ESTRATÉGIA DE PREVENÇÃO NO COMBATE DE LINKS MALICIOSOS

PEREIRA, Marcelo Eduardo
SILVA, Nathan Tagino
CACOSSI, Kleber Francisco
Universidade São Francisco
marcelo.eduardo@mail.usf.edu.br
nathan.tagino@mail.usf.edu.br

Marcelo Eduardo Pereira da Silva, Aluno do Curso de Engenharia de Computação, Universidade São Francisco ; Campus de Bragança Paulista - SP;
Nathan Tagino Silva, Aluno do Curso de Engenharia de Computação, Universidade São Francisco; Campus de Bragança Paulista - SP;
Orientador Professor Kleber Francisco Cacossi, curso de Engenharia de Computação, Universidade São Francisco, Campus de Bragança Paulista - SP.

Resumo. Desde a origem da internet, ainda nos anos 60, sempre houve a necessidade da existência de ferramentas de controle para auxiliar na proteção das informações contidas nas redes. Em um primeiro momento a preocupação partiu das entidades governamentais e militares, porém mais adiante a preocupação se voltou para o usuário comum, muito por conta da democratização do acesso, onde o uso de ferramentas *WEB* se tornou presente no dia a dia da maioria das pessoas, juntamente com o interesse dos criminosos que enxergam nessa democratização uma oportunidade para a aplicação de golpes. Recentemente a cibersegurança ganhou enfoque durante a pandemia do COVID-19, onde milhões de pessoas migraram para o trabalho remoto e sem o devido preparo se tornaram alvos de criminosos virtuais por meio dos chamados *links* maliciosos, técnica de engenharia social que visa enganar os usuários por meio de *sites* similares aos que são utilizados diariamente. Tendo em vista o aumento constante dos crimes virtuais, este projeto visa promover a criação de uma extensão de navegador que sirva de apoio para a identificação de *links* maliciosos, visando a proteção de dados em ambientes corporativos, domésticos e educacionais.

Palavras-chave: Proteção, *internet, phishing, malware, ransomware*, crimes virtuais.

Introdução

Com a recente democratização do acesso às redes, milhões de pessoas entraram no mundo virtual, entretanto, esse aumento é acompanhado do crescimento das aplicações de golpes na *internet*. Segundo dados da FEBRABAN (Federação Brasileira de Bancos) o Brasil foi o quinto país do mundo em número de denúncias de páginas criminosas no ano de 2022, tendo no contexto da pandemia um agravamento no número de casos, devido às medidas restritivas que levaram a um aumento significativo de atividades *online*, muitos indivíduos foram compelidos a migrar para o ambiente virtual. No entanto, devido à falta de preparo e orientação sobre os potenciais riscos cibernéticos, esses usuários tornaram-se alvos vulneráveis de criminosos virtuais. No período de quarentena, as instituições financeiras registraram aumento de 80% nas tentativas de ataques (FEDERAÇÃO BRASILEIRA DE BANCOS, 2020).

Nos ataques os criminosos fingem serem funcionários de instituições respeitáveis e confiáveis, como bancos, grandes lojas *online*, agências governamentais, entre outras, a fim

de induzir a vítima a acreditar nas informações falsas, o que, na realidade, se trata de uma a armadilha (WENDT; JORGE, 2013). Os criminosos escolhem geralmente esses sites para aplicar estratégias de roubo de informações, por meio de programas ou *sites*, para possíveis chantagens, assédio, falsidade ideológica, dentre outros crimes (WENDT; JORGE, 2013). Esse tipo de atividade se configura no chamado "crime cibernético", prática que detém o primeiro registro da nomenclatura no final da década de 1990, durante o encontro do G8 na França (ANDRION, 2021) e desde então serve para tipificar toda e qualquer atividade ilícita praticada em dispositivos de informática por meio da *internet*.

Origem da internet

Durante o período da guerra fria havia uma grande preocupação a respeito do armazenamento das informações de cunho militar, principalmente por conta de possíveis ataques de forças inimigas, dentro desse contexto surge a *Arpanet*, ferramenta capaz de conectar diversos dispositivos de forma remota e em rede, garantido assim, que as informações estejam a salvo. Conforme apontado por Corrêa (2013), os militares dos Estados Unidos consideraram a vulnerabilidade associada à centralização de informações em um único local. A partir desse reconhecimento, o governo manifestou desde o início sua preocupação em estabelecer regulamentações e criar mecanismos de controle da internet com o objetivo de assegurar a integridade das informações. Não demorou até que a *internet* se expandisse e chegasse aos usuários comuns, ainda durante os anos 90 a *internet* deixou de ser de uso exclusivamente das universidades e se tornou uma ferramenta de cunho comercial (EDUVIRGES; SANTOS, 2012), sendo portanto, uma abertura caracterizada como globalizada, favorecendo o avanço exponencial no número de dispositivos em todo o mundo (Figura 1).

Figura 1: Crescimento exponencial dispositivos conectados
(Fonte:https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html)

Com base no gráfico (Figura 1), verificamos um crescimento exponencial de dispositivos conectados de 1994 a 2020, evidenciando que a quantidade de dispositivos conectados está aumentando rapidamente ao longo do tempo, essa tendência sugere que a preocupação com a segurança dos dados também aumentará, à medida que nos tornamos cada

vez mais dependentes e imersos no meio digital. Conforme mais dispositivos se conectam à internet, mais dados serão gerados e compartilhados. Isso cria um ambiente propício para possíveis violações de segurança e ataques cibernéticos. Portanto, é crucial que as empresas e os usuários adotem medidas adequadas para proteger seus dados e informações pessoais.

Internet no Brasil

No Brasil o desenvolvimento das redes de *internet* foi impulsionado por objetivos estatais e militares, muito por conta do contexto histórico e militar da época, além de ser motivado pelo *boom* da *internet* nos anos 80 ("década das redes"). O interesse estatal no desenvolvimento das redes surgiu com o objetivo de superar o atraso no setor de telecomunicações em todo o território nacional. Vieira (2003) relata que o primeiro contato de um órgão brasileiro com a *internet* se deu no ano de 1988, onde a FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) realizou a primeira conexão de *internet* em parceria com o LNCC (Laboratório Nacional de Computação Científica), as entidades usaram de recursos próprios para realizar a conexão com as instituições norte americanas, e embora o modelo inicial tenha funcionado durante um período, foi motivador para a criação do chamado "*Backbone* Nacional" fomentando a conexão entre as instituições nacionais de pesquisa e recompensando os esforços acadêmicos.

Já no ano de 1992, com a implementação do *backbone* da RNP (Rede Nacional de Ensino e Pesquisa), a estrutura foi considerada como sendo a primeira rede de *internet* brasileira com alcance interestadual (STEIW, 2022). Já em 1995 surge o *backbone* nacional de uso misto (comercial e acadêmico), fruto do interesse dos Ministérios das Comunicações e da Ciência e Tecnologia. Corrêa (2013) destaca que de maneira geral o avanço da *internet* em solo nacional resvala nas barreiras sócio econômicas que limitam o acesso às redes, mas apesar das dificuldades iniciais o país se encontra em processo de consolidação desde a última década, outro fator que corrobora é a última pesquisa realizada em 2021 pelo IBGE (Instituto Brasileiro de Geografia e Estatística) demonstrando que o acesso à *internet* chegou ao número de 90% em todo o território nacional.

