suas táticas, tornando essencial que os usuários adotem medidas de segurança e compreendam as boas práticas de cibersegurança.

A pesquisa destacou que o phishing é uma das táticas mais comuns usadas pelos criminosos para obter informações pessoais e sensíveis. Isso pode levar a consequências graves, como roubo de identidade, fraudes financeiras e invasões de privacidade. A conscientização e a educação dos usuários desempenham um papel crucial na prevenção desses ataques. É importante que as pessoas saibam como identificar sinais de phishing e adotar medidas de segurança, como senhas fortes e autenticação em dois fatores. Além disso, a pesquisa ressaltou a importância do guideline de boas maneiras, para que possa identificar esses tipos de problemas e antecipalos.

O estudo também destacou a relevância da comunicação na era da internet, mostrando como a evolução da tecnologia e das redes sociais impactou a forma como nos comunicamos e compartilhamos informações. A comunicação é essencial para a sociedade, mas também representa um desafio em termos de segurança cibernética. A pesquisa enfatizou a importância de proteger informações pessoais e adotar medidas de segurança ao usar plataformas de mídia social.

Em relação aos crimes da informática, o estudo ressalta a natureza transnacional dos crimes cibernéticos e como os criminosos podem operar em âmbito global, tornando as investigações e a aplicação da lei mais desafiadoras. Medidas como atualização de

software, uso de senhas seguras e conscientização do usuário são essenciais para proteger contra esses crimes.

O caso de roubo de dados por meio de phishing em Pernambuco em 2022 ilustrou a gravidade da situação e como as quadrilhas de criminosos cibernéticos operam. A conscientização pública sobre os riscos e as medidas de segurança é fundamental para combater essas ameaças.

Em resumo, a pesquisa destaca a importância da segurança cibernética e da conscientização do público em relação aos riscos de roubo de dados em redes sociais. A proteção de informações pessoais e a adoção de práticas seguras através de um guia de boas maneiras (GuideLine), são essenciais para enfrentar essa crescente ameaça na era digital. Além disso, a atualização e o aprimoramento da legislação são necessários para combater eficazmente os crimes cibernéticos.

Como sugestão de trabalhos futuros, foi identificado que esta pesquisa pode ser expandida para abordar outros tipos de crimes que afetam as redes sociais. O phishing, embora seja um dos principais, não é o único responsável pelos danos e vulnerabilidades presentes nas redes sociais. Dessa forma, expandir a análise para abranger esses diferentes tipos de ataques proporciona uma compreensão mais completa dos desafios enfrentados nessas plataformas.

REFERÊNCIAS

BRUNA, S**. Segurança no WhatsApp Messenger em um estudo de caso com ataque de phishing**. Pucgoias.edu.br, 2021. Acesso em: 10 de novembro de 2023.

DANTE, Deniz Bessa. Teorias da Comunicação. 2006. Disponível em: http://portal.mec.gov.br/seb/arquivos/pdf/profunc/10_2_teor_com.pdf. Acesso em: 16 de maio de 2023.

FERREIRA, S. P. **Crimes cibernéticos: A ineficácia da legislação brasileira**. 2012. Disponível em: Pucgoias.edu.br. Acesso em: 12 de junho de 2023.

FRAGA, C**. O roubo de dados na internet está cada vez pior. Saiba evitar!** 2022. Disponível em: https://www.mutuus.net/blog/roubo-de-dados-na-internet/. Acesso em: 06 de setembro de 2023.

GERALDES, A. V. **Phishing.** Revista da Faculdade de Direito da Universidade de Lisboa, v. Vol. 54, nos 1-2 (2013). - p. 87-102, p. 87–102, 2013. Acesso em: 10 de novembro de 2023.

KHONJI, M., IRAQI, Y., JONES, A. **Phishing detection: A literature survey. 2013. IEEE Communications Surveys & Tutorials**, v. 15, n. 4, p. 2091–2121. Acesso em: 08 de setembro de 2023.

MARINHO, Jhemisson Moura. **Mídias Sociais.** 2017. Disponível em: https://dspace.sws.net.br/jspui/bitstream/prefix/196/1/MÍDIAS%20SOCIAIS.pdf. Acesso em: 16 de maio de 2023.

MAXIMO, D., CORREA, R. Intercom. 2014. - **Sociedade Brasileira de Estudos Interdisciplinares da Comunicação Interação em Mídias Sociais**. 2014. Disponível em: https://www.portalintercom.org.br/anais/nordeste2014/resumos/R42-0340-1.pdf. Acesso em: 29 de maio de 2023.

MELLO, E. R. DE et al. **Autenticação multi-fator em provedores de identidade Shibboleth**. 2018 Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/4245>. Acesso em: 15 nov. 2023.

MENESES, Erodines. **Crimes cibernéticos têm aumento de 237% em PE; veja como se proteger dos golpes aplicados pelo celular**. 2022. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2022/08/02/crimes-ciberneticos-tem-aumento-de-237percent-em-pe-veja-como-se-proteger-dos-golpes-aplicados-pelo-celular.ghtml. Acesso em: 12 de setembro de 2023.

MOURA, Daniel, BOMFIM, Nunes. **Proteção Contra-ataques de Phishing no Exército Brasileiro.** 2020. Disponível em: http://www.ebrevistas.eb.mil.br/OC/article/view/6011/5229. Acesso em: 16 de abril de 2023.

RECUERO, R. D. C. **Redes Sociais na Internet: Considerações Iniciais**. 2011. E-Compós, v. 2, 25 de novembro de 2011. Disponível em: https://sol.sbc.org.br/index.php/wie/article/view/21735/21559. Acesso em: 12 de junho de 2023.

SEVERINO, E. R. F. et al**. Como identificar invasões a sua privacidade e roubo de dados na Internet**. 2023. Anais da Exposição Anual de Tecnologia, Educação, Cultura, Ciências e Arte do Instituto Federal de São Paulo - Câmpus Guarulhos, v. 3. Acesso em: 12 de setembro de 2023.

SILVESTRE, Amanda, PRADO, Regis. **O Bem Jurídico nos Crimes Informáticos**. 2017. Acesso em: 31 de abril de 2023.

SMITH, A. **Social Media Use in 2018**. 2018. Pew Research Center. Acesso em: 21 de maio de 2023.

SOUZA, Dayse Suellen**. Linguagem e comunicação na sociedade contemporânea**. 2015. Disponível em: https://www.webartigos.com/artigos/linguagem-e-comunicacao-na-sociedade-contemporanea/134186. Acesso em: 31 de maio de 2023.