ATAQUES CIBERNÉTICOS: UMA ANÁLISE DO USO DO *SMARTPHONE* POR ALUNAS DO CURSO DE COSTURA 'CRIATIVIDADE EM RETALHOS' DO BAIRRO VILA SÃO JOÃO, EM VÁRZEA GRANDE-MT

Fabiano Pontes Pereira Silva
Mestre em Ciências da Computação (UFPE).
Professor Pesquisador (Fatec Senai-MT). Docente efetivo (IFMT).
DOI: http://lattes.cnpq.br/6710550167962984.
E-mail: fabiano.silva@fatecsenaimt.ind.br.

Lucas Eduardo Rosa Schier
Pós-graduado em Forense Computacional e Perícia Digital;
Graduação e, Defesa Cibernética pela Faculdade de
Tecnologia SENAI Mato Grosso (2024).
DOI: http://lattes.cnpq.br/0313641330529567.
E-mal: lsrosa@outlook.com.br.

Resumo: Este trabalho tem como objetivo analisar o uso do smartphone por mulheres moradoras de bairro de baixa renda e com baixo nível de escolaridade. Para isso foi escolhida a turma de alunas do curso de costura 'Criatividade em retalhos' do bairro Vila São João, em Várzea Grande-MT, por meio da metodologia mista quali-quantitativa, utilizando-se de pesquisa através de formulário online. Após a análise dos resultados, foi possível entender quais vulnerabilidades são enfrentadas por esse grupo de mulheres e elaborar um plano de boas práticas baseado em medidas preventivas de segurança cibernética. O plano de boa prática foi entregue por mensageiro online e publicado em domínio público disponível para consulta na internet.
Palavras-chave: Baixa renda. Inclusão digital. Mulheres. Vulnerabilidades.

Abstract: *This undergraduate thesis aims to analyze the use of smartphones by women residing in low-income neighborhoods with low educational levels. To this end, the group of students from the sewing course "Criatividade em Retalhos " in the Vila São João neighborhood in Várzea Grande, MT, was selected, utilizing a mixed-method (quali-quantitative) approach through an online survey. After analyzing the results, it was possible to understand the vulnerabilities faced by this group of women and to develop a best practices plan based*

on preventive cybersecurity measures. This best practices plan was delivered via online messenger and published in the public domain, available for consultation on the internet.
Keywords: *Digital inclusion. Low-Income. Vulnerabilities. Women.*

INTRODUÇÃO

Com o avanço da tecnologia e o baixo índice de inclusão digital das pessoas com baixa renda, questões como a falta de familiaridade com as práticas de segurança online, a confiança excessiva em desconhecidos e as dificuldades cognitivas podem torná-las mais vulneráveis a diferentes tipos de ataques cibernéticos.

Nesse sentido, o presente trabalho tem como objetivo principal entender o uso do smartphone e levantar informações dos possíveis riscos e vulnerabilidades enfrentados por um grupo de costureiras que vive no bairro Vila São João, na cidade de Várzea Grande-MT.

Para tanto, será realizada uma pesquisa, através de formulário online, para obter resultados sobre o uso do smartphone por essas pessoas e acerca do nível de escolaridade e idade.

A partir dos resultados da pesquisa, será possível propor ideias e medidas de prevenção mais eficazes, visando proteger essa parcela da população contra os golpes e fraudes digitais.

Portanto, este trabalho visa contribuir para a conscientização dessas mulheres contra os ataques cibernéticos, ressaltando a importância de uma abordagem educativa e preventiva na segurança digital para todas as classes sociais. Como não se tornar uma vítima de atividades ilegais e fraudes online, especialmente com o aumento da utilização de vários aplicativos no smartphone para questões pessoais e profissionais?

Este trabalho tem como objetivo principal analisar e entender como o uso do smartphone por mulheres de baixa renda e escolaridade pode ser perigoso de acordo com sua experiência e usabilidade. Após analisar os resultados da pesquisa realizada em campo, será

possível entender melhor o uso desses dispositivos por esse grupo de pessoas, e identificar os principais riscos de segurança enfrentados, que às vezes não são percebidos. Também possibilitará formular insights relevantes sobre estratégias de conscientização e dicas de uso menos vulnerável desses dispositivos.