Portanto, o propósito deste estudo foi destacar o progresso das técnicas empregadas na realização de fraudes virtuais, bem como classificar diversas categorias de ameaças cibernéticas. Além disso, teve também como objetivo a criação de uma extensão para o navegador "*Google Chrome*", destinada a verificar a autenticidade de *links* pertencentes a instituições bancárias, sites governamentais, portais de notícia e lojas mais conhecidas pelos brasileiros, contribuindo assim para a detecção de potenciais riscos de segurança *online*.

Material e Métodos

Público Alvo

O público-alvo desta aplicação são usuários de *internet* em geral, independentemente da idade ou nível de conhecimento técnico, isso se deve ao fato de que o acesso a *links* maliciosos e a ameaça de *phishing, malware ou ransomware* não estão limitados a um único grupo demográfico. Pessoas de todas as idades e níveis de conhecimento podem ser alvos de ataques cibernéticos e se beneficiar da conscientização e educação sobre os perigos associados aos *links* maliciosos, isso inclui usuários comuns que realizam atividades diárias na *internet*, como redes sociais, *e-mails*, compras *online* e navegação em geral. A aplicação pode ser importante para educar crianças e adolescentes desde cedo sobre os riscos da *internet,* bem como idosos podem ser influenciados positivamente com o uso da extensão, especialmente quando se trata de clicar em *links* desconhecidos, uma vez que são

frequentemente alvos de golpes *online* devido à falta de familiaridade com as práticas de segurança digital. Profissionais, principalmente funcionários de grandes empresas, serão beneficiados pelo uso da aplicação, já que podem ser alvos de ataques direcionados, como *spear phishing*, que visam obter acesso a informações confidenciais. Além disso, pequenas empresas, mesmo com recursos limitados, precisam proteger seus negócios contra ameaças *online*. Outro possível grupo favorecido são os educadores que poderão usar a aplicação como uma ferramenta de ensino para conscientização dos alunos sobre segurança cibernética, além disso, pais e responsáveis podem utilizá-la como uma ferramenta educacional para proteger seus filhos e dependentes dos perigos *online*.

Descrição da extensão WEB

Extensões do navegador, são códigos ou programas que podem ser implementados no navegador de internet do seu computador ou celular para desempenhar funções específicas, ou para alterar a aparência do navegador. Dessa forma, foi proposto o desenvolvimento de uma aplicação de extensão para navegadores, em um primeiro momento focado para o navegador *Google Chrome*. A aplicação terá como objetivo identificar possíveis *links* maliciosos e notificar o usuário a respeito do perigo que ele corre ao acessar determinada página. A escolha pelo navegador da *Google* se deu por conta de que quase 41% dos usuários da *internet* mundial optam por navegar na *web* por meio do *Google Chrome*, o que corresponde a pouco mais de 3,2 bilhões de pessoas. Os números impressionantes revelam o quão popular é o navegador da principal empresa de tecnologia do planeta (CIRIACO, 2021). Para a interface da extensão foram utilizadas as linguagens HTML (*HyperText Markup Language*) para marcação e estruturação de código e CSS (*Cascading Style Sheets*) para estilização da interface da página, além disso o programa conta com a estruturação lógica através da linguagem Javascript, as três linguagens foram a trindade das páginas *web*, estando presente na grande maioria dos sites e aplicações *web*.

Funcionalidades e recursos da extensão

A extensão para o Google Chrome possui funcionalidades e recursos que ajudam a identificar se um site é falso ou verdadeiro com base em uma lista de *URLs* confiáveis, essa extensão verifica a *URL* do *site* que o usuário está visitando de forma automática e constante, a verificação ocorre a cada meio segundo, sempre verificando se a página em questão pertence às *URLs* já identificadas previamente como confiáveis pelos desenvolvedores, determinando se o *site* é legítimo ou se há indícios de que possa ser falso. Além disso, a extensão emite alerta de *phishing* para *sites* criminosos já conhecidos (*sites* de *downloads* de *torrents*, ou de pirataria em geral). Isso ajuda a proteger os usuários comuns contra possíveis ataques de *phishing* e a tomar precauções adicionais ao interagir com o *site*.

Ao entrar em contato com esse tipo de *site* a extensão emite um alerta para o usuário, indicando que a página em questão já foi identificada como perigosa. Essa classificação ajuda os usuários a tomar decisões informadas sobre a confiabilidade do *site* antes de prosseguir com qualquer interação. Para garantir a eficácia da extensão, ela pode ser regularmente abastecida com informações e *URLs* confiáveis, garantindo que os usuários tenham acesso a um banco de dados atualizado para uma melhor detecção de *sites* falsos. A lista de *URLs* seguras conta com os sites mais comumente utilizados pelos brasileiros, *sites* de notícias (G1, UOL, Folha de São Paulo, Estadão, entre outros), páginas governamentais (como bancos estatais, .gov, inep, entre outros), *sites* de instituições financeiras privadas (Bradesco, Santander, Itaú, entre outros) e *sites* de compras *online* (mercado livre, olx, ifood, etc..).

Como primeira implementação e validação para testes foram incluídos sites institucionais da Universidade São Francisco, para atender as esferas educacionais e administrativas, além de que a estrutura da extensão é montada para receber possíveis atualizações, para incluir ou reclassificar sites. Na extensão mencionada, existem mais de 20 *sites* governamentais brasileiros, mais de 70 *sites* de compras, mais de 45 *sites* de bancos e uma variedade de outros *sites*, como notícias, faculdades entre outros (Tabela 1).

Tabela 1: Exemplos dos sites utilizados na extensão.

SITES DE BANCOS	SITES DE COMPRAS	SITES DO GOVERNO	OUTROS SITES
Banco do Brasil: www.bb.com.br	Casas Bahia: www.casasbahia.com.br	GOV: www.gov.br	Universidade São Francisco: www.usf.edu.br
Itaú: www.itau.com.br	Magazine Luiza: www.magazineluiza.com.br	Presidência da República: www.gov.br/planalto	Youtube: www.youtube.com
Bradesco: www.bradesco.com.br	Submarino: www.submarino.com.br	Senado Federal: www.senado.leg.br	G1 notícia: g1.globo.com
Santander: www.santander.com.br	Americanas: www.americanas.com.br	Câmara dos Deputados: www.camara.leg.br	UOL notícia: www.uol.com.br

(Fonte: Os próprios autores)

Implementação e arquitetura da extensão

Para implementação da extensão é necessário que o usuário acesse a página de extensões de seu navegador, para o caso do *Google Chrome* é possível por meio da *URL* "chrome://extensions/" (Figura 2).

