UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

COMPORTAMENTO EM SEGURANÇA DA INFORMAÇÃO NA INTERNET, UMA ABORDAGEM SOB A ÓTICA DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO

Felipe Saulo Rodrigues de Souza Catojo

Orientadora
Simone Bacellar Leal Ferreira

RIO DE JANEIRO, RJ - BRASIL
DEZEMBRO DE 2020

COMPORTAMENTO EM SEGURANÇA DA INFORMAÇÃO NA INTERNET, UMA ABORDAGEM SOB A ÓTICA DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO

Felipe Saulo Rodrigues de Souza Catojo

DISSERTAÇÃO APRESENTADA COMO REQUISITO PARCIAL PARA OBTENÇÃO DO TÍTULO DE MESTRE PELO PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA DA UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO (UNIRIO). APROVADA PELA COMISSÃO EXAMINADORA ABAIXO ASSINADA.

Em conformidade com a Resolução nº 5.257 de 25/03/2020 e a Ordem de Serviço PROPGPI nº 3 de 2/07/2020, esta ata vai somente por mim assinada, atestando que a defesa ocorreu com a participação dos componentes abaixo listados.

Aprovada por:

_____

Simone Bacellar Leal Ferreira, D.Sc. - UNIRIO

_____

Sean Wolfgand Matsui Siqueira, Ph.D. - UNIRIO

_____

Aline da Silva Alves, D.Sc. – Fundação Oswaldo Cruz

RIO DE JANEIRO, RJ – BRASIL

DEZEMBRO DE 2020

Catalogação informatizada pelo(a) autor(a)

C357 CATOJO, FELIPE SAULO RODRIGUES DE SOUZA
COMPORTAMENTO EM SEGURANÇA DA INFORMAÇÃO NA INTERNET, UMA ABORDAGEM SOB A ÓTICA DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO / FELIPE SAULO RODRIGUES DE SOUZA CATOJO. -- Rio de Janeiro, 2020.
132

Orientador: Simone Bacellar Leal Ferreira .
Dissertação (Mestrado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Informática, 2020.

1. idosos. 2. teoria da motivação para a proteção. 3. segurança da informação. 4. protection motivation theory. 5. home users. I. , Simone Bacellar Leal Ferreira, orient. II. Título.

SUMÁRIO

1 INTRODUÇÃO 1
1.1 Problema de pesquisa 2
1.2 Objetivo de pesquisa 3
1.3 Relevância da pesquisa 4
1.4 Delimitação da pesquisa 6
1.5 Estrutura da dissertação 6
2. REFERENCIAL TEÓRICO 7
2.1 ENVELHECIMENTO POPULACIONAL E TIC (TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO) NA TERCEIRA IDADE 7
2.3 TEORIAS COMPORTAMENTAIS 13
2.3.1. Teoria da Ação Racionalizada (*Theory of Reasoned Action* - TRA) - proposta por Fishbein e Ajzen (1975) 14
2.3.2. Teoria do Comportamento Planejado (*Theory Of Planned Behavior* - TPB) - proposta por Ajzen, 1985 14
2.3.3. Teoria Da Motivação Para A Proteção (*Protection Motivation Theory - PMT*), proposta por Rogers, 1975 15
2.3.4. Teoria Da Dissuasão (*Deterrence Theory* – DT) – proposta inicialmente por Beccaria, 1963 18
2.4 SEGURANÇA DA INFORMAÇÃO 19
2.5 TRABALHOS RELACIONADOS 21
3 METODOLOGIA 27
3.1 ETAPAS DO MÉTODO 28
3.1.1 Determinação dos perfis dos usuários participantes da pesquisa 28
3.1.2 Definição da teoria de avaliação comportamental aplicada; 29
3.1.3 Elaboração do questionário 29
3.1.4 Aplicação do questionário 29
3.1.5 Definição dos parâmetros de segurança da informação avaliados 30
3.1.6 Seleção do site para execução das tarefas na etapa de observação de usuários; 31
3.1.7 Execução da pesquisa com grupo de terceira idade com o método etnográfico 32
3.1.8 Análise dos dados e discussão dos resultados. 33
3.1.9 Elaboração de recomendações; 33
4. PREPARAÇÃO E EXECUÇÃO DA PESQUISA 35
4.1 Preparação da Pesquisa 35

4.1.1 Elaboração do material utilizado durante a sessão 35
4.1.2 Preparação do ambiente e execução 35
4.1.3 Definição das perguntas do questionário 38
4.2 Execução da pesquisa 42
4.2.1 Questionário 42
4.2.1.2 Estatística descritiva dos resultados obtidos 43
4.2.2 Observação de usuários 56
4.2.2.1 Imagem e descrição dos itens de segurança em que os usuários interagiram 56
4.2.2.2 Usuários selecionados para os testes 62
4.2.2.3 Análise dos resultados 77
5 – RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO 84
6 - CONCLUSÃO 95
7 - REFERÊNCIAS BIBLIOGRÁFICAS 98
APÊNDICE 1 - TERMO DE CONSENTIMENTO 108
APÊNDICE 2 - QUESTIONÁRIO 109
APÊNDICE 3 - AÇÕES DE SEGURANÇA 112

LISTA DE ILUSTRAÇÕES

TABELA 1 - PROCESSOS COGNITIVOS DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO E VARIÁVEIS NÃO DIRETAMENTE OBSERVÁVEIS ASSOCIADAS 17

TABELA 2 - AÇÕES DE SEGURANÇA DA INFORMAÇÃO SELECIONADAS 31

TABELA 3 - MATRIZ DE CORRELAÇÃO DAS VARIÁVEIS DE PERFIL (GÊNERO, IDADE, ETC.) E DAS VARIÁVEIS DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO 40

TABELA 4 - QUESTÕES ELABORADAS E VARIÁVEIS ANALISADAS 41

TABELA 5 - FREQUÊNCIA RELATIVA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 1 A 5) 44

TABELA 6 - FREQUÊNCIA RELATIVA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 6 A 10) 45

TABELA 7 - FREQUÊNCIA ABSOLUTA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 1 A 5) 46

TABELA 8 - FREQUÊNCIA ABSOLUTA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 6 A 10) 47

FIGURA 1 - DADOS DA ASSERTIVA “EU TROCO MINHAS SENHAS COM FREQUÊNCIA”, DO PÚBLICO DE TERCEIRA IDADE 48

FIGURA 2 - DADOS DA ASSERTIVA “UM VÍRUS PODE SER PREJUDICIAL”, DO PÚBLICO DE TERCEIRA IDADE 49

FIGURA 3 - DADOS DA ASSERTIVA “AS MINHAS CHANCES DE SER INFECTADO POR VÍRUS SÃO ALTAS”, DO PÚBLICO DE TERCEIRA IDADE 49

FIGURA 4 - DADOS DA ASSERTIVA “MINHAS INFORMAÇÕES PESSOAIS JÁ FORAM VIOLADAS”, DO PÚBLICO DE TERCEIRA IDADE 50

FIGURA 5 - DADOS DA ASSERTIVA “CONSIDERO FÁCIL TOMAR AS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO NECESSÁRIAS”, DO PÚBLICO DE TERCEIRA IDADE 51

FIGURA 6 - DADOS DA ASSERTIVA “ACREDITO QUE UM SOFTWARE DE PROTEÇÃO POSSA SER ÚTIL PARA DETECTAR E REMOVER VÍRUS”, DO PÚBLICO DE TERCEIRA IDADE 51

FIGURA 7 - DADOS DA ASSERTIVA “ACATO A OPINIÃO DAS PESSOAS DO MEU CÍRCULO SOCIAL SOBRE OS CUIDADOS QUE DEVEM SER TOMADOS AO CONVERSAR COM DESCONHECIDOS NA INTERNET, OU TOMAR OUTRAS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO”, DO PÚBLICO DE TERCEIRA IDADE 52

FIGURA 8 - DADOS DA ASSERTIVA “ACREDITO QUE SOFTWARES PARA PROTEÇÃO E SEGURANÇA POSSAM CAUSAR PROBLEMAS EM OUTROS PROGRAMAS NO MEU COMPUTADOR”, DO PÚBLICO DE TERCEIRA IDADE 53

FIGURA 9 - DADOS DA ASSERTIVA “TENHO O HÁBITO DE TOMAR MEDIDAS DE PROTEÇÃO NA INTERNET”, DO PÚBLICO DE TERCEIRA IDADE 54
FIGURA 10 - DADOS DA ASSERTIVA “CONSIGO INSTALAR SOFTWARES DE PROTEÇÃO MESMO NÃO HAVENDO NINGUÉM PARA ME ENSINAR”, DO PÚBLICO DE TERCEIRA IDADE 54
TABELA 9 - MEDIDAS DE TENDÊNCIA CENTRAL 55
FIGURA 11 - AÇÃO 1 – VERIFICAR CADEADO 56
FIGURA 12 - AÇÃO 2 – VERIFICAR HTTPS 57
FIGURA 13 - AÇÃO 3 – VERIFICAR CERTIFICADO DE SEGURANÇA 57
FIGURA 14 - AÇÃO 4 – VERIFICAR DOMÍNIO 58
FIGURA 15 - AÇÃO 5 – VERIFICAR FIREWALL 58
FIGURA 16 - AÇÃO 6 – NAVEGAR ANÔNIMO 58
FIGURA 17 - AÇÃO 7 – REALIZAR *LOGIN* E *LOGOUT* 59
FIGURA 18 - AÇÃO 8 – IDENTIFICAR DESTINO DE URL ANTES DE CLICAR 60
FIGURA 19 - AÇÃO 9 – IDENTIFICAR PHISHING 61
FIGURA 20 - AÇÃO 10 – DEFINIR SENHA FORTE 62
TABELA 10 - USUÁRIOS SELECIONADOS PARA OS TESTES 63
TABELA 11 - INFORMAÇÕES SOBRE A CONCLUSÃO DE CADA AÇÃO PELO PÚBLICO IDOSO 79
TABELA 12 - INFORMAÇÕES SOBRE O TEMPO DE CONCLUSÃO DE CADA AÇÃO PELO PÚBLICO IDOSO 82

Agradecimentos

Em primeiro lugar, gostaria de agradecer a Deus! Sem ele, jamais teria chegado até aqui.

À minha família, pelo apoio incondicional ao longo de toda essa jornada.

Aos meus pais, Alceli e Francisca, por todo amor, carinho e dedicação. Vocês sempre estarão em meu coração!

Agradecimentos especiais a minha orientadora Simone Bacellar Leal Ferreira, sempre extraíndo o melhor de mim, contribuíndo de forma decisiva para uma formação plena, pude aprender muito com você, não só em matéria de conhecimento, mas também como pessoa. Obrigado por tudo, desde já!