Deseja-se que, ao término deste estudo, seja possível aumentar a percepção sobre as vulnerabilidades e insegurança encontradas por essa classe no que diz respeito à segurança online.

1. DESENVOLVIMENTO

1.1. *Smartphones* (celulares inteligentes)

Para que um dispositivo móvel se torne "inteligente" é necessário possuir um sistema operacional instalado e com conexão à internet. Segundo informações do Statcounter (2022), a participação no mercado de sistemas operacionais móveis no Brasil até abril de 2022 está assim distribuída: 1) *Android*, com 85,98%; 2) *IOS*, com 13,85%; 3) *Samsung*, com 0,15%; 4) *Windows*, com 0,01%; 5) Desconhecidos, com 0,01%; e 6) *Playstation*, com 0%.

Diante disso, podemos afirmar que os sistemas operacionais móveis mais usados pelos brasileiros são o *Android* (criado pelo *Google*) e em segundo lugar temos o *IOS,* desenvolvido pela *Apple*.

Segundo MCCarty (2011), o primeiro celular a ser considerado um *smartphone*, o Simon, foi desenvolvido pela IBM, ainda no ano de 1992, e possuía uma tela *touchscreen* (sensível ao toque) e um teclado atrelado que permitia ao usuário receber e enviar mensagens de fax, além de *e-mails*, algo extremamente revolucionário para época.

De acordo com Lemos (2007, p. 25):

> O que chamamos de telefone celular é um Dispositivo (um artefato, uma tecnologia de comunicação); híbrido, já que congrega funções de telefone, computador, máquina fotográfica, câmera de vídeo, proces-

> sador de texto, GPS, entre outras; Móvel, isto é, portátil e conectado em mobilidade funcionando por redes sem fio digitais, ou seja, de Conexão; e Multirredes, já que pode empregar diversas redes, como Bluetooth [...], internet (Wi-Fi ou Wi-Max) e redes de satélites para uso como dispositivo GPS.

Os celulares eram objetos considerados essenciais para o mundo corporativo, útil ao trabalho de executivos, já hoje é cada vez mais indispensável à vida em sociedade. Diversas versões de *smartphones* já estão amplamente disponíveis, consumadas e, na expressão de Lemos (2007, p. 9), são uma espécie de "tele tudo", "um dispositivo que é ao mesmo tempo telefone, máquina fotográfica, televisão, cinema, receptor de informações jornalísticas, difusor de e-mails e SMS (...), GPS, tocador de música (MP3 e outros formatos), carteira eletrônica (...)".

2. ENGENHARIA SOCIAL

A partir do avanço da tecnologia, uma gama variada de ameaças, tanto digitais quanto físicas, surgiu, colocando em risco a segurança das informações e dos usuários que as manipulam. Esse período de vulnerabilidade no uso de meios digitais para o compartilhamento de informações teve início com o lançamento do primeiro vírus no sistema, em 1982, por um estudante de 15 anos, através de disquetes. No entanto, esse vírus não representava qualquer perigo para o sistema (Rohr, 2008).

Desde então, a preocupação com a segurança tornou-se parte integrante do dia a dia, visto que os criminosos, valendo-se da ingenuidade das pessoas, encontram uma ampla oportunidade para realizar roubos e furtos virtuais, já que não existem sistemas completamente seguros. Entretanto, graças ao avanço tecnológico, também são desenvolvidos meios eficazes para mitigar os riscos associados à segurança da informação (Santos, 2008).

Engenharia social é o termo que descreve o campo dedicado ao estudo das técnicas e estratégias empregadas na obtenção de informações sensíveis ou confidenciais de uma organização ou até mesmo informações pessoais, valendo-se das pessoas, sejam elas funcionários, colaboradores ou membros da sociedade. Tais informações são obtidas por meio da exploração da ingenuidade ou da confiança (Eiras, 2004).

Segundo Hadnagy e Maxwell (2009), no âmbito da segurança na utilização de tecnologias de informação e comunicação, a engenharia social engloba as estratégias empregadas para obter e comprometer o valor da informação, assim como para acessar dados cruciais e confidenciais de organizações e/ou sistemas computacionais, aproveitando-se da confiança das pessoas.