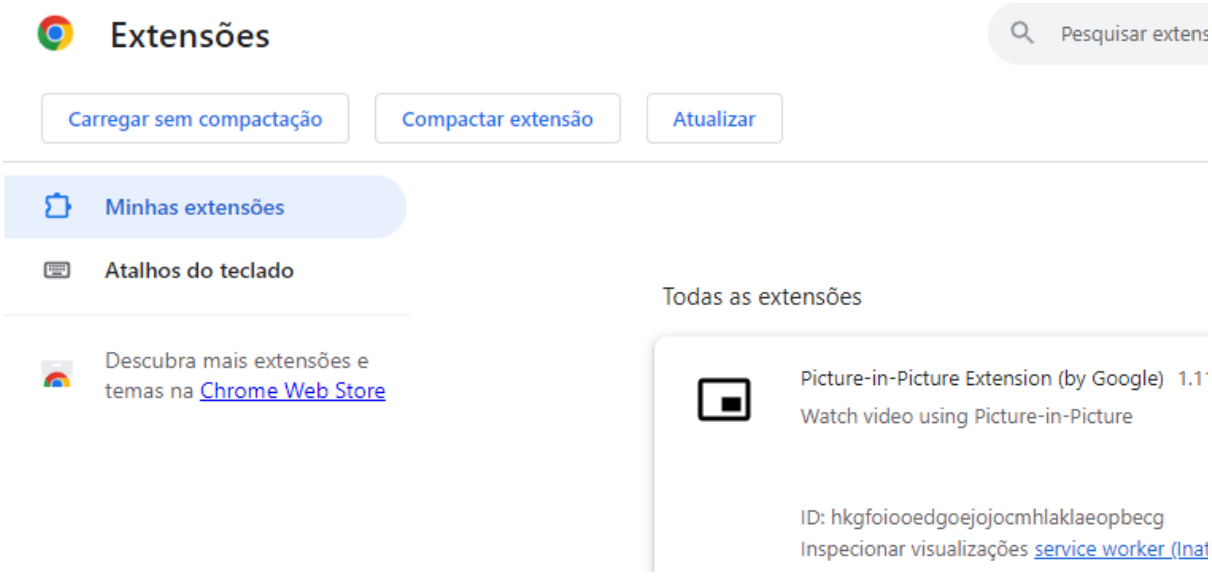


Figura 2: Local onde adiciona a extensão. (Fonte: Os próprios autores)

Para incluir basta clicar em “carregar sem compactação” e incluir o arquivo da extensão, após isso a extensão já estará devidamente instalada no navegador (Figura 3).

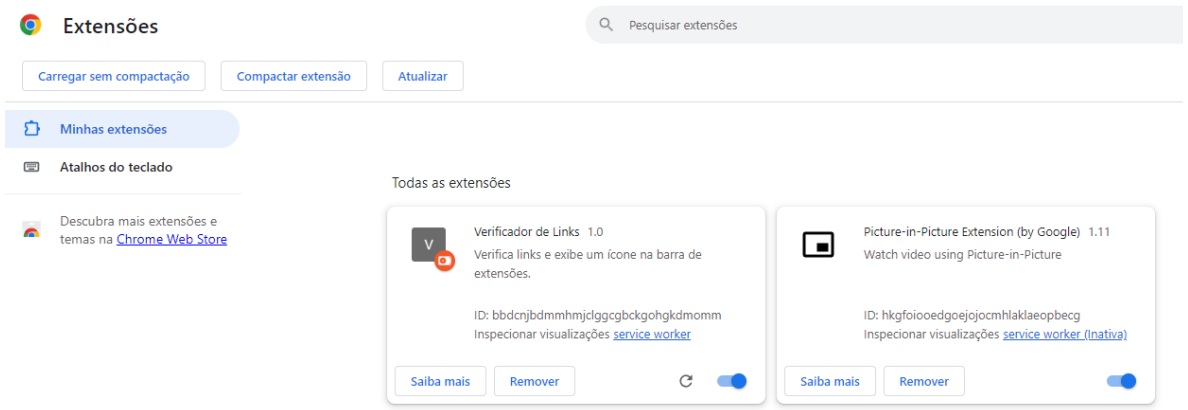


Figura 3: Local da extensão após instalação. (Fonte: Os próprios autores)

Resultados e Discussão

O presente estudo analisou o progresso das técnicas utilizadas pelos criminosos e a classificação das diversas categorias de ameaças cibernéticas com a finalidade da criação de um sistema que auxiliasse usuários da *internet* a não caírem em golpes por meio dos *links* maliciosos.

Endereços Web

Para simplificar a navegação dentro da *internet* foram criadas diversas ferramentas que tornam as informações mais acessíveis, uma delas é a *URL (Uniform Resource Locator*), em português (Localizador Uniforme de Recursos), ferramenta que utiliza o sistema DNS (do inglês, *Domain Name System*) para “traduzir” endereços numéricos em texto, simplificando a navegação dos usuários (COSSETI, 2023). No momento do acesso no site o endereço é automaticamente convertido em um endereço numérico via DNS, por exemplo, ao inserir o endereço do site da Polícia Civil do Estado de São Paulo (www.policiacivil.sp.gov.br) ocorre simultaneamente a tradução para o endereço numérico de IP 200.144.4.82. (WENDT; JORGE, 2013).

Figura 4: Endereço *URL* da Universidade São Francisco (Fonte: Os próprios autores)

A Figura 4 demonstra a composição de um endereço *web*, que é padronizada para facilitar a identificação e navegação entre as páginas *web*, em geral a maioria dos endereços conhecidos começa com o chamado *Scheme*, protocolo usado por servidores para acesso de páginas *web* que utilizam da linguagem de hipertexto HTML (*HyperText Markup Language*), o *scheme* da *URL* pode aparecer de duas diferentes formas, “http://” ou “https://”, nas duas ocorre a abreviação do termo *“Hypertext Transfer Protocol*”, já na segunda ocorre a adição da letra S, que representa “*Secure*”, indicando que o *link* possui ações de segurança para garantir

a integridade do site (PIRES, 2022). O *Scheme* de um site é acompanhado do subdomínio "www" sigla de abreviação para *World Wide Web* (Rede mundial de computadores), posteriormente ocorre a inserção do chamado "*top-level domain*" ou nome do *site* (usf, por exemplo), seguido de seu "*second-level-domain*" ou extensão, que indica o caráter do *site*, a sigla ".edu" indica *sites* voltados para instituições de ensino e ".br" para *sites* brasileiros (MORAES, 2018).

Embora seja um conceito de fácil entendimento há vários golpes que podem ser originados de *URLs*, dentre eles destacam-se os ataques homográficos, que se caracterizam como o uso de caracteres semelhantes para se passar por outro *site* (DCIBER, 2022). Para realizar o ataque os criminosos falsificam com certa exatidão um *site* real, para que a vítima não veja a diferença em um primeiro momento, se alguém *clicar* em um *link* para visitar o *site* de um banco conhecido, por exemplo, acaba acessando um *site* falso, projetado para coletar informações da vítima (WENDT; JORGE, 2013).