Ao meu amigo Fellipe Wood, que me estimulou a participar do programa e me apoiou durante essa trajetória.

A todos os professores do PPGI/UNIRIO, que contribuiram com a minha formação por meio de exemplos e de ensinamentos que certamente levarei comigo ao longo da vida.

Aos membros da banca, Sean Siqueira (UNIRIO) e Aline da Silva Alves (Fundação Oswaldo Cruz) por terem aceitado me avaliar.

Às pessoas que conheci, aos colegas que fiz no NAU (Núcleo de Acessibilidade e Usabilidade), em especial a Carolina Christina do Sacramento Nardi, pelas conversas elucidativas que muito ajudaram no aprendizado e na organização das minhas ideias.

À esta Universidade, pela experiência única que vivenciei.

Aos voluntários que abriram mão do seu tempo para contribuir com essa pesquisa.

Minha imensa gratidão a esta egrégia instituição de ensino e as pessoas que fazem parte dela.

Catojo, Felipe Saulo Rodrigues de Souza. Comportamento em Segurança da Informação na Internet, Uma Abordagem sob a Ótica da Teoria da Motivação para a Proteção. UNIRIO, 2020. 110 páginas. Dissertação de Mestrado. Departamento de Informática Aplicada, UNIRIO.

RESUMO

Entender os comportamentos dos usuários domésticos em segurança da informação tem sido uma tarefa desafiadora e também pouco abordada na literatura. Como contraponto, as pesquisas com usuários organizacionais têm recebido atenção considerável. Essa pesquisa teve o objetivo de obter o comportamento em segurança da informação dos usuários idosos com setenta anos, realizando um estudo sob a ótica da Teoria da Motivação para Proteção (PMT - Protection Motivation Theory), cuja finalidade é entender o que estimula a tomada de decisão dos usuários em situação de risco, tendo sido escolhida em função do seu extenso uso na literatura e por sua eficácia em prever comportamentos em segurança; o propósito de obter o comportamento é direcionar adequadamente as recomendações de segurança da informação. Para atender a este objetivo, este estudo contou com trinta participantes, sendo vinte idosos em uma parte quantitativa que responderam a dez questões fechadas de segurança da informação e mais dez idosos em uma parte qualitativa. Os resultados indicaram que as variáveis da *PMT* mais negligênciadas por este público foram “Autoeficácia”, “Experiência prévia com riscos de segurança” e “Suporte de Segurança Percebido”, indicando que o público de terceira idade possui dificuldades para desempenhar tarefas relacionadas a segurança da informação e que tendem a necessitar de suporte para realizar atividades de segurança, além de acreditarem que nunca foram alvo de algum ataque de *malware*. A etapa qualitativa também demonstrou que a maioria dos usuários carecem de conhecimento sobre conceitos básicos em segurança da informação, tendo dificuldades na execução de algumas atividades de segurança, em especial as atividades de verificação da situação de suas ferramentas de segurança (antivírus, *firewall*) e na definição de senhas fortes.

Palavras-chave: Usuário doméstico, segurança da informação, comportamento, Teoria da Motivação para a Proteção, idosos.

ABSTRACT

Understanding the behaviors of home users in information security has been a challenging task and also little addressed in the literature. In contrast, surveys of organizational users have received considerable attention. This research aimed to obtain the information security behavior of elderly users aged seventy or more, carrying out a study under the perspective of the Protection Motivation Theory (PMT), whose purpose is to understand which encourages decision-making by users at risk, having been chosen because of its extensive use in the literature and for its effectiveness in predicting safety behaviors; the purpose of obtaining the behavior is to properly address the information security recommendations. To achieve that objective, this study had thirty participants, twenty of whom were elderly in a quantitative part who answered ten closed questions of information security and another ten elderly in a qualitative part. The results indicated that the PMT variables most neglected by this public were "Self-efficacy", "Previous experience with security risks" and "Perceived Security Support", indicating that the elderly public has difficulties to perform tasks related to information security and who tend to need support to perform security activities, in addition to believing that they have never been the target of any malware attack. The qualitative stage also demonstrated that most users lack knowledge about basic concepts in information security, having difficulties in the execution of some security activities, especially the activities of checking the situation of their security tools (anti-virus, firewall) and setting strong passwords.

Key words: Home-user, information security, behavior, Protection Motivation Theory, PMT; elderly.

1 INTRODUÇÃO

Os usuários de internet tendem a não se comportar de maneira segura no que tange às suas informações ao lidar com tecnologias (MAYER et al, 2017). Usuários domésticos, em especial, possuem um fator agravante, visto que no ambiente doméstico inexiste uma política de segurança da informação ou uma conduta a ser respeitada (MAYER et al, 2017).

Com base nisso, os usuários domésticos estão mais suscetíveis a vulnerabilidades de segurança da informação, pois decidem por conta própria como devem se proteger e, sobretudo, se ou como devem executar um comportamento de segurança (THOMPSON et al, 2017).

Quando os dispositivos dos usuários são comprometidos em razão da concretização das ameaças que exploram essas vulnerabilidades, não apenas os seus dados pessoais e profissionais são expostos, mas seu dispositivo se torna uma via ideal para que indivíduos de má-fé ataquem organizações e distribuam material ilegal ou eticamente comprometido (LI & SIPONEN, 2011).

Além disso, à medida que as ameaças on-line continuam avançando e se multiplicando, aumenta o potencial de ser vítima de ataques (EMC CORPORATION, 2013 *apud* BOOTHROYD, 2014). Ao longo do tempo, os ataques na internet e em sistemas conectados à internet se tornaram mais sofisticados, enquanto a habilidade e o conhecimento exigidos para montar um ataque diminuíram. Os ataques se tornaram mais automatizados e podem causar mais danos a esses usuários (STALLINGS, 2014).

Foram encontrados poucos trabalhos na literatura retratando estudos comportamentais de segurança da informação no ambiente doméstico, principalmente, ao público idoso com idade igual ou superior a setenta anos, e aplicando uma abordagem metodológica mista (qualitativa e quantitativa) de avaliação à luz da *Teoria da Motivação da Proteção*.

Assim, essa pesquisa abordou o comportamento dos usuários em segurança da informação com idosos de setenta anos ou mais de idade, através de um questionário respondido por vinte pessoas. Avaliou também o conhecimento de mais dez voluntários de terceira idade em uma amostra

adicional sobre dez atividades relacionadas à segurança da informação na internet em uma etapa de *Observação de usuários,* qualitativa*,* em que esses voluntários interagiram com diversos itens de segurança da informação.

Foram realizadas análises dessas interações e do questionário, em seguida os resultados foram sintetizados em tabelas e em imagens. A análise da etapa de questionário concluiu que as variáveis da *PMT* mais negligenciadas por este público foram: “Autoeficácia”, “Experiência prévia com riscos de segurança” e “Suporte de Segurança Percebido”, indicando que o público de terceira idade possui dificuldades para desempenhar tarefas relacionadas à segurança da informação e que tendem a necessitar de suporte para realizar atividades de segurança, além de acreditarem que nunca foram alvo de algum ataque de *malware.* Já a etapa de *Observação de usuários* também demonstrou que a maioria dos usuários necessitam de conhecimento sobre conceitos básicos em segurança da informação, o que aumenta o risco de violação de dados e também a probabilidade das ameaças se concretizarem e causarem algum tipo de impacto na privacidade dos usuários ou, na segurança das informações. A pesquisa gerou 25 recomendações de segurança da informação distribuídas por treze categorias.

1.1 Problema de pesquisa

O problema abordado nessa dissertação é que empresas, governos e organizações empreendem esforços para conscientizar funcionários e cidadãos a como agir corretamente na internet de modo a evitar potenciais ameaças de segurança da informação (THOMPSON et al, 2017); no entanto, é possível observar que muitos desses esforços não surtem o efeito desejado. Inúmeras recomendações são disseminadas, mas pouca atenção é dada ao comportamento e às atitudes dos usuários (BADA et al, 2015). Para melhor elaborar as diretrizes e recomendações, é necessário conhecer essas reações para ser mais eficaz na conscientização dos usuários e consequentemente no combate a ameaças digitais.

Existem ameaças conhecidas em segurança da informação (ETSI GS, 2015), como por exemplo:

1. Ameaças oriundas da configuração incorreta dos serviços;
2. Ameaças oriundas de vulnerabilidade de software;
3. Ameaças oriundas do próprio comportamento do usuário.

Dessas ameaças, o comportamento do usuário é uma das mais exploradas pelos criminosos, que lançam mão de técnicas de engenharia social [1] e buscam comprometer sites com códigos maliciosos para violar as informações pessoais dos usuários e das empresas (IBM, 2019).

O relatório da *International Business Machines Corporation* – IBM denominado *Cost of a Data Breach* aponta que 51% dos ataques ocorrem por vias maliciosas e criminosas, enquanto que 24% dos ataques ocorrem devido à falha humana e 25% ocorrem devido a falhas nos sistemas (IBM, 2019).

O comportamento é uma das vulnerabilidades enfatizadas também pelo *European Telecommunications Standards Institute Group* Specification (ETSI GS, 2015) como um dos vetores de ataque, e na literatura, poucos estudos objetivam compreender a temática em questão, principamente quando se trata de usuários domésticos idosos com 70 anos ou mais de idade.

Dessa forma, o problema de pesquisa consiste em entender o comportamento dos usuários em segurança, os seus pontos fracos e fortes para conseguir elaborar recomendações que modifique o comportamento do usuário com mais eficácia.

1.2 Objetivo de pesquisa

Objetivo principal

[1] *Engenharia Social* é a manipulação emocional e psicológica do indivíduo para descobrir informações confidenciais com o intuito de executar ações maliciosas contra uma organização ou contra o próprio indivíduo (EMINAĐAOĐLU et al, 2009 *apud* WILSON, 2018).

A presente pesquisa teve como objetivo entender o comportamento em segurança da informação de vinte usuários idosos com setenta anos ou mais em uma parte quantitativa, sob a ótica *da Teoria da Motivação para Proteção,* e também de aferir o conhecimento de mais dez usuários idosos em matéria de segurança da informação em uma parte qualitativa, com o propósito de propor recomendações de segurança da informação.

Objetivos intermediários

Os objetivos intermediários tornam-se necessários para viabilizar a conclusão do objetivo principal:

1. Analisar as variáveis que influenciam o comportamento em segurança da informação no uso das TICs à luz da *Teoria Da Motivação Para A Proteção*.
2. Identificar as principais vulnerabilidades comportamentais relacionadas à segurança da informação dos usuários;
3. Propor recomendações de segurança da informação.