Na esfera das Ciências Políticas, a Engenharia social refere-se às estratégias e métodos direcionados à manipulação das pessoas, visando induzi-las a realizar ações que, em circunstâncias normais, não tomariam, em larga escala, ou a divulgar informações pessoais ou corporativas voluntariamente, aproveitando-se da vulnerabilidade humana (Hadnagy; Maxwell, 2009).

3. CIBERSEGURANÇA

A cibersegurança emerge como um componente essencial nos estudos do ciberespaço, os quais têm ganhado considerável destaque nas últimas décadas, principalmente devido ao aumento exponencial de ataques e ameaças cibernéticas. Esse cenário tem impulsionado a necessidade de ampla discussão sobre o tema, inclusive pelo Conselho Nacional de Segurança da ONU, sendo constantemente monitorado pela União Internacional de Telecomunicações, uma agência especializada da ONU. Essa crescente preocupação com a segurança internacional tem evoluído paralelamente aos avanços tecnológicos que estão reconfigurando a sociedade (Fonseca, 2021)

Diante do cenário atual, no qual milhões de dados são trocados diariamente pela internet, torna-se evidente a importância do estudo do ciberespaço no âmbito das relações internacionais. Embora a internet seja central nesse contexto, como expressado pelo termo cunhado pelo escritor norte-americano-canadense de ficção William Gibson para seu livro, Fonseca (2021, s/p) ressalta que:

> O ciberespaço configura-se como um universo sem fronteiras e multifacetado, por onde trafega uma infinidade de informações, podendo impactar várias áreas e estar suscetível a distintas abordagens, por meio de diversas perspectivas: política, sociológica, jurídica, tecnológica, entre outras. No que se refere às Relações Internacionais (RI), é inquestionável a capilaridade e as implicações do ciberespaço nas temáticas inerentes à área.

Por essa razão, o tema tornou-se uma questão recorrente nas discussões entre governos e organizações internacionais, ganhando destaque na agenda da segurança internacional, sendo reconhecido como segurança cibernética (Lopes, 2016, p. 16).

Em 2010, ocorreu um incidente que foi como um ponto de reviravolta significativo para a segurança internacional, pois foi considerado por diversos acadêmicos como um dos primeiros ataques cibernéticos. Um *worm* de computador, denominado Stuxnet, foi responsável por infectar uma usina nuclear de enriquecimento de urânio no Irã, danificando as centrífugas nucleares e comprometendo o avanço do programa nuclear do país (Fonseca, 2021).

Três anos depois, em 2013, outra situação aconteceu, em que Edward Snowden, um ex-funcionário da Agência Nacional de Segurança dos EUA, revelou um sistema de monitoramento de dados do governo estadunidense, que espionava a comunicação até mesmo de países amigos e suas populações.

4. IDENTIDADE DIGITAL

O sujeito pós-moderno tornou-se ávido por informação, levando a uma busca excessiva por dados em todos os aspectos de sua vida, inclusive nas interações que estabelece no ciberespaço. Tudo o que existe na internet é informação codificada. Em outras palavras, sua própria existência virtual é formada por código informacional, permitindo-lhe modular e construir sua identidade de acordo com seus desejos ou as necessidades da comunidade virtual à qual pertence. Isso faz com que haja uma modulação das identidades, permitindo que o sujeito virtual não corresponda necessariamente ao sujeito real, mas possa construir uma nova identidade que se adapte ao ambiente virtualizado.

> A virtualização não é uma desrealização (a transformação de uma realidade num conjunto de possíveis), mas uma mutação de identidade, um deslocamento do centro de gravidade ontológico do objeto considerado: em vez de se definir principalmente por sua atualidade (uma "solução"), a entidade passa a encontrar sua consistência essencial num campo problemático (Lévy, 1996, p. 17-18).