Outra técnica comum utilizada por criminosos é o chamado "*typosquatting*" (ou em português erro de digitação) que consiste em se aproveitar de erros comuns na digitação de *sites* para a criação de páginas *web* falsas, como o *site* "www.youtube.com.br" poderia levar a criação de uma página chamada "www.yotube.com", com o propósito de atrair usuários desatentos. Tendo em vista a fragilidade do sistema de *URLs*, a *Google* manifestou interesse em acabar com esse tipo de protocolo ainda em 2018, a fim de conter a proliferação de *sites* falsos, entretanto a iniciativa da empresa levou a uma forte discordância por parte da indústria que não pretende estabelecer uma mudança de padrão (DUTRA, 2023), sendo assim, a expectativa é que não exista uma mudança no padrão das *URLs* em um futuro próximo.

Links Maliciosos

Um tipo de ataque virtual mais comum ocorre por meio das *URLs*, quando criminosos desenvolvem endereços *web* falsos, que tem como objetivo ser muito similar a *sites* já conhecidos, para assim ter acesso a informações sigilosas e confidenciais, esses tipos de golpes são conhecidos como *links* maliciosos. Wendt e Jorge (2013) destacam que para o funcionamento de um *link* malicioso os criminosos utilizam de Engenharia Social para alterar as emoções do "alvo", como resultado, lidam principalmente com o medo, a ganância, a simpatia e a curiosidade, o internauta, por essa motivação, muitas vezes fornecerá informações que não deveria ou clicar em *links* que levam a *sites* que possuem conteúdo prejudicial e/ou execução de códigos nocivos em sua máquina.

Outro aspecto é a utilização do chamado efeito de saliência (ou viés de familiaridade), quando um criminoso emprega este método, ele procurará chamar a atenção das suas vítimas pretendidas, utilizando a morte celebridades, atores famosos, acidente ou outro evento pertinente trazendo o foco para a notícia em si, fazendo com que o indivíduo não se atente ao restante das informações, como o endereço da notícia. Um caso que ocorreu em 2016, por exemplo, quando um *hacker* utilizou de uma notícia falsa referente à morte do ator Brad Pitt para espalhar um *malware* capaz de capturar o *e-mail* e a senha do *Facebook* das vítimas (TECHTUDO, 2016) (Figura 5).

Figura 5: Notícia falsa com características semelhantes do portal norte americano Fox News **(**Fonte:https://www.techtudo.com.br/noticias/2016/09/falsa-notica-sobre-morte-de-brad-pitt-espalha-virus-no-facebook.ghtml)

Para a propagação do *link* o *hacker* utilizou de características semelhantes a outras notícias do portal norte americano *Fox News* para causar viés de similaridade nas vítimas, que uma vez impactadas pela informação da morte de um ator conhecido caiam no golpe sem se atentar ao *site* falso. A divulgação desses *links* está diretamente ligada às redes sociais, uma vez que as mesmas são terreno fértil para a divulgação de notícias, sejam elas verdadeiras ou não, uma vez que a engenharia por trás dessas plataformas (algoritmo) juntamente com o comportamento influenciado por elas geram o epicentro da desordem da informação (FOSTER; CARVALHO; FILGUEIRAS; AVILA, 2021), dentro de uma rede social o usuário comum está diante de informações e notícias a respeito de assuntos de interesse próprio, a fim de gerar engajamento e manter o utilizador na plataforma, facilitando assim a entrega de *links*.

Tipos de Links Maliciosos

Os tipos mais comuns de *links* maliciosos são: *phishing, malware, ransomware*. O *phishing* é derivado da palavra inglesa *fishing*, que significa pescar, ou seja, o comportamento de quem busca informações sobre um usuário de computador, técnica de engenharia social (OLÍVIO, 2010). A palavra também é utilizada para descrever o comportamento de indivíduos que desejam comunicar mensagens que visam induzir a vítima a preencher formulários com suas informações pessoais ou a instalar códigos maliciosos.

Durante um ataque *fishing* a vítima receberá um e-mail, clicará no endereço de um site específico (*link*) encontrado no corpo do e-mail e será levada a um site semelhante àquele que pretendia visitar. O *site* pode ter a capacidade de documentar todos os dados inseridos (*spyware*), incluindo número de conta bancária, cartões de crédito, senha e muitos outros dados importantes. (WENDT; JORGE, 2013). Para que a vítima não desconfie do ataque, os criminosos utilizam réplicas de *sites* reais, com mensagens críveis como o bloqueio de contas, por exemplo, ou outras estratégias mais chamativas, como o *e-mail* falso recebido por funcionários da Universidade São Francisco que simulava uma notícia do portal G1 relativa ao resgate do Fundo de Garantia por Tempo de Serviço (FGTS) (Figura 6A). Ao clicar no *link* os usuários eram redirecionados para o *site* falso de domínio e aparência muito similar ao site original, nele existia a suposta "notícia" seguida de um botão que redirecionava para um formulário onde um usuário desatento poderia cair com facilidade no golpe.

Prática muito comum, como observamos em outra situação, mas com o mesmo *site* e notícia sendo exibido o *site* falso do G1, um conhecido portal de notícias, incentivando as

pessoas clicarem em um *link* para ver informações sobre o FGTS (Fundo de Garantia do Tempo de Serviço) (Figura 6B). No entanto, ao clicar no *link*, os usuários eram redirecionados para um *site* malicioso que extraia informações pessoais ou instalava *malware* em seus dispositivos.

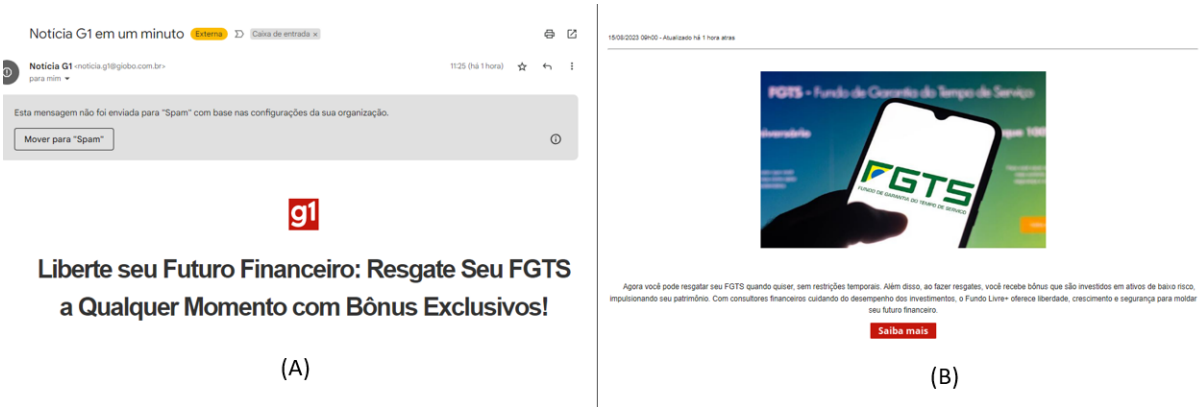


Figura 6: Mostra um e-mail falso sobre o FGTS. (Fonte: Os próprios Autores)