1.3 Relevância da pesquisa

A terceira idade representa hoje quase 11% da população brasileira e o número de brasileiros com mais de 60 anos está avançando, e superou os trinta milhões em 2017; além disso, o grupo de 65 anos ou mais de idade é o que mais rapidamente cresce, e o grupo de 70 anos ou mais de idade, normalmente, já está aposentado ou está na iminência de se aposentar, segundo a Pesquisa Nacional por Amostra de Domicílios Contínua do Instituto Brasileiro de Geografia e Estatistica (IBGE, 2018), (BRASIL, 1988) e (BRASIL, 1991).

Além do fato de que a quantidade de pessoas mais velhas está crescendo, o uso da tecnologia também vem aumentando em ritmo acelerado. A quantidade de pessoas que fazem uso da internet mais do que dobrou,

passando de 8% em 2012 para 19% em 2016, de acordo com o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC, 2017).

Ainda segundo o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação - CETIC, em 2017 a quantidade de domicílios com acesso à internet no território nacional está se expandindo, e chegou a 61% dos domicílios, o que equivale a quase 42,1 milhões de domicílios, o que representa um aumento de sete pontos em relação ao percentual observado em 2016 (CETIC, 2017).

Esse aumento da utilização da tecnologia no ambiente doméstico traz uma preocupação, considerando que os computadores de usuários em suas residências são invadidos para serem utilizados como um vetor de ataque às empresas e organizações.

No tocante à segurança da informação, conforme o *Cost of a Data Breach Report*, relatório que foi elaborado com a participação de 500 empresas e 3000 pessoas da área de informática, o custo médio total da violação de dados dessas empresas equivale a $3,92 milhões. Já o custo por registro perdido equivale a $150, enquanto que o tempo para identificar e conter uma violação é de 279 dias (IBM, 2019)

No Brasil, conforme o relatório supracitado, o custo por registro violado é de $69 e o custo por dado violado é de $1.35. Além disso, o relatório ainda aponta que 51% dos ataques ocorrem por vias maliciosas e criminosas, enquanto que 24% dos ataques ocorrem devido à falha humana e 25% ocorrem devido a falhas nos sistemas (IBM, 2019).

Além disso, o comportamento em segurança da informação é um campo importante para pesquisas em Sistemas de Informação (OMIDOSU e OPHOFF, 2016).

Portanto, espera-se que a presente pesquisa contribua com o entendimento do comportamento dos voluntários de terceira idade em segurança da informação na internet, como também produza recomendações para ações preventivas no uso de serviços digitais, considerando a tendência de aumento da expectativa de vida das pessoas, do aumento crescente de

usuários idosos nas Tecnologias da Informação e Comunicação (TICs) e também do crescente número de tentativas de violação de dados.

1.4 Delimitação da pesquisa

Essa pesquisa se ateve a identificar as variáveis da *Teoria da Motivação para a Proteção* mais negligenciadas pelos usuários ao tomar uma decisão sobre segurança da informação na internet e, também a explorar as fragilidades e as forças dos usuários, com relação a diversas atividades de segurança da informação e fornecer recomendações para as fragilidades identificadas.

1.5 Estrutura da dissertação

A dissertação divide-se em seis capítulos, incluindo este de introdução:

O capítulo 2 (Referencial teórico) apresenta informações sobre terceira idade, envelhecimento populacional, idosos e as TICs (Tecnologias de Informação e Comunicação), contexto de uso das TICs e segurança da informação. Nesse capítulo também são apresentados conceitos de teorias comportamentais amplamente utilizadas em pesquisas de desempenho em segurança da informação. Por último são referenciados trabalhos de outros autores sobre o tema da presente pesquisa.

O capítulo 3 (Metodologia) detalha o método utilizado no questionário, o método utilizado na observação de usuários, os procedimentos de coleta de dados e critérios de avaliação empregados durante o processo de pesquisa.

O capítulo 4 (Preparação e execução da pesquisa) detalha a execução da pesquisa, abrangendo a etapa de Questionário e de Observação de usuários.

O capítulo 5 (Recomendações de segurança da informação) apresenta as recomendações elaboradas com base nos resultados das etapas anteriores.

O capítulo 6 (Conclusões) apresenta a culminância da pesquisa.

2. REFERENCIAL TEÓRICO

Este capítulo apresenta informações sobre o envelhecimento populacional e a adesão dos idosos à tecnologia, bem como os seus contextos de uso. São apresentados conceitos sobre teorias do comportamento, além de referenciar outros trabalhos da literatura sobre segurança da informação e vulnerabilidade de idosos na internet, com objetivo de reforçar a relevância do tema abordado nesta pesquisa.

2.1 ENVELHECIMENTO POPULACIONAL E TIC (TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO) NA TERCEIRA IDADE

No contexto global, conforme o relatório "*World Population Ageing*", existem 703 milhões de pessoas acima de 65 anos ou mais no mundo em 2020. Além disso, a expectativa é que esse número dobre para 1.5 bilhão em 2050 (United Nations, 2019).

Vale ressaltar também que, conforme o relatório apontado, o envelhecimento populacional não leva necessariamente a um declínio macroeconômico. De forma oposta, com políticas sensatas e bem definidas pode haver um crescimento, inclusive (United Nations, 2019).

Já no tocante aos países emergentes, o que inclui o Brasil, a pesquisa "*Aging in Brazil*", afirma que do número estimado de dois bilhões dos adultos que representarão 22% da população global em 2050, oitenta por cento estarão vivendo em países em desenvolvimento (NEUMANN & ALBERT, 2018). Além disso, os idosos de sessenta anos ou mais representarão 18,6% da população no Brasil em 2030 e 33,7% em 2060 (IBGE, 2009).

Um ponto curioso e que reforça o fenômeno do envelhecimento é que uma criança que nasceu no Brasil em 2015, tem uma expectativa de viver vinte anos a mais em relação àquela que nasceu cinquenta anos antes (*World Report on Aging and Health*, 2015).

A Lei brasileira de número 10.741, de 1º de outubro de 2003, define como idoso todo aquele com idade igual ou superior a sessenta anos (BRASIL, 2003), indo ao encontro do padrão adotado pela Organização Mundial da Saúde – OMS - (KPOLOVIE et al, 2017). No entanto, em uma nação desenvolvida, tal como no Japão, a atual definição oficial de idoso é de 65 anos (TOKUDA & HINOHARA, 2008).

A OMS faz distinção de acordo com o índice de desenvolvimento humano (IDH) dos países (KPOLOVIE et al, 2017); na Papua-Nova Guiné, por exemplo, pessoas com 45 anos, já se sentem mais velhas, como se já fossem idosas (GBD 2017).

Existem alguns fatores que influenciam o envelhecimento saudável, como, por exemplo, o fator genético, o fator físico e social, além do status socioeconômico do indivíduo (WHO, 2018).

Alguns problemas de saúde identificados nos idosos decorrem do isolamento social (GRENADE & BOLDY, 2008 apud NARDI, 2016). Todavia, a maioria dos idosos prefere envelhecer em seus lares, e, por este motivo, a tecnologia pode desempenhar um papel importante, estimulando-os para que se mantenham sempre conectados e ativos e tornando-os mais independentes (PEEK et al, 2016).

As Tecnologias da Informação e Comunicação diminuem o isolamento do indivíduo por meio de quatro aspectos: “(1) conexão externa com o mundo, (2) ganho de suporte social, (3) participação em atividades desejadas, e (4) incremento da autoconfiança” (CHEN e SCHULZ, 2016).

Para esse público, as Tecnologias de Informação e Comunicação auxiliam na manutenção da capacidade cognitiva e contribuem para o enriquecimento da qualidade de vida (SLEGER; BOXTEL; JOLLES, 2011 *apud* AUGUSTO, JOSÉ, 2017).

No entanto, por falta de investimentos em inovações para os usuários de terceira idade, há uma escassez de serviços mais completos e amigáveis para essas pessoas (Malgarinou M., Goulia E., 1997; Emke-Poulopoulou I, 1999 *apud* ROUPA et al, 2010).

Além disso, muitos produtos e serviços existentes geralmente não são adequados às necessidades dos usuários de terceira idade, trazendo o sentimento de frustração e fazendo com que o indivíduo continue dependendo de outras pessoas (Cutler D.M., Meara E., 2016; Malgarinou M., Goulia E, 1997; Emke-Poulopoulou I, 1999. *apud* ROUPA et al, 2010).

Diferenças geracionais relacionadas à exposição à tecnologia podem reduzir o aproveitamento das tecnologias por pessoas da terceira idade. Essas diferenças são notáveis no uso de novas tecnologias e às vezes são chamadas de “desigualdade digital” ou mesmo “fosso digital” (CHANG et al, 2004). A desigualdade digital refere-se a uma disparidade relacionada ao acesso ou uso da tecnologia da informação e comunicação entre as gerações (CHANG et al, 2004).

À medida que novas tecnologias são desenvolvidas, os idosos podem não se adaptar a novos recursos ou capacidades. Por isso, continuam usando a tecnologia desenvolvida quando eram jovens, mesmo que tenha sido substituída por uma tecnologia mais nova e aprimorada. Dessa forma, a desigualdade digital é uma situação contínua, mudando a cada geração (CHARNESS & BOOT, 2005 *apud* WALLACE, GRAHAM, & SARACENO, 2013).

Embora muitos produtos e serviços desenvolvidos não sejam tão amigáveis para os usuários de terceira idade, inúmeras tecnologias foram desenvolvidas com o objetivo de atender a demanda do público da terceira idade; a pesquisa de (DEEN, 2015) identificou algumas:

1. “Dispositivos vestíveis como detectores de queda, monitores de pressão, medidores de gasto de energia diário, entre outros;
2. Técnicas de predição para identificar enfermidades em seus estágios iniciais;
3. Sensores para detecção de proximidade;
4. Tecnologias de reconhecimento de padrões, para detectar comportamentos inusuais;

5. Tecnologias que mensuram o tempo em que o indivíduo passou sentado, parado e caminhando.” (DEEN, 2015)”.

Além dessas, outras tecnologias de cuidados à saúde proveem suporte para tratamento contínuo, permitindo que pacientes possam se cuidar em casa ao invés de no hospital (MIRANDA, 2019).

Com relação à interação do público da terceira idade com os serviços digitais, a pesquisa conduzida pela (MEDALERTHELP, 2018) demonstrou que o público de terceira idade interage com os serviços digitais nos moldes a seguir:

1. “No tocante ao uso, passam cerca de 27 horas por semana on-line, sendo que 82% dos idosos usam mecanismos de busca para coletar informações desejadas;
2. No tocante ao propósito de utilização, 78% fazem uso devido à facilidade que possuem para acessar as suas informações, 60% utilizam para interarem-se dos assuntos que permeiam a sua vida cidadã, como a política e, 33% por ser uma fonte confiável para se informar;
3. A maior parte utiliza redes sociais para comunicar-se e entreter-se (MEDALERTHELP, 2018)”.