Por meio de comunidades virtuais, é possível formar novos grupos, com perfis e características próprias que atendam às necessidades específicas dessas comunidades. Lévy (1999) descreve esse processo como "inteligência coletiva", embora Rüdiger (2002) alerte que a interatividade virtual não substitui nem equivale à interação social:

> [...] as redes não são outro mundo, mas uma mediação da sociedade em que vivemos: as redes apenas pretendem, com maior ou menor sucesso, passar por tal coisa. O ciberespaço não é em geral, segundo tudo indica, uma nova realidade, mas uma sublimação tecnológica da realidade com que estamos acostumados (Rüdiger, 2002, p. 17).

Conforme Bauman (2005), tudo se torna fluido, inclusive as identidades e relações na cibercultura, seguindo esse princípio de fluidez. Como entidades moldadas por novas realidades, tudo nesse ambiente se torna volátil, bastando um clique do mouse ou a mudança de página.

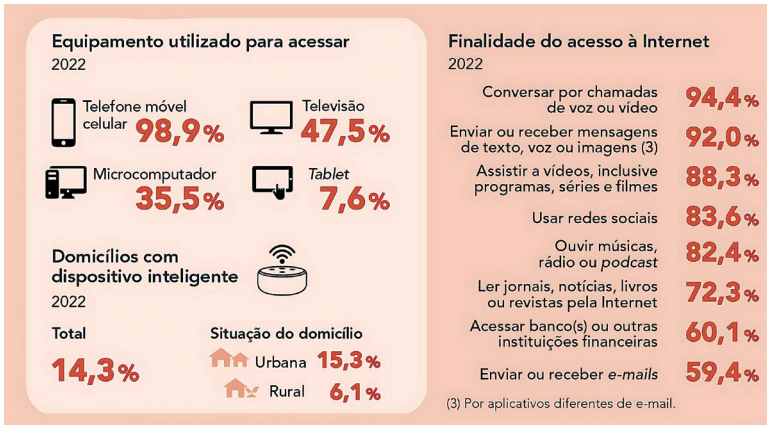
> [...], a "identidade" só nos é revelada como algo a ser inventado, e não descoberto; como alvo de um esforço, "um objetivo"; como uma coisa que ainda se precisa construir a partir do zero ou escolher entre alternativas e então lutar por ela e protegê-la lutando ainda mais – mesmo que, para que essa luta seja vitoriosa, a verdade sobre a condição precária e eternamente inconclusa da identidade deva ser, e tenda a ser, suprimida e laboriosamente oculta (Bauman, 2005, p. 21).

5. UM OLHAR PARA A ATUALIDADE

Segundo dados publicados pelo IBGE 2022 (figura 1), o smartphone é o principal meio de acesso à internet, conforme mostrado na Figura 1, ainda é possível perceber que os maiores índices de uso da internet pelo smartphone são para conversas, chamadas de voz ou vídeo, compartilhamento de mídias e entretenimento. Apesar disso o uso para movimentações financeiras tem crescido muito desde a criação do sistema de pagamentos por Pix, pelo qual o usuário precisa utilizar os aplicativos bancários para efetuar pagamentos não somente a empresas como também entre pessoas físicas.

O uso de aplicativos do governo como: Meu INSS, Carteira de trabalho digital e aplicativo GOV, que contêm documentos pessoais com dados sensíveis e é capaz de assinar documentos por meio da assinatura digital, entre outros aplicativos, também é comum em smartphones de todos os brasileiros. Sendo assim o smartphone é o dispositivo portátil mais desejado por ataques de invasão.

Figura 1- Meio de acesso mais utilizado



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Pesquisas por Amostra de Domicílios, Pesquisa Nacional por Amostra de Domicílios Contínua 2021-2022.

6. METODOLOGIA

A metodologia deste trabalho, cujo objetivo é analisar o uso do smartphone e entender os riscos quanto a sua utilização, é dada como análise, que segundo Gil (2008) é o exame necessário para identificar suas relações fundamentais.

Dessa forma, na primeira fase foi definido o tema juntamente com a escolha do público a ser estudado, considerando sua faixa etária e nível de escolaridade. Sendo assim, foi escolhida uma turma de alunas do curso de costura "Criatividade em retalhos", composta por 14 mulheres que residem no bairro periférico Vila São João, da cidade de Várzea Grande-MT.