Outras formas são por meio de *e-mails*, no qual são informados que a senha de plataformas de assinatura expirou ou que a fatura está em atraso. Como exemplo, o caso de um *e-mail* falso da Microsoft informando ao usuário que sua senha expirou e que é necessário renová-la (Figura 7A). Esse tipo de *e-mail* é projetado para enganar os usuários e levá-los a fornecer suas informações de *login* em um *site* falso, onde os criminosos podem capturar essas informações para acessar suas contas. Em outra situação, é mostrado um *e-mail* falso informando ao usuário que sua fatura da *Netflix* está em atraso e que ele precisa clicar em um *link* para efetuar o pagamento (Figura 7B). Esse *e-mail* falso é arquitetado para enganar os usuários e levá-los a fornecer informações de pagamento em um *site* falso, onde os criminosos podem apropriar-se de informações financeiras.

Figura 7: Exemplo de *e-mails* falsos que ao clicar redireciona a *sites* falsos (Fonte:https://blog.usecure.io/pt/the-most-common-examples-of-a-phishing-email).

Outro ataque recorrente é o de *malware*, *software* ou código malicioso destinado a invadir, causar danos ou tirar vantagem de computadores, ou dispositivos móveis. Algumas variantes extremas de *malware* são dedicadas a dados financeiros e outras informações pessoais confidenciais e são empregadas para cometer violência, fraude e roubo de identidade. De forma geral este tipo de *software* tem como objetivo causar danos ou levar a uma falha do sistema. *Adware*, espiões, vírus, *bots*, cavalos de Tróia, *worms* e *rootkits* são exemplos de *softwares* maliciosos (ALECRIM, 2016).

Um *malware* apresenta diferentes ramificações, juntamente com nomenclaturas atribuídas a cada uma delas. Um exemplo comum mencionado é o *malware Banker*. É um tipo específico de *malware* que visa roubar informações financeiras, como credenciais de *login* de contas bancárias (Figura 8).

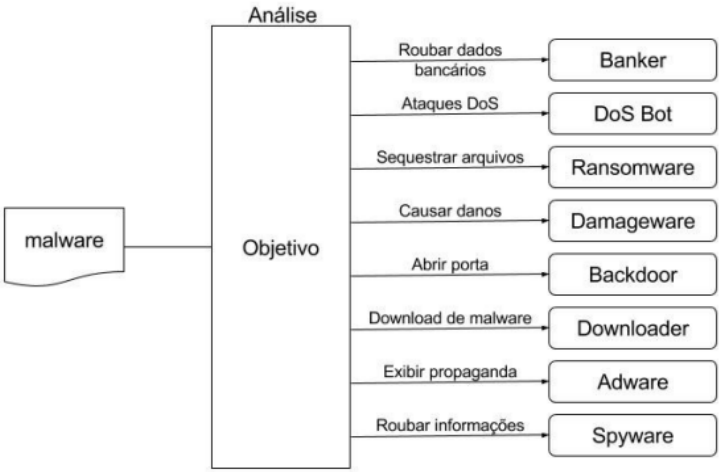
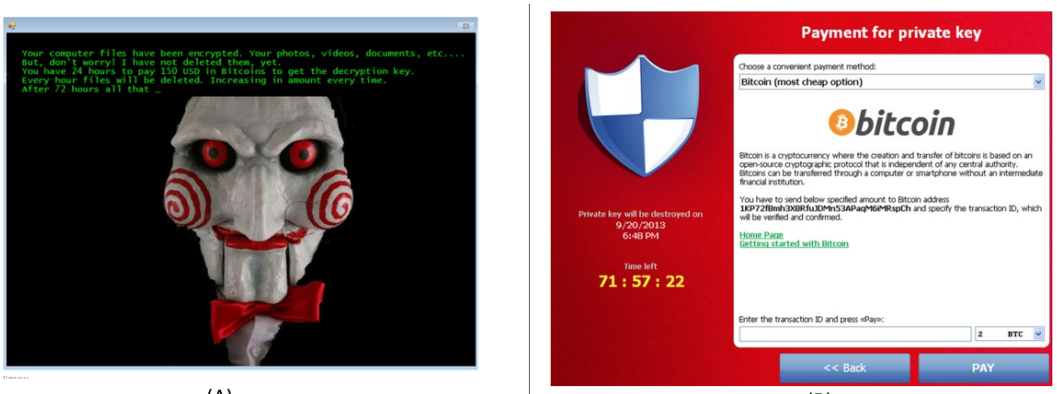


Figura 8: Ramificações de um *malware* e suas nomenclaturas (Fonte: Crimes Cibernéticos: Ameaças e Procedimentos de Investigação - Volume 2).

O ataque *ransomware* por sua vez tem como objetivo impedir o acesso ao sistema infectado, e exigir um pagamento pela liberação do acesso ao sistema, como forma de resgate, eles inibem os arquivos ou componentes essenciais do sistema operacional infectado, Geralmente empregam protocolos criptográficos para proteger arquivos, o que normalmente torna impossível acessar arquivos sem a chave criptográfica. Outro fator de risco é a não garantia de que o criminoso compartilhará a chave para descriptografar os arquivos após concordar em pagar o valor solicitado (ALECRIM, 2016).

Outra forma de ataque é no qual os criminosos bloqueiam o acesso aos dados da vítima e exigem um resgate para liberá-los. Os criminosos sequestram os dados das vítimas e estabelecem um prazo de 72 horas para o pagamento de um valor determinado. Para aumentar a sensação de urgência, os criminosos apagam parte dos dados a cada hora. O objetivo é pressionar as vítimas a pagar o valor exigido dentro de um prazo limite, caso contrário, os dados podem ser permanentemente perdidos ou divulgados (Figura 9).



(A) (B)

Figura 9: Exemplos de ataque *ransomware* no qual sequestram os dados das vítimas (Fonte: https://www.infowester.com/ransomware.php)

Principais sites alvos de links maliciosos

Os alvos mais comuns são os golpes de *Internet banking*, neste tipo de fraude a vítima recebe *e-mails* através de programas de comunicação regulares ou cartões de crédito, etc, com a ajuda de programas de distribuição em massa de *e-mails* (*spam*) o criminoso encaminha inúmeras mensagens em poucas horas. Com o acesso à conta os criminosos podem realizar transações financeiras no banco, compartilhar as informações com outros criminosos cibernéticos ou tirar vantagem das pessoas por meio de transferência de dinheiro e pagamento de boleto (WENDT; JORGE, 2013).