Entretanto, ainda há algumas dificuldades enfrentadas pelo público da terceira idade na adoção da tecnologia e de serviços digitais. Idosos estão abertos à tecnologia; no entanto, pode haver barreiras associadas, tais como problemas de usabilidade e acessibilidade (VAPORTZIS et al, 2017).

Existem outros pontos enfrentados pelos idosos em relação às tecnologias, que são (PEWRESEARCH, 2017):

1. “Limitações físicas para usufruir das tecnologias;
2. Ceticismo em relação às vantagens que a tecnologia pode prover;

3. Dificuldades para aprender e entender novas tecnologias” (PEWRESEARCH, 2014).

Já em matéria de segurança da informação, no que concerne às vulnerabilidades mais críticas de segurança da informação enfrentadas pelo público de terceira idade, evidenciam-se os ataques baseados em engenharia social na utilização de senhas e credenciais (VIANA, 2017).

Engenharia Social é a manipulação emocional e psicológica do indivíduo para descobrir informações confidenciais com o intuito de executar ações maliciosas contra uma organização ou contra o próprio indivíduo (EMINAĐAOĐLU et al, 2009 *apud* WILSON, 2018).

O público de terceira idade também confia a segurança de suas informações a terceiros, recebendo suporte de técnicos e de softwares externos, o que os deixa mais expostos a riscos de segurança da informação (BOOTHROYD, 2017).

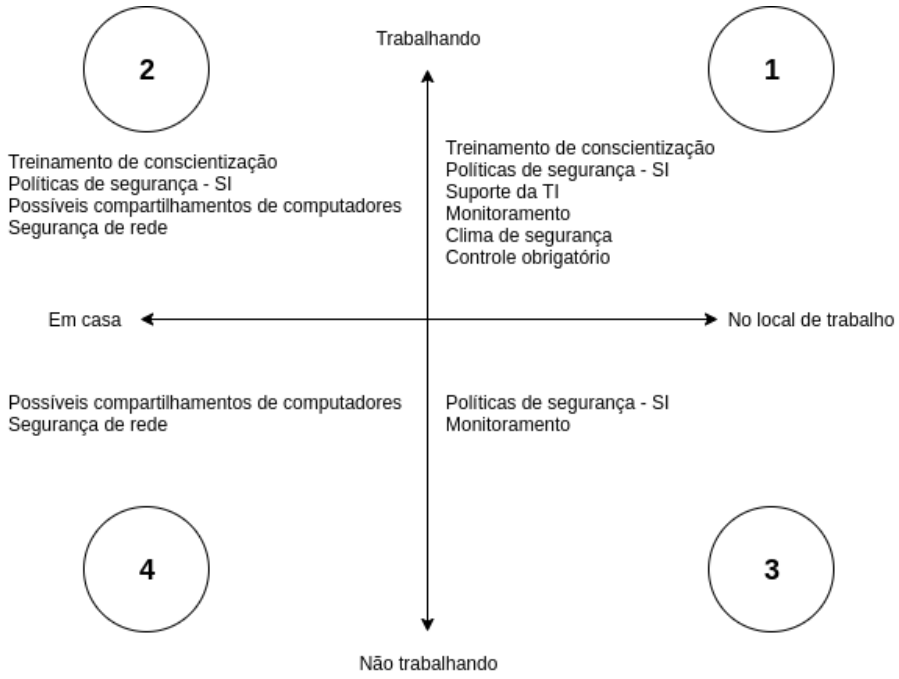
Embora usuários de terceira idade tenham consciência da importância da utilização de um software para segurança da informação, alguns acreditam que estão totalmente seguros apenas pelo fato de utilizá-lo. Sobretudo, ainda há inúmeras ameaças à privacidade e à segurança que permeiam as informações, além do fato de que nenhum software é cem por cento eficaz (BOOTHROYD, 2017). Uma outra vulnerabilidade apontada, é que adultos com 65 anos ou mais fazem pouco para protegerem-se em comparação a outros grupos de faixas etárias distintas (RAINIE et al, 2013).

2.2 CONTEXTO DE USO DAS TICs (TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO)

Ao estudar a segurança da informação dos usuários de Tecnologias da Informação e Comunicação, a dimensão de uso das TICs pode ser definida como o local em que o usuário se encontra ao utilizar a tecnologia, eis que este local pode ser em seu próprio lar, ou mesmo dentro da empresa a qual este usuário exerça suas atividades laborais (LI, 2015).

Concernentemente ao contexto de uso, este será relacionado se o usuário estiver fazendo uso recreativo ou profissional da tecnologia no momento, isto é, se este estiver exercendo atividades laborais no momento ou não, dentro ou fora da empresa ou do seu lar (LI, 2015).

FIGURA 1 – DIMENSÃO E CONTEXTO DE USO DAS TICs



Fonte: (LI, 2015), traduzido pelo autor.

O modo como o usuário se comporta no ambiente em que está inserido pode divergir, isto é, um usuário dentro de uma organização com políticas de segurança que estabeleça punições como, por exemplo, o encerramento do contrato de trabalho em caso de descumprimento das regras estabelecidas deve se comportar corretamente, o que pode não ocorrer dentro do ambiente doméstico, no qual inexiste uma política de conduta a ser seguida (MAYER et al, 2017).

Com base nisso, os usuários domésticos estão mais suscetíveis a vulnerabilidades de segurança da informação, pois decidem de forma independente como devem se proteger e, sobretudo, se devem ou como devem executar um comportamento de segurança (THOMPSON et al, 2017).

2.3 TEORIAS COMPORTAMENTAIS

As teoriais comportamentais são muito utilizadas em outras áreas do conhecimento como, por exemplo, a criminologia, a economia e a psicologia; sendo que atualmente as pesquisas em segurança da informação têm aplicado de forma ampla essas teorias (LI, 2015).

As teorias do comportamento mais adotadas nas pesquisas em sistemas de informação encontradas na literatura são as seguintes (OMIDOSU e OPHOFF, 2016):

1. “Teoria Do Comportamento Planejado (*Theory Of Planned Behavior* - TPB) - proposta por Ajzen, 1991;
2. Teoria Da Motivação Para A Proteção (*Protection Motivation Theory* - PMT) - proposta por Rogers, 1975;
3. Teoria Da Dissuasão (*Deterrence Theory* – DT) - proposta por Beccaria, 1963”.

Todavia, também existem outras teorias do comportamento: teoria da escolha racional, teoria da ação racionalizada, teoria social cognitiva, teoria do controle, teoria do desenvolvimento moral cognitivo, teoria dos tipos motivacionais de valores, modelo de aceitação de tecnologia, entre outras (OMIDOSU e OPHOFF, 2016). No contexto mais geral, existem diversas teorias de sistemas de informação[2] (LARSEN & EARGLE, 2015).

[2] Principais teorias de sistemas de informação: https://is.theorizeit.org/wiki/Main_Page

2.3.1. Teoria da Ação Racionalizada (*Theory of Reasoned Action* - TRA) - proposta por Fishbein e Ajzen (1975)

Essa teoria sustenta que a ação do indivíduo é determinada pela sua intenção comportamental, e enfatiza que essa intenção comportamental é influenciada pela combinação de dois fatores; segundo (LEE e CHAN, 2018), são eles:

1. “Normas subjetivas;
2. Atitude em relação a executar um dado comportamento.”

Este framework afirma que a adesão a um comportamento específico só pode ser influenciada indiretamente pelos dois fatores já mencionados; e que esses fatores auxiliam na elucidação do controle volitivo (ou da vontade do indivíduo) e também do controle do comportamento (LEE e CHAN, 2018).

2.3.2. Teoria do Comportamento Planejado (*Theory Of Planned Behavior* - TPB) - proposta por Ajzen, 1985

A *Teoria do Comportamento Planejado* faz parte da psicologia social, que é um ramo específico da psicologia, e defende que o comportamento dos indivíduos em um dado contexto é antecedido por uma intenção, que é influenciada por três fatores motivadores (LIU et al, 2019) e (HOWE et al, 2012), são eles:

1. “Atitude, que é a tendência do indivíduo em executar um dado comportamento;
2. Normas subjetivas, se referem à crença de que uma pessoa ou um grupo de pessoas irá ou irão aprovar o comportamento executado, isto é, uma visão social que o indivíduo tem sobre a aprovação ou não de sua conduta;
3. Controle Comportamental Percebido, diz respeito a quanto o indivíduo se autoconsidera capaz de executar um comportamento.”

O modelo da *Teoria do Comportamento Planejado* estende a *Teoria da Ação Racionalizada* e adiciona a percepção sobre o controle do comportamento como mais uma de suas variáveis preditoras, de modo que totaliza, portanto, um total de três variáveis preditoras (TAYLOR e TODD, 1995 *apud* SILVA, 2019).

2.3.3. Teoria Da Motivação Para A Proteção (*Protection Motivation Theory - PMT*), proposta por Rogers, 1975

A finalidade da *Teoria Da Motivação Para A Proteção* (PMT) é elucidar os efeitos do apelo ao medo no comportamento das pessoas, além de estudar a tomada de decisões das pessoas em ocasiões de risco (MADDUX e ROGERS, 1983).

Recentemente, pesquisadores têm utilizado a PMT no campo de Gestão de Segurança da Informação; todavia, nos estágios iniciais o apelo ao medo era utilizado principalmente na área de medicina (ZHU et al, 2018).

A pesquisa denominada "*Comparing three models to explain precautionary online behavioural intentions*" conduzida por (VAN SHAIK et al, 2017), por meio de uma *survey* e da aplicação de métodos estatísticos para descobrir a utilidade de teoria, concluiu que a PMT é uma teoria eficaz para predizer tipos distintos de comportamentos preventivos, além de afirmar que a *PMT* já foi amplamente testada para predizer intenções futuras ou explicar comportamentos ocorridos (VAN SHAIK et al, 2017).

Em síntese, a *Teoria da Motivação para a Proteção* defende que quando as pessoas se sentem suscetíveis em relação a ameaças que possam ter consequências graves, mas percebem que podem fazer algo para evitar e sentem-se preparadas para agir, elas se motivam a evitar a ameaça (RIPPETOE & ROGERS, 1987 apud FLOYD, PRENTICE-DUNN, & ROGERS, 2000).