Salienta-se que foi desenvolvida uma abordagem quantitativa, e para isso foi elaborado um questionário online projetado para obter informações detalhadas sobre os padrões de uso do smartphone, que foi aplicado de forma online com 100% de participação das alunas. Após a obtenção das respostas, foi construído um referencial teórico por meio de pesquisas de publicações físicas e em bases online. Após a organização do material foi feita uma síntese de toda a literatura reunida para a execução da análise e outros pontos levantados neste trabalho.

Os dados foram coletados e processados pela plataforma Google Forms, e foi feita uma análise descritiva dos resultados para identificar padrões e tendências do uso do smartphone, incluindo funcionalidades mais empregadas e quais eram os sistemas operacionais dos dispositivos utilizados.

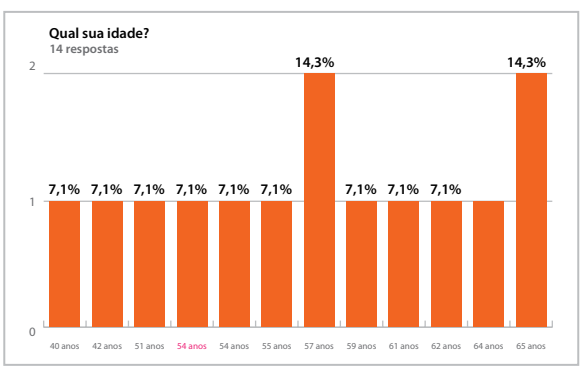
Os participantes foram informados de que esses dados trariam informações e que estas seriam mantidas em sigilo, e para lhes assegurar que sua privacidade não seria violada, não foi feita nenhuma coleta de dados sensíveis, como nomes, dados de contato, entre outros, apenas dados considerados cruciais para a execução desta análise de forma anônima.

7. DISCUSSÃO E RESULTADOS

Este capítulo traz os resultados obtidos através do questionário aplicado ao grupo de estudo, os dados foram coletados, processados e analisados estatisticamente, visando identificar padrões de uso, níveis de conhecimento, preferências do usuário e riscos quanto à utilização do smartphone.

Analisando os resultados da pergunta número 1 da pesquisa, foi possível perceber que todos os respondentes possuem idade superior a 40 anos e que a maioria tem acima de 50 anos, conforme mostra a Figura 2.

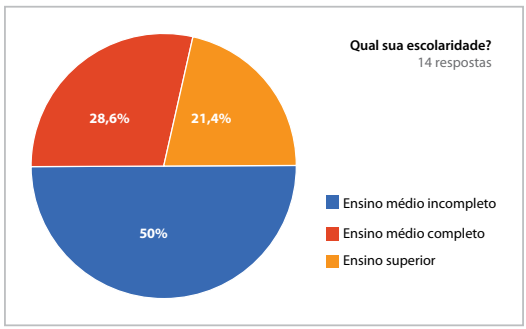
Figura 2 – Faixa etária



Fonte: Elaborada pelo autor (2024).

A partir da análise dos resultados da pergunta número 2, foi possível observar que pelo 50% do grupo possui escolaridade inferior ao ensino médio, como exibido na Figura 3.

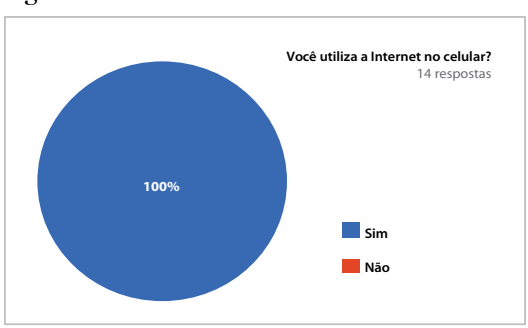
Figura 3 – Nível de escolaridade



Fonte: Elaborada pelo autor (2024).