Apesar de ser o grande alvo de ataques virtuais, os aplicativos financeiros não são as únicas fontes de golpes, *sites* de varejo fraudulentos têm sido comuns, especialmente aqueles que realizam vendas de produtos *online*, a vítima realiza o pagamento e não recebe nenhuma mercadoria. Um fator atrativo para as vítimas é o preço, uma vez que o preço praticado pelo *site* fraudulento é normalmente inferior à média de outros sites de varejo *online*, em média 25% a 50% inferior ao das lojas *online* tradicionais (WENDT; JORGE, 2013). Essa estratégia dos preços abaixo para os produtos faz com que o usuário comum desvie o foco da sua atenção e concentre-se apenas para o valor em si, realizando o pagamento rapidamente para conseguir o produto e com isso, acaba caindo no chamado golpe financeiro. Forçando ainda mais as compras, os criminosos utilizam as chamadas promoções relâmpagos, ou seja, a vítima tem poucas horas, ou até mesmo minutos para realizar o pagamento, não havendo assim tempo para checagem do *link* ou da comparação com o preço de uma unidade física da loja em questão. Outro ponto que pode ser notado é a cópia quase que perfeita do *site* original, tendo como única diferença a *URL* (cantinhodobaianinho.com), que usa a mascote das Casas Bahia como referência (Figura 10A).

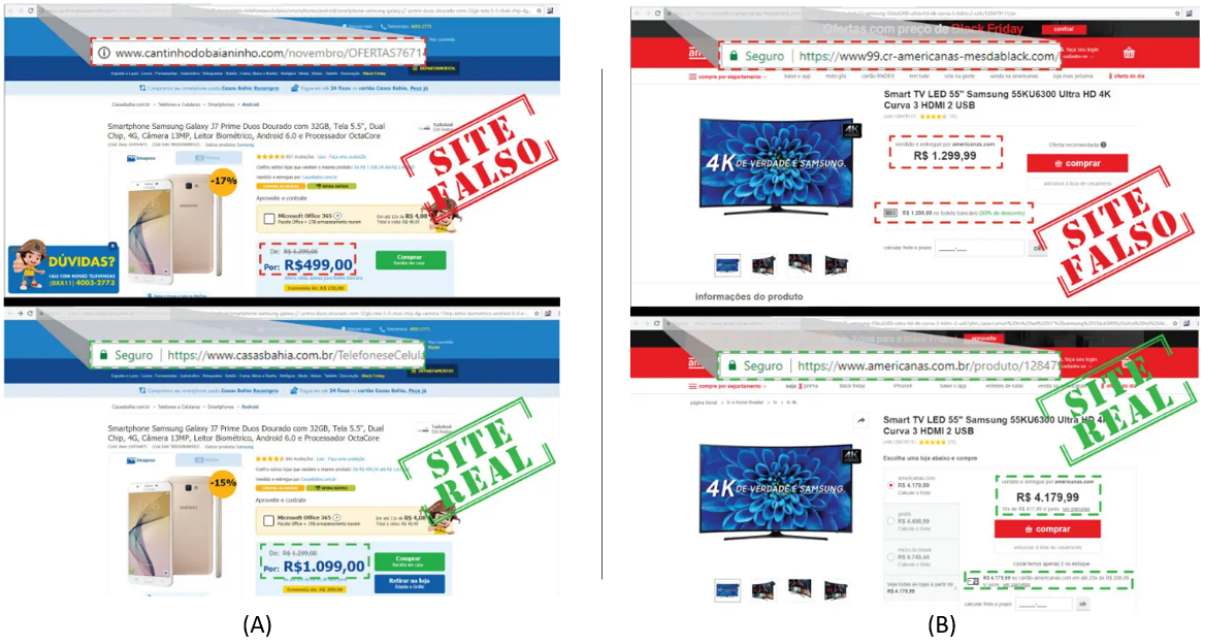


Figura 10: Comparação de *sites* falsos e originais
(Fonte:https://veja.abril.com.br/economia/golpistas-criam-sites-falsos-da-casas-bahia-e-americanas).

Aumento no número de golpes durante a pandemia do COVID 19

Durante o período de pandemia, houve diversas medidas do governo visando o controle do avanço do vírus, dentre essas medidas destaca-se o *lockdown*, medida que atingiu cerca de 46% das empresas, segundo dados da Pesquisa Gestão de Pessoas na crise do COVID 19 (USP, 2020). Entretanto a migração da jornada de trabalho para o modelo remoto sem o devido treinamento para os funcionários ocasionou no aumento do número de golpes e ataques virtuais. Durante a pandemia o Brasil registrou aumento de 66,2% dos casos, atingindo a marca de 200.322 registros no ano de 2022 (Fórum Brasileiro de Segurança Pública, 2023), esses golpes causaram um prejuízo de cerca de 551 milhões de reais aos brasileiros, sendo em média 17 tentativas de golpes por hora durante o ano de 2022 (VASCONCELOS, 2023).

Legislação

Em novembro de 2001 foi celebrada a Convenção sobre Crimes Cibernéticos, em Budapeste (Hungria), o projeto foi desenvolvido com apoio de especialistas e o objetivo foi de facilitar a cooperação internacional no combate aos *cibercrimes*. Conforme destacado por Macedo (2020) esse foi o primeiro projeto internacional com enfoque para os crimes ocorridos na *internet*. O Brasil recebeu o convite para adesão à convenção em dezembro de 2019 e após a análise legislativa a adesão foi aprovada pelo senado em dezembro de 2021, de acordo com o decreto de nº 11.491/2023, assinado pelo então vice-presidente, Geraldo Alckmin. A entrada do governo brasileiro no acordo corrobora com a recente criação da lei nº 12.965/2014, conhecida como o "Marco Civil da *Internet*", que embora tenha criado ferramentas legislativas para o combate de crimes *cibernéticos* se restringindo às limitações do território nacional, e como a maior parte dos crimes virtuais não respeitam fronteiras, a cooperação entre os países é fundamental para o combate dos crimes praticados na *internet* (AGÊNCIA SENADO, 2021).

Existiram também outras medidas anteriores para o combate de crimes cibernéticos, a Lei 12.735/2012, estabeleceu que as polícias civis e a polícia federal devessem criar setores e equipes especializadas para combater crimes realizados em redes de computadores, dispositivos de comunicação ou sistemas informatizados, essa medida pretendia fortalecer a capacidade de investigação e repressão dos delitos *cibernéticos* (WENDT; JORGE, 2013). Outra importante lei para o combate de crimes virtuais é a de número 12.737/2012, conhecida como Lei Carolina Dieckmann, onde a mesma tipifica o crime de invasão de dispositivo informático. As medidas, no entanto, não foram suficientes para armar as autoridades, surgindo então, o projeto do Marco Civil da Internet Brasileira, proposto pelo Ministério da Justiça, utilizado como justificativa para a demora na aprovação da lei de crimes eletrônicos (WENDT; JORGE, 2013).