A teoria sustenta que o apelo ao medo tem o potencial de alterar o comportamento dos usuários, estimulando seu temor interior. Deve-se buscar um ponto de equilíbrio no apelo ao medo dos usuários para que se tenha resultados satisfatórios na mudança de comportamento (SE-HOON, 2008 apud ZHU et al, 2018).

A *PMT* é uma teoria utilizada de forma isolada ou em combinação com outra teoria como, por exemplo, a teoria da *abordagem da ação racionalizada - reasoned action approach* – RAA, o *modelo de probabilidade de elaboração da persuasão - elaboration likelihood model* (ELM), *Teoria social cognitiva*, entre outras (JANSEN & VAN SCHAIK, 2017). Além do mais, essa teoria é vista em cerca de 40% dos estudos encontrados na literatura (OMIDOSU e OPHOFF, 2016).

Em um estudo realizado para verificar a eficácia do modelo da *Teoria da Motivação para a Proteção,* constatou-se que até 64% da variância no comportamento em segurança da informação pode ser explicado por esta teoria (JANSEN & VAN SCHAIK, 2017).

A teoria da motivação para a proteção faz menção a dois processos cognitivos: 1) Avaliação de ameaças e 2) Avaliação de enfrentamento às ameaças (JANSEN, 2015).

A avaliação de ameaças está associada ao processo de verificação da probabilidade e do impacto da ameaça; já o enfretamento a ameaças é o processo no qual o indivíduo planeja as ações de enfrentamento à ameaça (JANSEN, 2015).

Além disso, cada um dos dois processos cognitivos possui variáveis não diretamente observáveis associadas, conforme exemplificado a seguir (JANSEN, 2015):

TABELA 1 - PROCESSOS COGNITIVOS DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO E VARIÁVEIS NÃO DIRETAMENTE OBSERVÁVEIS ASSOCIADAS

Processos cognitivos	**Variáveis não diretamente observáveis associadas**
Avaliação de ameaças	1. Vulnerabilidade Percebida: vulnerabilidade percebida pelo indivíduo, isto é, se o indivíduo percebeu alguma ameaça que represente um risco a sua segurança; 2. Severidade Percebida: gravidade percebida pelo indivíduo.
Avaliação de enfrentamento a ameaças	1. Eficácia da Resposta: sensação do indivíduo sobre se a resposta fará surtir efeito relevante; 2. Autoeficácia: Crença pessoal sobre a autocapacidade para executar a resposta recomendada de enfrentamento; 3. Custo da resposta: Qual o custo para o indivíduo em executar a resposta recomendada; 4. Local de controle: Pode ser interno ou externo. Um sistema on-line de emissão de laudos médicos, por exemplo, é externo, pois a responsabilidade da privacidade de cada paciente a ser mantida é do hospital; 5. Normas Injuntivas: Normas que determinam a conduta sob a qual o indivíduo deve se pautar. 6. Normas Descritivas: Percepção de que outros estão ou não estão executando um comportamento específico; 7. Atitude: Sentimento pessoal, podendo este ser negativo ou positivo sobre executar um comportamento;

Fonte: (JANSEN, 2015) traduzido pelo autor.

Variáveis preditoras, no presente contexto, são aquelas que auxiliam na previsão do comportamento do usuário em segurança da informação. Uma variável preditora é mais suscetível a prever um dado comportamento se ela tiver um relacionamento mais forte com as intenções do usuário; para medir isso, é preciso realizar um questionário tendente a levantar as intenções desses usuários e executar os testes estatísticos apropriados (TSAI et al, 2016)

As variáveis preditoras do comportamento contidas nessa Teoria, que são as evidenciadas na Tabela 1 de autoria de (JANSEN, 2015) e traduzida pelo autor, são de utilidade notável; algumas variáveis preditoras são mais influentes do que outras. As variáveis: etnia, nível escolar, renda, e suscetibilidade a ameaças não são boas preditoras das intenções e comportamentos de segurança, porém outras variáveis preditoras como a idade, experiência prévia em internet, eficácia da resposta, suporte de segurança percebido, custo da resposta entre outros estão fortemente ligadas às intenções de segurança dos usuários (TSAI et al, 2016).

Isso significa que algumas dessas variáveis influenciam em maior grau o comportamento em segurança da informação dos usuários do que outras, isto é, elas correlacionam-se mais, possibilitando, dessa forma, predizer mais o comportamento (DUPUIS & CROSSLER, 2019).

2.3.4. Teoria Da Dissuasão (*Deterrence Theory* – DT) – proposta inicialmente por Beccaria, 1963

A Teoria da Dissuasão trata das sanções e punições como um meio para desencorajar uma conduta tida como inadequada, como por exemplo a invasão a um computador alheio, uma violação de dados ou uma violação a uma política de segurança estabelecida, entre outras condutas (CARTER et al, 2016).

Esta teoria afirma que o indivíduo, ao perpetrar uma conduta inadequada, tomará uma decisão racional, ponderando as sanções que poderá sofrer em decorrência da violação da conduta e os benefícios que essa violação proporcionará caso se concretize (CARTER et al, 2016).

A teoria preconiza que a quantidade de condutas delituosas praticadas por marginais relacionadas a crimes computacionais decrescerá em função da punição a ser aplicada e da certeza que a reprimenda recairá sobre o sujeito infrator (LI & MIKKO, 2011).

Ou seja, o ponto chave dessa teoria é que o indivíduo ao executar uma conduta delituosa, busca a majoração dos benefícios e a minoração dos custos (D'ARCY & HERATH, 2011).

2.4 SEGURANÇA DA INFORMAÇÃO

Segurança da informação significa tomar ações tendentes a prevenção e proteção das informações contra acesso não autorizado e também contra o seu comprometimento (NEOGY, 2017).

Conforme (WHITMAN e MATTORD, 2015), (DANTAS, 2011), (CHERDANTSEVA e HILTON, 2013) e (ARBABI e SHAJARI, 2019) os pilares da segurança da informação são três:

1. Confidencialidade: propriedade que assegura que a informação seja revelada ou disponibilizada apenas a indivíduos, processos, organizações ou entidades que estejam autorizadas a acessar tal informação (BECKERS, 2015).
2. Integridade: propriedade que assegura a completude e a acurácia dos dados; isto é, os dados que possuem essa característica são isentos de alterações não autorizadas ou não detectadas (BORITZ, 2005).
3. Disponibilidade: propriedade que cuida do tempo em que um serviço está em funcionamento; sendo, portanto, uma propriedade sempre desejável, uma vez que serviços indisponíveis são sempre causa de insatisfação (NEOGY, 2017).

Os pilares de segurança da informação são propriedades sempre desejáveis, todavia, com o aumento exponencial dos dados na web, que advém da adoção massiva dos indivíduos a sistemas digitais, o número de ataques digitais também aumenta, potencializando a chance de vítimas, aumentando a suscetibilidade a ataques de toda a rede e ameaçando as

propriedades tão desejáveis de confidencialidade, integridade e disponibilidade (BENDOVSCHI, 2015).

Para mitigar essa suscetibilidade, deve-se conscientizar o usuário em segurança da informação. Entretanto, a conscientização em segurança da informação na forma que vem sendo realizada não está funcionando a contento (BADA et al, 2015).

O ato de veicular avisos em demasia ao usuário pode trazer efeitos indesejados e provocar a evasão do usuário das boas práticas no comportamento em segurança da informação, que deixará de se preocupar com as ameaças digitais (BADA et al, 2015).

O comportamento do usuário é uma vulnerabilidade levada em conta pelo *European Telecommunications Standards Institute Group Specification* (ETSI GS, 2015), que elenca quatro categorias de vulnerabilidades:

1. Vulnerabilidades Comportamentais: são aquelas que podem ser atribuídas a um dado usuário, sendo importante discernir o comportamento adequado ou esperado do comportamento realmente praticado; visto poder haver um descuido ou até mesmo má-fé no tocante ao comportamento executado. O objetivo é realizar posteriormente um trabalho de conscientização e adequação do comportamento dos usuários (ETSI GS, 2015).
2. Vulnerabilidades de *Software*: são aquelas relacionadas às falhas existentes nos softwares, passíveis de serem exploradas por indivíduos com má-fé, abrindo brechas para que tais indivíduos possam conduzir ataques, provocando incidentes de segurança; vale ressaltar que essa vulnerabilidade é mais difícil de ser corrigida, pois trata-se de código de programação, cuja origem da falha se dá durante o processo de construção da ferramenta de software (ETSI GS, 2015).
3. Vulnerabilidades de Configuração: essa modalidade de vulnerabilidade diz respeito a fragilidade da configuração efetuada nas ferramentas de segurança, como por exemplo um firewall inadequadamente

configurado, políticas de segurança da informação não reforçadas ou barreiras físicas de segurança mal implementadas (ETSI GS, 2015).

4. Vulnerabilidades Gerais de Segurança (Técnica ou Organizacional)*:* são vulnerabilidades consideradas de mais alto nível, que provocam um efeito maior devido a sua natureza, por exemplo, as falhas ou mal funcionamento dos processos de segurança, ou das ferramentas técnicas de segurança (ETSI GS, 2015).

2.5 TRABALHOS RELACIONADOS

A pesquisa de (BOOTHROYD, 2017), realizada com idosos, evidenciou que o público de terceira idade confia a segurança de suas Informações a terceiros, recebendo suporte de técnicos e de softwares externos, o que os expõe mais a riscos de segurança da informação. A pesquisa contou com a participação de 31 voluntários, sendo quinze idosos e dezesseis adultos não idosos. As faixas etárias foram divididas em duas, sendo a primeira compreendendo pessoas de 18 a 29 anos e a segunda 65 a 88 anos. A pesquisa foi conduzida por meio de um documento de entrevista, contendo dezessete questões. Como método de análise qualitativa dos dados, a autora utilizou a análise temática. Foi utilizada uma análise qualitativa que preconiza a aplicação de seis etapas:

1. Organizar e preparar os dados para análise;
2. Ler e observar os dados para familiarizar-se;
3. Codificar e rotular grupos etários separadamente, para que os detalhes não obtidos no contexto mais amplo possam ser obtidos a partir dessa codificação etária feita de forma separada;
4. Agrupar códigos relacionados entre si em um mesmo tema;
5. Confirmar como os temas são definidos e representados;
6. Comparar os temas.

O que chamou a atenção nessa pesquisa foi o fato de que a pesquisadora utilizou o *teste exato de fisher* para o processo de comparação das faixas. Um achado foi identificar que os adultos mais velhos possuem aproximadamente o mesmo conhecimento do que os adultos mais jovem no que se refere a riscos em serviços de e-mail, mas que, todavia, demonstraram uma compreensão menos ampla dos riscos advindos de redes sociais como o Facebook.