Dos dados obtidos na pergunta número 3 foi possível constatar que 100% do grupo possui pelo menos um smartphone com conexão à internet, conforme a Figura 4:

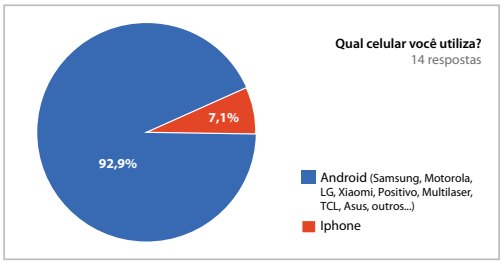
Figura 4 – Conectividade



Fonte: Elaborada pelo autor (2024).

Observando os resultados da pergunta número 4, conforme apresentado na Figura 5, verifica-se que o dispositivo mais utilizado é o com sistema operacional Android.

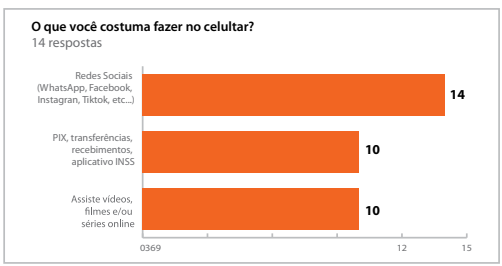
Figura 5 – Tipo de dispositivo



Fonte: Elaborada pelo autor (2024).

A partir da pergunta número 5, é possível inferir quais são as principais atividades realizadas através do smartphone, como demonstrado na Figura 6.

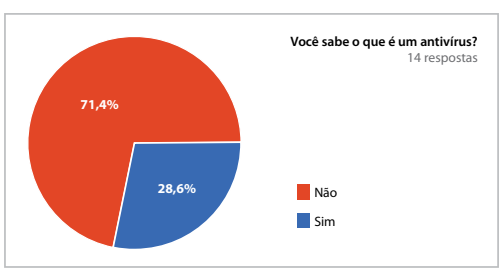
Figura 6 – Usabilidade do Smartphone



Fonte: Elaborada pelo autor (2024).

A pergunta número 6 mostra que 71,4% dos entrevistados não sabem o que é um antivírus, conforme a Figura 7.

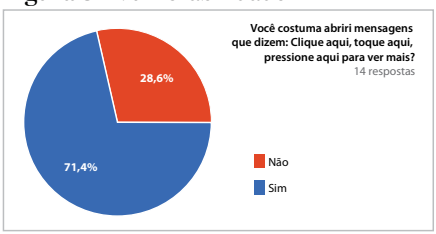
Figura 7 – Antivírus



Fonte: Elaborada pelo autor (2024).

De acordo com as respostas da pergunta número 7, verifica-se que a maioria dos entrevistados se tornam vulneráveis pela curiosidade em mensagens com sugestão de clique e abertura de links, como mostrado na figura 8:

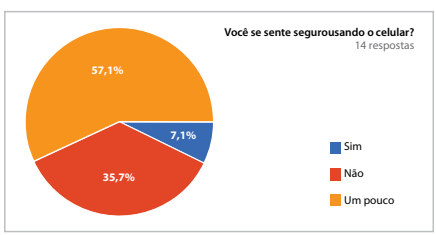
Figura 8 – Vulnerabilidade



Fonte: Elaborada pelo autor (2024).

A pergunta número 8 evidencia que mais da metade dos respondentes se sente "um pouco seguro" ao usar o celular, como demonstrado na Figura 9:

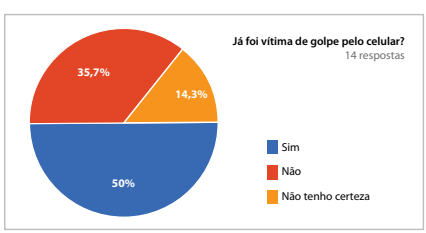
Figura 9 – Sensação de segurança



Fonte: Elaborada pelo autor (2024).

A última pergunta do questionário (número 9) mostra que 50% dos entrevistados já sofreram algum tipo de golpe pelo celular, conforme a Figura 10:

Figura 10 – Experiência



Fonte: Elaborada pelo autor (2024).

A partir deste levantamento, foi possível observar quais são as atividades mais desenvolvidas no dia a dia desse grupo, também pode-se mensurar qual o nível de confiança que seus componentes possuem ao utilizar o dispositivo, assim como o nível de conhecimento em relação ao uso seguro da conexão à internet por meio do dispositivo móvel.