Com isso, o presente estudo possibilitou a criação de um método eficaz por meio de uma extensão web. A extensão conta com uma interface simples e objetiva, de modo a facilitar o uso para usuários com pouco contato com tecnologia, uma vez que eles são os maiores alvos dos criminosos virtuais. Dentro da interface existem três diferentes "estados", um verde, indicando que o *site* está presente dentro da lista de páginas seguras, um vermelho, indicando o contrário, ou seja, que a página é indicada como insegura e um estágio intermediário, o amarelo, que indica que a página deve ser recarregada para análise (Figura 11).

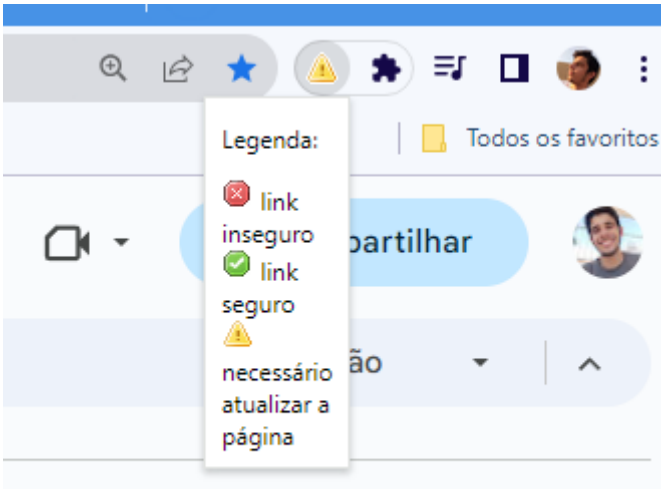


Figura 11: Interface existem três diferentes "estados" (Fonte: Os próprios autores).

Assim, o usuário pode utilizar o navegador da mesma forma do qual está acostumado e quando tiver dúvidas a respeito da veracidade da página pode contar com a extensão para legitimar o acesso (Figura 12).

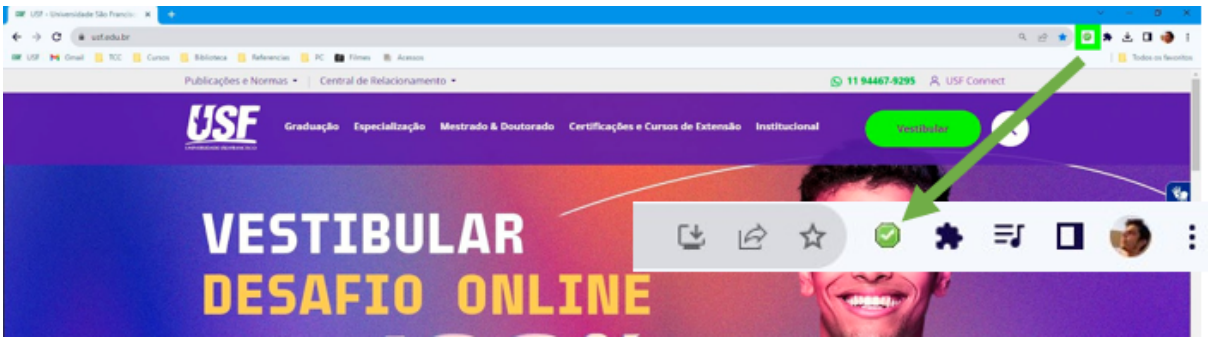


Figura 12: Apresenta em verde que o *site* é seguro no canto superior direito (Fonte: Os próprios autores).

Ao acessar uma página segura à extensão indica por meio do ícone verde a veracidade e autenticidade da página, já em uma página suspeita o padrão de ícone muda automaticamente para o vermelho (Figura 13).

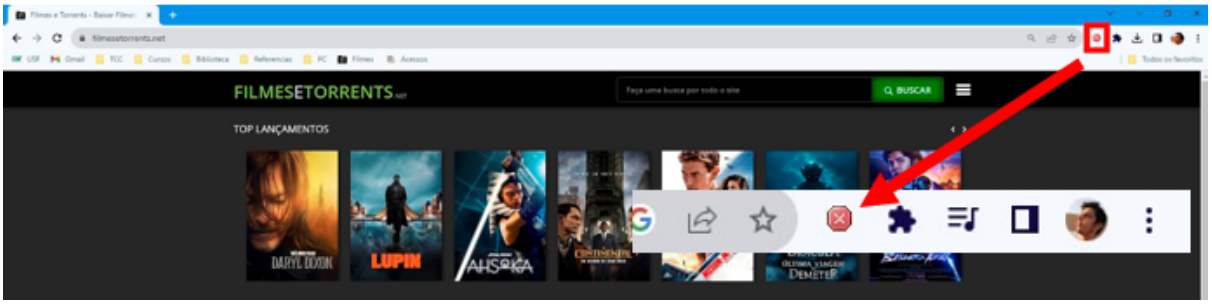


Figura 13: Apresenta em vermelho que o *site* não é seguro no canto superior direito (Fonte: Os próprios autores)

Quando um *site* não é seguro, aparece no meio da tela uma mensagem ou um ícone indicando essa falta de segurança. Essa mensagem alerta o usuário sobre possíveis riscos ao acessar o *site* (Figura 14). É crucial tratar essas mensagens com seriedade e evitar acessar o *site* se ele for reconhecido como não seguro. Isso pode significar que o *site* não possui um certificado de segurança válido, não utiliza criptografia adequada para proteger as informações dos usuários ou pode estar associado a atividades maliciosas.

Figura 14: Mensagem que aparece na tela quando o *site* não é seguro (Fonte: Os próprios autores)

A identificação dos *links* funciona com precisão, de forma rápida e contínua, sem causar transtornos para os usuários, essa fluidez contribui para uma experiência positiva e agradável, além disso, a extensão oferece uma camada adicional de segurança ao navegar na *web*, ajudando os usuários a identificarem *sites* falsos e proteger-se contra possíveis ataques de *phishing*. Com interface simples e objetiva, é uma ferramenta útil para usuários de todas as idades, especialmente idosos e profissionais que lidam com informações sensíveis, além de pessoas que não possuem conhecimento sobre os perigos de *links* maliciosos na *internet*.

Conclusões

Os *links* maliciosos estão cada vez mais presentes no dia a dia dos usuários da *internet*, tornando necessário o estabelecimento de estratégias para combater os mesmos, com isso a aplicação desenvolvida no presente trabalho surge como uma alternativa simples e eficaz para o combate dos criminosos da *internet*, sua interface clara e otimizada permite que diferentes tipos de usuários possam usufruir da aplicação, tanto para os usuários mais familiarizados com tecnologia quanto usuários com pouco conhecimento, como idosos e

crianças. Isso se deve por conta do uso de ícones simples e intuitivos, com cores características e aviso para *sites* considerados perigosos, além disso, a otimização promovida durante o desenvolvimento do projeto permite que a extensão tenha desempenho sólido em diferentes configurações de máquinas e a sua arquitetura permite atualizações contínuas e possíveis implementações de melhorias na extensão.