A pesquisa de (VIANA, 2017), separou a amostra em cinco faixas etárias distintas, e identificou as vulnerabilidades mais críticas de segurança da informação enfrentadas pelo público de terceira idade, uma dessas vulnerabilidades está relacionada a fragilidade desse público em ataques baseados em *engenharia social* na utilização de senhas e credenciais. Essa pesquisa utilizou a análise fatorial exploratória e a análise fatorial confirmatória para produção dos fatores de segurança da informação utilizados na pesquisa. O pesquisador utilizou quatro dimensões de mensuração e uma escala *likert* com onze pontos (zero a dez) e 32 itens de mensuração numa etapa quantitativa. Foi utilizado o método de Análise de Variâncias (*ANOVA*) para comparação das faixas etárias, uma vez que este é o teste paramétrico adequado para comparação de três ou mais populações por meio da análise das variâncias amostrais e, nesse caso o trabalho considerou 5 grupos etários. Também foi utilizado o teste de *Kruskal-Wallis*, que é um teste alternativo ao *ANOVA* para mais de duas amostras independentes, no sentido de verificar se são oriundas de uma mesma população, na hipótese em que os pressupostos de normalidade da distribuição e a homocedasticidade dos dados não forem atendidos. Além disso, também foram utilizados outros testes estatísticos. O tamanho dessa amostra foi de 312, sendo 239 respondentes on-line e 73 offline, em papel. O que chamou a atenção nessa pesquisa foi que para verificar se havia diferença nas amostras obtidas entre os questionários em papel e o on-line o pesquisador utilizou o teste *Mann-Whitney,* que é o teste apropriado na ocasião do não atendimento do pressuposto da normalidade da distribuição dos dados, e é considerado um teste não paramétrico utilizado para verificar se duas amostras independentes são oriundas de uma mesma população, sendo um teste alternativo ao teste t de *Student*. Os *softwares* para

testes estatísticos utilizados nessa pesquisa foram o R e o *SPSS*. Identificou também que a maior parte de uso da grande rede se dá voluntariamente (apenas pela vontade de utilizá-la) e não por compulsoriedade ou necessidade.

A pesquisa de (MCGILL & THOMPSON, 2018), realizada na Austrália sobre os efeitos de gênero sobre o comportamento em segurança da informação revelou que as mulheres exibem níveis significativamente mais baixos de comportamento de segurança do que os homens. Além disso, também revelou que em muitos casos as percepções e comportamentos individuais também variam de acordo com o sexo. Para isso o estudo utilizou os seguintes itens de mensuração:

1. Ter backups recentes;
2. Ter instalado software de segurança;
3. Usar software de segurança;
4. Habilitar atualizações automáticas de software;
5. Proteger dispositivo com senhas;
6. Ter um firewall habilitado na rede residencial.

O estudo identificou que os homens executam muito mais as atividades acima do que as mulheres.

A pesquisa de (JANSEN, 2015), estudou o comportamento em segurança da informação no contexto de uso de "*online banking"* sob o ponto de vista da *Teoria da Motivação para a Proteção*, utilizou quatro variáveis de controle com o intuito de excluir os seus efeitos sobre os resultados, são elas: 1) experiência na internet; 2) hábito; 3) variáveis demográficas e 4) vitimização de fraudes bancária *on-line*; e concluiu que apenas as ferramentas de segurança não são suficientes para garantir a salvaguarda dos dados contra violação, e que o comportamento do usuário também é essencial.

A pesquisa de (TSAI et al, 2016) concluiu que as covariáveis etnia, nível escolar, renda, e suscetibilidade à ameaças não estão correlacionados de maneira estatisticamente significativa com as intenções de segurança e que

alguns outros preditores como a idade, experiência prévia em internet, eficácia da resposta, suporte de segurança percebido, custo da resposta entre outros estão fortemente ligados às intenções de segurança dos usuários. O pesquisador elaborou uma matriz de correlação para verificar a correlação entre as variáveis e covariáveis e as intenções de segurança. Para a coleta dos dados, a pesquisa utilizou o Amazon's MechanicalTurk (MTurk; http://www.mturk.com) e obteve 988 respondentes, utilizando uma escala likert de cinco pontos para as questões. Para cada variável latente da *Teoria da Motivação para a Proteção* foram associados alguns itens de mensuração.

A pesquisa de (MCCORMAC et al, 2017), num contexto organizacional, concluiu que adultos mais velhos, com mais de 35 anos, são mais conscientes sobre segurança da informação em comparação aos mais jovens, talvez pelo fato de os jovens terem mais apetite a risco do que as pessoas mais velhas, se comportando mais arriscadamente nos aspectos de segurança da informação. O estudo utilizou uma escala de likert de cinco pontos, sendo zero um indicativo de que a atividade de risco nunca é executada e cinco sendo um indicativo de que a atividade de risco é executada diariamente. Alguns itens de mensuração foram: compartilhamento de senhas com amigos e colegas; uso da mesma senha para múltiplos sites e clicar em *links* recebidos por e-mail. Essa pesquisa identificou que os empregados dentro de organizações costumam relaxar a segurança das informações uma vez que percebem um suporte técnico ativo que resolverá eventuais incidentes que possam ocorrer decorrentes da sua má-conduta na internet, devolvendo a responsabilidade da segurança para seus empregadores e para a sua gestão. Também identificou que grande parte dos participantes necessitam de conhecimentos em segurança da informação e possuem lacunas no que se refere a habilidades nessa área.

A pesquisa de (VAN BAVELA et al, 2019), com uma amostra de 2024 respondentes, teve o objetivo de explorar o efeito das notificações e avisos no comportamento em segurança, sob a ótica da *Teoria da Motivação Para a Proteção*. Nessa pesquisa, os autores identificaram que uma mensagem de enfrentamento (ou *coping message*), aconselhando o usuário sobre como reduzir a sua exposição a riscos, foi significamente mais eficaz quando

comparado ao apelo ao medo (*threat appeal*), isoladamente. O estudo identificou que o apelo ao medo levou os participantes da pesquisa a um maior percentual de desistência logo no início do experimento, sendo responsável por 65.3% da evasão. A combinação de mensagem de enfretamento com mensagem de apelo ao medo foi responsável por 61.4% da evasão. O experimento consistiu em realizar uma compra simulada (*mock*) on-line de um produto. O autor também afirmou que a literatura tem dado considerável atenção no apelo ao medo, quando uma abordagem interessante deveria ser a de buscar proposições para se testar novas formas de enfrentamento à ameaças.

A pesquisa de (JANSEN & VAN SCHAIK, 2017), conduzida por meio de uma "*survey*" avaliou três modelos para o estudo do comportamento preventivo na internet: 1) *Teoria da Motivação para a Proteção*; 2) *Teoria da Ação Racionalizada* e 3) *Modelo integrado entre as duas teorias anteriores*. Nesse estudo, os pesquisadores avaliaram a significância estatística de cada variável preditora dessas teorias. Revelaram que o modelo da *Teoria da Motivação para a Proteção* explicou 64% da variância no comportamento em segurança da informação e que o modelo da *Teoria da Ação Racional* explicou 63% da variância no comportamento em Segurança. Concluíram que ambas as teorias são ótimas preditoras do comportamento em segurança. Para a análise de resultados, foi utilizado o *SmartPLS*, com a finalidade de extrair o coeficiente de determinação dos modelos e determinar a significância dos caminhos (*paths*) representado pela conexão das variáveis preditoras com a variável latente na forma de equação estrutural.

A presente pesquisa contou com duas partes, sendo a primeira quantitativa denominada de "questionário" e a segunda qualitativa denominada "observação". A primeira etapa verificou o comportamento em segurança da informação dos usuários sob a ótica da *Teoria da Motivação para a Proteção*; a segunda etapa, a de observação, em que foram conduzidas sessões de observação, teve o propósito de aferir o conhecimento dos voluntários sobre o tema abordado a partir da observação de algumas ações executadas pelos participantes da pesquisa. A partir dessas duas etapas, o pesquisador propôs

algumas recomendações em segurança da informação com base nas situações verificadas.

Na presente pesquisa foi considerada a faixa etária de terceira idade; o público idoso aqui considerado foi de setenta anos ou mais de idade, sendo por isso um diferencial. A etapa quantitativa do estudo concluiu que as variáveis da *PMT* mais negligenciadas foram “Autoeficácia”, “Experiência prévia com riscos de segurança” e “Suporte de Segurança Percebido”, indicando que o público de terceira idade possui dificuldades para desempenhar tarefas relacionadas a segurança da informação e que tendem a necessitar de suporte para realizar atividades de segurança, além de acreditarem que nunca foram alvo de algum ataque de malware.

Já a etapa qualitativa demonstrou que grande parte dos usuários necessitam de conhecimento sobre conceitos básicos em segurança da informação, tendo dificuldades na execução de algumas atividades de segurança, em especial as atividades de verificação da situação de suas ferramentas de segurança (antivírus, *firewall*) e de definição de senhas fortes.

Além de terem sido encontrados poucos trabalhos que tratam do tema de segurança da informação de usuários domésticos idosos sob o ponto de vista da Teoria da Motivação para a Proteção, o autor não encontrou outras pesquisas que abordassem um estudo dessa natureza com o uso de uma metodologia mista, qualitativa e quantitativa e principalmente com idosos de setenta anos ou mais de idade e no contexto do Brasil.

3 METODOLOGIA

Este capítulo apresenta os aspectos da metodologia científica que serão abordados na presente pesquisa bem como as etapas e limitações do método de pesquisa.

A metodologia científica retrata o estudo dos métodos de pesquisa e procura adotar seis aspectos: abordagem de pesquisa, posição epistemológica, método de pesquisa, finalidade, técnica de coleta de dados e técnica de análise de dados (FILIPPO et al, 2011).

A presente pesquisa considerou uma abordagem mista, qualitativa e quantitativa. Na pesquisa qualitativa, o pesquisador baseia seus estudos a partir da interpretação do mundo real (OLIVEIRA, 2008). Já a pesquisa quantitativa lida com a quantificação e análise de variáveis com o intuito de obter resultados (APUKE, 2017).

Para a aplicação do método, a presente pesquisa levou em conta uma das diretrizes evidenciadas por (LI, 2015), em sua tese de doutorado, que é a de analisar o contexto; para tanto, o pesquisador selecionou usuários no contexto doméstico, isso significa que outros contextos não foram considerados.

Como trata-se de pesquisa exploratória cujo objetivo é apresentar novas evidências, ideias ou clarificar algo, e até mesmo concluir que algo não existe, foram conduzidos testes com um grupo específico de usuários, a fim de identificar eventuais dificuldades no uso e oportunidades para elaborar recomendações apropriadas.