Com as respostas obtidas no instrumento metodológico aplicado, foi possível identificar os riscos da população escolhida, ou seja, elementos vulneráveis para os quais a defesa cibernética atua como importante área para mitigar esse cenário de riscos. Contudo, foi concebido um Plano de Boas Práticas online, disponível por um domínio público para facilitar o acesso e promover eficiência na solução dos riscos encontrados. Disponível em: https://bit.ly/lucas_schier

CONSIDERAÇÕES FINAIS

O estudo "Ataques Cibernéticos: uma análise do uso do smartphone por alunas do curso de costura 'Criatividade em Retalhos', Vila São João, Várzea Grande-MT" levanta a questão: Como evitar fraudes online com o aumento do uso do smartphone? Um questionário revelou necessidades, resultando em um "Plano de Boas Práticas", publicado em um site de domínio público. Futuramente, fabricantes poderão oferecer cartilhas personalizadas durante a inicialização dos dispositivos.

REFERÊNCIAS

BAUMAN, Zygmunt. **Identidade**: entrevista a Benedetto Vecchi. Rio de Janeiro, Jorge Zahar Ed., 2005.

CNSEG.ORG.BR. **"Proteção contra riscos cibernéticos cresce 880% em cinco anos"**. Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização-CNseg. Disponível em: https://cnseg.org.br/noticias/protecao-contra-riscos-ciberneticos-cresce-880-em-cinco-anos/. Acesso em: 20 abr. 2024.

EIRAS, M. C. **Engenharia Social e Estelionato Eletrônico.** 2004. 40 f. Monografia (Conclusão de Curso – lato sensu). IBPINET – The internet school e Uni-Rio. Graduação em Segurança da Informação na Internet, Rio de Janeiro.

FONSECA, Leila Oliveira da. A cibersegurança sob o prisma das Relações Internacionais. **Revista Relações Exteriores**, 20/10/2021. Disponível em: https://relacoesexteriores.com.br/ciberseguranca-relacoes-internacionais/. Acesso em: 3 jan. 2024.

GIL, A. C. **Métodos e Técnicas de Pesquisa Socia**l. 6. ed. São Paulo: Atlas, 2008.

HADNAGY, C.; MAXWELL, E. **Social Engineering Defined.** Social engineering framework. 2009. Disponível em: http://www.social-engineer.org/framework/Social_Engineering_Defined. Acesso em: 2 fev. 2024.

LEMOS, André. Comunicação e práticas sociais no espaço urbano: as características dos Dispositivos Híbridos Móveis de Conexão Multirredes (DHMCM). Comunicação, Mídia e Consumo. **Consumo**, São Paulo, v. 4, n. 10, p. 23-40, 2007.

LEMOS, André. Mídias locativas e territórios informacionais. In: ARANTES, P.; LÉVY, Pierre. **Cibercultura.** São Paulo: Ed. 34, 1999.

LÉVY, Pierre. **O que é virtual?** São Paulo: Ed. 34, 1996.

LOPES, Gills Villar. **Relações Internacionais Cibernéticas (CiberRI):** uma defesa acadêmica a partir dos estudos de segurança Internacional. 2016, 171 f. Tese (Doutorado em Ciências Políticas) – Programa de Pós-Graduação em Ciências Políticas da Universidade Federal de Pernambuco. Recife: Universidade Federal de Pernambuco, 2016.

MCCARTY, Brad. **The History of the Smartphone.** 2011. Disponível em: http://thenextweb.com/mobile/2011/12/06/the-history-of-the-smartphone/. Acesso em: 15 mar. 2024.

ROHR, A. **Engenharia Social:** Uma Ameaça À Sociedade Da Informação. Perspectivas Online, 2013.

RÜDIGER, Francisco. **Elementos para a crítica da cibercultura**: sujeito, objeto e interação na era das novas tecnologias de comunicação. São Paulo: Hacker Editores, 2002.

STATCOUNTER. **Statcounter Global Stats**. [S.I] [1999]. Disponível em: https://gs.statcounter.com/. Acesso em: 30 abr. 2024.