Referências Bibliográficas

AGÊNCIA SENADO. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. 2021. Disponivel em:< https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico> Acesso em: 27 de setembro de 2023.

ALECRIM, Emerson. **O que é Ransomware?**. 2019. Disponível em: <https://www.infowester.com/ransomware.php>. Acesso em: 25 de setembro de 2023.

ANDRION, ROSELI. **História da segurança virtual: a origem do cibercrime.** 2021. Disponível em :< https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-cibercrime-203073/> Acesso em: 25 de setembro de 2023.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição de mecanismos de governança.** 2006. 239 p. Dissertação (Mestrado em Engenharia de Sistemas e Computação). Universidade Federal do Rio de Janeiro, 2006. Disponível em: <https://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso: 16 de setembro de 2023.

CIRIACO, Douglas. **Google Chrome já tem mais de 3,2 bilhões de usuários.** 2021. Disponível em : <https://canaltech.com.br/apps/google-chrome-ja-tem-mais-de-32-bilhoes-de-usuarios-185780/> Acesso: 16 de setembro de 2023.

CORRÊA, Fabiano Simões. **Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da Internet.** 2013. 171 p. Dissertação (Mestrado em Psicologia). Universidade de São Paulo, 2013. Disponível em: <https://www.teses.usp.br/teses/disponiveis/59/59137/tde-08102013-162610/publico/Fabiano_Correa_Mestrado.pdf>. Acesso: 16 de setembro de 2023.

COSSETTI, Melissa Cruz. **O que é DNS? .**2023. Disponível em: <https://tecnoblog.net/responde/o-que-e-dns/>Acesso em: 25 de setembro de 2023.

DCIBER. **Ataques de phishing homógrafos: quando a conscientização do usuário não é suficiente.** 2022. Disponível em: <https://dciber.org/ataques-de-phishing-homografos-quando-a-conscientizacao-do-usuario-nao-e-suficiente/>. Acesso em: 25 de setembro de 2023.

DUTRA, Daniel . **O que é URL? Entenda o que significa o endereço de sites da Internet.** 2023. Disponível em:

<https://www.techtudo.com.br/guia/2023/05/o-que-e-url-entenda-o-que-significa-o-endereco-de-sites-da-internet-edsoftwares.ghtml>Acesso em: 25 de setembro de 2023.

EDUVIRGES, Joelson Ramos ; SANTOS, Maria Nery dos. **A contextualização da Internet na sociedade da informação.** Universidade Estadual do Piauí , 2011-2012. Disponível em: <https://periodicos.ufmg.br/index.php/moci/article/download/17450/14233/48590>. Acesso: 16 de setembro de 2023.

FEDERAÇÃO BRASILEIRA DE BANCOS. **Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los.** São Paulo, 2020. Disponível em: <https://portal.febraban.org.br/noticia/3522/pt-br/>. Acesso: 16 de setembro de 2023.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 25 de setembro de 2023.

FOSTER, Rene ; CARVALHO, Rodrigo ; FILGUEIRAS, Alberto; AVILA, Emanuelle. **Fake News: O Que É, Como Se Faz E Por Que Funciona?. 2021.** Disponível em: <https://preprints.scielo.org/index.php/scielo/preprint/download/3294/5938/6206> Acesso: 20 de setembro de 2023.

IBGE. **Internet já é acessível em 90% dos domicílios do país em 2021.** 2022. Disponivel em:<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021#:~:text=Em%202021%2C%20o%20celular%20era,computador%20(42%2C2%25)>. Acesso: 16 de setembro de 2023.

MORAES, Daniel. **O que é URL e como ela é decisiva para o sucesso da sua estratégia digita**l. 2018. Disponível em: < https://rockcontent.com/br/blog/url/>. Acesso: 16 de setembro de 2023.

OLIVO, CLEBER KIEL. **Avaliação de características para detecção de phishing de email.** 2010. Disponível em: <https://www.inf.ufpr.br/lesoliveira/download/CleberOlivoMSC.pdf>

PIRES, Julio. **O que é HTTPS?,** 2022. Disponível em : <https://www.hostgator.com.br/blog/o-que-e-https/> Acesso: 20 de setembro de 2023.

RAMOS, Rahellen. **Lockdown: o que é e como funciona.** 2020. Disponível em: <https://www.politize.com.br/lockdown/?https://www.politize.com.br/&gclid=Cj0KCQjwvL-oBhCxARIsAHkOiu2dzt3eAEqdFkZJxoQp9TKss73DKE3mS8LThBagd78thz9iMvYCqaEaAunQEALw_wcB> . Acesso em: 25 de setembro de 2023.

STEIW, Leandro. **ENTENDA O QUE É E PARA QUE SERVE UM BACKBONE**.2022. Disponível em:< https://www.insper.edu.br/noticias/entenda-o-que-e-e-para-que-serve-um-backbone/> Acesso: 20 de setembro de 2023.

TECHTUDO. **Falsa notícia sobre a morte de Brad Pitt espalha vírus no Facebook**. 2016. Disponível em: <https://www.techtudo.com.br/noticias/2016/09/falsa-notica-sobre-morte-de-brad-pitt-espalha-virus-no-facebook.ghtml> Acesso: 20 de setembro de 2023.

UNIVERSIDADE DE SÃO PAULO. **Pesquisa gestão de pessoas na crise covid-19**. 2020. Disponível em:<https://jornal.usp.br/wp-content/uploads/2020/11/Pesquisa-Gest%C3%A3o-de-Pessoas-na-Crise-de-Covid-19-ITA.pdf> Acesso em: 25 de setembro de 2023.

VASCONCELOS, Rosália. **Brasileiros tiveram prejuízo de R$ 551 milhões com golpe online;** proteja-se. 2023. Disponivel em: <https://www.uol.com.br/tilt/noticias/redacao/2023/02/07/medo-de-comprar-online-veja-os-golpes-recentes-mais-aplicados.html>Acesso em: 25 de setembro de 2023.

VEJA. **Golpistas criam sites falsos da Casas Bahia e Americanas.** 2017. Disponível em: <https://veja.abril.com.br/economia/golpistas-criam-sites-falsos-da-casas-bahia-e-americanas> Acesso em: 25 de setembro de 2023.

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. 2003. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=tR4t1Lg2uCcC&oi=fnd&pg=PR18&dq=internet+no+brasil&ots=0j_XUONqB6&sig=6WfGTzpe_-GOrc1W2io2iKUAfew#v=onepage&q=internet%20no%20brasil&f=false> Acesso em: 25 de setembro de 2023.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação** - Volume 2. BRASPORT Livros e Multimídia Ltda, 2013. Acesso em: 25 de setembro de 2023 . Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=iGY-AgAAQBAJ&oi=fnd&pg=PA1&dq=links+maliciosos&ots=OsJTMDabQq&sig=FAF4TszwbJxOCRIixRP3DVnpA1c#v=onepage&q=links%20maliciosos&f=false>