Considerando que a maioria das pesquisas sobre o tema são eminentemente quantitativas, conforme evidencia (OMIDOSU e OPHOFF, 2016); o pesquisador não encontrou orientações para que os testes fossem ou não conduzidos em ambiente controlado em relação a etapa qualitativa.

Há, todavia, orientação de que testes com participantes possam ocorrer em dois lugares (CYBIS et al, 2010):

1. em laboratório; ou

2. ambiente real de trabalho.

Como não foi possível conduzir os testes nos ambientes mencionados (1 e 2) em razão da COVID-19, optou-se por realizar por meio de vídeo conferência, e o ambiente para a execução das ações foi o próprio domicílio do usuário, remotamente.

3.1 ETAPAS DO MÉTODO

1. Determinação dos perfis dos usuários participantes da pesquisa;
2. Definição da teoria de avaliação comportamental aplicada;
3. Elaboração do questionário;
4. Aplicação do questionário e análise;
5. Definição dos parâmetros de segurança da informação avaliados na etapa de *Observação de usuários*;
6. Seleção do *site* para execução das tarefas;
7. Execução da pesquisa com grupo de terceira idade com o método etnográfico;
8. Análise dos resultados e discussão dos resultados.
9. Elaboração de recomendações.

3.1.1 Determinação dos perfis dos usuários participantes da pesquisa

O perfil selecionado foi o usuário idoso, com 70 anos ou mais. Para definição da faixa etária foram usados os mesmos critérios do CETIC.br na definição das faixas etárias da última pesquisa TIC domicílios de 2018, porém com algumas adaptações; apesar do CETIC.br, do IBGE e o Estatuto do Idoso (BRASIL, Lei n° 10.741, 2003) adotarem a faixa de 60 anos ou mais para o usuário idoso, para fins dessa pesquisa foram considerados idosos apenas os respondentes com idade igual ou superior a 70 anos, considerando dois aspectos, sendo o primeiro que o envelhecimento ocasiona o declínio de funções cognitivas importantes para o bom uso dessas tecnologias e o segundo é que pessoas nessa faixa etária já estão aposentadas ou na iminência de se aposentar, e com isso o uso do computador no contexto

doméstico fica mais evidente (PAK, PRICE, & THATCHER, 2009), (BRASIL, 1988) e (BRASIL, 1991).

Foi utilizado também o critério de tempo de experiência com internet de dois anos ou mais de uso para todos os usuários, a fim de obter participantes com domínio das ferramentas digitais.

3.1.2 Definição da teoria de avaliação comportamental aplicada;

A teoria selecionada para o presente estudo foi a Teoria da Motivação para a Proteção (*PMT*). O motivo para essa seleção foi o fato de que os pesquisadores (JANSEN & VAN SCHAIK, 2017) conduziram um estudo por meio de uma *survey* que avaliou três modelos para o estudo do comportamento preventivo na internet: 1) Teoria da Motivação para a Proteção; 2) Teoria da Ação Racionalizada e 3) Modelo integrado entre as duas teorias anteriores. Nesse estudo, os pesquisadores avaliaram a significância estatística de cada variável preditora dessas teorias. Revelaram que o modelo da Teoria da Motivação para a Proteção explicou 64% da variância no comportamento em segurança da informação.

3.1.3 Elaboração do questionário

Esse questionário teve o objetivo de auxiliar na compreensão do comportamento em segurança da informação dos usuários à luz da Teoria da Motivação para a Proteção. O questionário foi composto por quatrorze questões fechadas, sendo quatro relativas ao perfil dos voluntários e dez relativas aos itens de mensuração da teoria utilizada. As respostas de doze usuários foram coletadas presencialmente, antes da pandemia de COVID-19 e a dos outros oito voluntários foram coletadas de forma on-line.

3.1.4 Aplicação do questionário

Foi aplicado um questionário pela internet através do *Google Forms*. O método utilizado para disseminação do formulário foi o *snowball* (bola de neve),

que consiste em acessar um respondente, que tem acesso a outro respondente, que acessa um terceiro e assim por diante (VOGT, 1999).

Para aumentar o número de participantes, optou-se por aplicar o questionário também de forma presencial, onde foram convidadas mais pessoas; para tanto, o pesquisador selecionou os respondentes do seu círculo social, amigos, conhecido de amigos, e outras pessoas que utilizam a internet e que se disponibilizaram a participar da pesquisa.

O questionário teve 26 respondentes. Após a limpeza dos dados, restaram vinte respondentes. O questionário submetido aos respondentes que apresentavam ocorrência de valores faltantes para alguma resposta não foram considerados; também não foram considerados respondentes que não utilizavam a internet.

3.1.5 Definição dos parâmetros de segurança da informação avaliados

Para a definição dos parâmetros de segurança avaliados, o pesquisador se baseou em três textos:

1. Indicadores de vulnerabilidades comportamentais definidos pelo *European Telecommunications Standards Institute Group Specification* (ETSI GS, 2015).
2. Estudo de (HOWE, *et al, 2012)*, que relaciona os comportamentos estudados por (LEE et al 2005).
3. Norma *International Organization for Standardization* (ISO 27002, 2013).

A tabela 2 a seguir ilustra as ações de segurança da informação selecionadas.

TABELA 2 - AÇÕES DE SEGURANÇA DA INFORMAÇÃO SELECIONADAS

Ações de segurança da informação	
1	Analisar ícone de cadeado fechado que é indicado pelo navegador;
2	Analisar prefixo de *HTTPS*;
3	Verificar certificados de segurança;
4	Analisar nome de domínio;
5	Verificar *firewall*;
6	Navegar anônimo;
7	Realizar *logout* após o término das atividades;
8	Mover cursor do *mouse* sobre *url* antes de clicar;
9	Identificar conteúdo *phishing;*
10	Definir senha forte;

Fonte: (ISO 27002, 2013), (LEE *et al*, 2005 apud HOWE *et al,* 2012*)* e (ETSI GS, 2015), adaptado pelo autor.

3.1.6 Seleção do site para execução das tarefas na etapa de observação de usuários;

Para a seleção do *site* em que os participantes executaram as tarefas, também foi levado em conta a pesquisa empreendida pelo CETIC.br, relativamente à atividade realizada na internet pelos Brasileiros em seus domicílios. Verificou-se que os usuários usam a internet principalmente para realizar atividades de comunicação, com o uso de serviços de mensagens (90%) e redes sociais (77%). Além disso, também foi frequente a realização de atividades culturais na rede, como assistir a vídeos e ouvir músicas, ambas realizadas por 71% dos usuários (CETIC.br, 2017).

A quantidade de usuários selecionados para realização da fase observacional foi definida em razão do estudo de (MALTERUD at al, 2016) que

afirma que um princípio comumente estabelecido para determinar o tamanho da amostra em um estudo qualitativo é que N deve ser suficientemente grande e variado para elucidar os objetivos do estudo (KUZEL, 1999, & MARSHALL, 1996, & PATTON, 2015 *apud* MALTERUD et al, 2016).

A quantidade definida é suficiente porque foram selecionados participantes com características heterogêneas, o que possibilitou o atingimento dos objetivos da pesquisa para o perfil estudado. Para exemplificar, a pesquisa de Dhamija (DHAMIJA at el. 2006), com 22 pessoas, concluiu que os participantes careciam de conhecimentos críticos sobre informática e segurança (por exemplo, sete nunca haviam ouvido falar de *phishing*[3] antes), e que participantes mais experientes ainda podiam ser enganados por manobras visuais.

3.1.7 Execução da pesquisa com grupo de terceira idade com o método etnográfico.

A pesquisa foi desenvolvida a partir de duas fases:

1. Questionário;
2. Observação de usuários.

Primeiramente foi aplicado um questionário para avaliar as variáveis da teoria selecionada**.** O objetivo do questionário foi avaliar as variáveis consideradas pelos participantes que influenciam na sua tomada de decisão em relação ao seu comportamento na internet.

Para a elaboração do questionário, foi extraída uma questão para servir como item de mensuração para cada variável considerada na teoria da

3 É o ato de tentar induzir os clientes a divulgar suas informações de segurança pessoal; seus números de cartão de crédito, detalhes da conta bancária ou outras informações confidenciais, mascarando-se como empresas confiáveis em um e-mail (JAHANKHANI et al., 2014).

motivação da proteção, constante da pesquisa de (TSAI et al., 2016), de forma a tornar o roteiro enxuto e viabilizar as entrevistas considerando o tempo disponível; vale ressaltar que embora a redução de variáveis acarrete na diminuição da capacidade explicativa do modelo, isso não trará prejuízo aos testes, já que na presente pesquisa são verificadas apenas as variáveis associadas ao comportamento dos voluntários idosos com setenta anos ou mais de idade no Brasil que são negligenciadas, com o intuito de estudar como essas variáveis se associam aos perfis estudados.

A *observação de usuários* teve o objetivo de avaliar se os usuários se atentam para aspectos importantes de segurança da informação ao navegar na internet. Para avaliar a parte prática, foi empreendido o método de *observação direta*. A *observação direta* é uma técnica relevante para investigar habilidades e práticas no meio social e reconhecer as ações e as atitudes coletivas na vida social. É buscar a compreensão de aspectos como diferenças sociais, culturais e históricos (ROCHA e ECKERT, 2008).

3.1.8 Análise dos dados e discussão dos resultados.

Nessa etapa buscou-se elucidar as questões relacionadas a etapa de questionário e de observação, baseando-se nos resultados obtidos e nos pontos mais importantes identificados.

Na etapa de *observação dos usuários* foram avaliados diversos fatores, como por exemplo, a capacidade dos participantes em concluir ou não as tarefas, além do tempo transcorrido na execução.

3.1.9 Elaboração de recomendações;

Após análise e comparação dos resultados obtidos durante a *observação dos usuários*, foram criadas recomendações em segurança da informação, considerando aspectos comportamentais da *Teoria da Motivação para a Proteção* da pesquisa "*Understanding online safety behaviors: A protection motivation theory perspective*" (TSAI et al, 2016). Espera-se que

essas recomendações contribuam para redução das ocorrências de violação de dados em segurança da informação e para a educação dos usuários.

4. PREPARAÇÃO E EXECUÇÃO DA PESQUISA

Este capítulo apresenta as avaliações realizadas sob a ótica da *Teoria da Motivação para a Proteção*, com o objetivo de verificar quais são os comportamentos em segurança da informação que mais são negligenciadas por meio da etapa de *Questionário;* além disso, também qualifica o conhecimento dos voluntários em matéria de segurança da informação por meio da etapa de *Observação de usuários*.

4.1 Preparação da Pesquisa

4.1.1 Elaboração do material utilizado durante a sessão

Como material de apoio para os testes, foram desenvolvidos:

1. um questionário composto, em sua maior parte, por perguntas fechadas, voltadas para identificar o perfil do voluntário e para coletar as informações de construtos da Teoria da Motivação para a Proteção por meio dos itens de mensuração;
2. Uma lista de ações a serem executadas pelos participantes em um site selecionado pelo pesquisador, com o objetivo de registrar as principais dificuldades dos participantes no tocante aos aspectos práticos de segurança.

Os modelos do questionário e da lista de ações que foram executadas pelos participantes na etapa de *Observação* estão disponíveis no APÊNDICE 2 e no APÊNDICE 3, respectivamente.

4.1.2 Preparação do ambiente e execução

Na primeira parte da pesquisa, que foi qualitativa, foi aplicado um questionário como instrumento para a coleta das informações, com a finalidade de realizar um levantamento do perfil dos participantes e de avaliar as variáveis

da teoria da motivação para a proteção que mais se relacionam com os estímulos para a tomada de decisão dos usuários em segurança da informação.

Na segunda etapa da pesquisa, que foi qualitativa, foi feita a *Observação de usuários* utilizando o método etnográfico; foi necessária a preparação do ambiente no qual as interações ocorreram. Foi instalada a ferramenta "*obsstudio*[4]" no computador do pesquisador com o objetivo de capturar as imagens da tela em tempo real para posterior estudo; além disso, foi utilizado o *Google Meet* para iniciar uma sala de reunião por vídeo conferencia com os usuários que participaram da pesquisa.

Para os participantes que optaram por realizar as ações por meio de um *smartphone,* foi necessário a instalação dos aplicativos denominados *Google Meet* e *Google Chrome*, ambos localizados na *Play Store* do *Android*; para os usuários que optaram por executar as ações por meio de um computador *desktop* ou *notebook*, foi necessário apenas a instalação do *Google Chrome*, já que para acessar uma sala de videoconferência por meio do *Google Meet* em um computador *desktop* não é necessário a instalação de um aplicativo do tipo cliente.

Antes e durante o processo de teste com os usuários, o pesquisador utilizou as etapas a seguir como forma de organização:

Antes da videoconferência:

1. Pesquisador entrou em contato com os participantes por meio de telefone e redes sociais para explicar a pesquisa e pedir participação.
2. Foi enviada uma mensagem para a conta de e-mail dos voluntários que aceitaram a participar da pesquisa com o termo de consentimento para

[4] Link para ferramenta *obsstudio*: https://obsproject.com/pt-br/download

assinatura bem como o endereço virtual da sala de reunião no Google Meet.

Durante a videoconferência:

1. Após estabelecida a videoconferência, os usuários foram informados de que os dados de cunho pessoal não são compartilhados.
2. Foi registrado o nome, a idade, a profissão e escolaridade do participante.
3. Foi apresentada a lista das ações de segurança da informação e de que não há consequências caso a atividade não seja concluída.
4. Os usuários foram informados que as atividades são cronometradas.
5. Os usuários foram informados de que o pesquisador não poderia interferir nas ações enquanto elas estivessem sendo executadas.
6. Foram registrados dados dos testes em tempo real, como por exemplo: comentários dos usuários, dúvidas, questionamentos, sensações, reclamações, impressões sobre o teste, tempo que o usuário levou para terminar a tarefa e se conseguiu concluir ou não a tarefa.
7. Foi solicitado ao usuário o compartilhamento da tela do computador ou do celular.
8. Foi solicitado ao usuário para acessar o *YouTube*.
9. O usuário foi questionado sobre o que significava cada uma das 10 ações. Para as tarefas em que o usuário conseguiu compreender, foi solicitado a executar cada uma delas. Para as ações em que o usuário não soube responder, o campo de conclusão da tarefa foi rotulado como “Não aplicável” ou “N/A”, de forma a melhor representar a realidade.
10. Os usuários foram questionados sobre o que acharam do teste.

4.1.3 Definição das perguntas do questionário

O questionário teve o objetivo de levantar o perfil dos voluntários e coletar informações sobre o comportamento dos usuários em segurança da informação. Nesta seção são apresentados os detalhes da seleção das questões.

O questionário foi dividido em duas seções, sendo a primeira relacionada ao levantamento de perfil dos voluntários e a segunda para a coleta das informações sobre o comportamento em segurança da informação, sob a ótica da *Teoria da Motivação para a Proteção*.

Para avaliar a relação das variáveis da *Teoria da Motivação para a Proteção* com as intenções de segurança dos usuários e idosos, o pesquisador selecionou algumas questões baseadas no estudo quantitativo realizado por (TSAI et al, 2016).

Por exemplo, para avaliar a variável não diretamente observável denominada autoconfiança no enfrentamento às ameaças, (TSAI et al, 2016) utilizou afirmações a serem quantificadas pelos participantes da pesquisa em uma escala *likert* de cinco pontos; as questões foram:

1. “Sinto-me a vontade tomando medidas para salvaguardar meu computador doméstico principal”;
2. “Tomar medidas de segurança necessárias está inteiramente sob o meu controle”;
3. “Eu tenho os recursos e o conhecimento para tomar medidas de segurança necessárias”;
4. “Tomar medidas de segurança é fácil” e;
5. “Eu sinto-me estressado quando penso sobre questões de segurança on-line”.

Vale ressaltar que todas essas são perguntas são itens de mensuração associadas a variável não diretamente observável denominada *autoeficácia*, conceito similar ao de *autoconfiança* (BARBER, 2008).

Baseado nisso, o pesquisador selecionou para o presente estudo um item de mensuração associado a cada variável não diretamente observável, para avaliar quantitativamente a influência da idade do usuário nesses comportamentos.

Essas afirmações foram elaboradas de forma que pudessem ser respondidas em uma escala *likert* com cinco alternativas, vejamos:

1. Discordo totalmente;
2. Discordo parcialmente;
3. Não sei responder;
4. Concordo parcialmente;
5. Concordo totalmente.

Para melhor exemplificar, é possível observar através da Tabela 3, do estudo de (TSAI et al, 2016), por meio da matriz de correlação, que algumas variáveis têm um peso maior do que outras nas intenções de segurança dos usuários. A *correlação de Pearson*, mostra que as variáveis etnia, escolaridade, renda e susceptibilidade a ameaças não estão relacionadas de forma estatisticamente significativa com as intenções de segurança dos usuários. Já as variáveis: gênero, idade, autoeficácia, eficácia da resposta, entre outras, estão relacionadas com significância estatística às intenções de segurança dos usuários (*$p < 0,05$, significando evidencia moderada e **$p < 0.01$, significando evidencia muito forte sobre o grau de correlação exibido na tabela). Cabe frisar que a pesquisa referenciada demonstra que a idade possui relação com as intenções de segurança dos usuários.

TABELA 3 - MATRIZ DE CORRELAÇÃO DAS VARIÁVEIS DE PERFIL (GÊNERO, IDADE, ETC.) E DAS VARIÁVEIS DA TEORIA DA MOTIVAÇÃO PARA A PROTEÇÃO

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Intenções de Segurança	1														
2	Gênero	0.07*	1													
3	Etnia	0	-0.03	1												
4	Idade	0.09**	0.17**	0.11**	1											
5	Escolaridade	-0.04	0.06	-0.04	0.03	1										
6	Renda	0.01	0.01	.06	.09**	0.20**	1									
7	Ameaça Percebida	0.26**	0.20**	-0.01	0.11**	0.04	-0.01	1								
8	Suscetibilidade à ameaça	-.04	.08*	-0.06	0.20**	-0.01	0.02	0.05	1							
9	Experiência prévia com perigos de segurança	0.11**	0.02	-0.04	0.12**	0.01	-0.02	0.14**	0.35**	1						
10	Autoconfiança no enfretamento	0.26**	-0.19**	0.04	-0.13**	-0.02	-0.03	0.12**	-0.44**	-0.16**	1					
11	Eficácia da resposta	0.46**	-0.01	0.06	0.01	-0.03	-0.02	0.21**	-0.22	0.15**	0.31**	1				
12	Normas subjetivas	0.28**	0.11**	0.03	0.10**	-0.03	0.01	0.16**	0.15**	0.11**	-0.01	0.23**	1			
13	Custo da resposta	-0.35**	0.05	-0.04	-0.02	-0.02	-0.04	-0.11**	0.37**	0.11**	-0.50**	-0.34**	-0.07**	1		
14	Hábito em Segurança	0.53**	-0.06	0.02	0.06	0	0	0.16**	-0.26**	-0.05	0.58**	0.44**	0.13**	-0.49**	1	
15	Responsabilidade Pessoal	0.43**	0.05	0.04	0.15**	-0.01	0.02	0.20**	-0.06	.07*	0.24**	0.39**	0.27**	-0.26**	0.35**	1
16	Suporte de Segurança Percebido	0.26**	-0.11**	0.08*	-0.08*	0.06	0.04	0.11**	-0.14**	0.03	0.35**	0.51**	0.19**	-0.28**	0.38**	0.25**

Notas: *p < .05 (evidencia moderada), **p < .01 (evidencia muito forte).

Fonte: (TSAI et al, 2016), traduzido pelo autor.

Dessa forma, na presente pesquisa foi utilizado instrumento de mensuração semelhante à do estudo conduzido por (TSAI et al, 2016), entranto, o principal objetivo aqui foi avaliar as variáveis mais negligenciadas pelo público de terceira idade.

Foram elaboradas dez questões para a composição do questionário. Cada uma dessas questões atuou como um item de mensuração. Os itens de mensuração estão associados às variáveis da qual se efetuou a análise, a tabela 4 demonstra essa relação:

TABELA 4 - QUESTÕES ELABORADAS E VARIÁVEIS ANALISADAS

Questão do questionário	**Variável medida**
1. Eu troco as minhas senhas com frequência	Intenções de Segurança
2. Um vírus pode ser prejudicial	Severidade da Ameaça
3. As minhas chances de ser infectado por vírus são altas	Suscetibilidade à ameaça
4. Minhas informações pessoais já foram violadas	Experiências passadas com riscos de segurança
5. Considero fácil tomar as medidas de segurança da informação necessárias	Autoconfiança no enfrentamento a ameaças (autoeficácia)
6. Acredito que um software de proteção possa ser útil para detectar e remover vírus	Eficácia da resposta
7. Acato a opinião das pessoas do meu círculo social sobre os cuidados que devem ser tomados ao conversar com desconhecidos na internet ou tomar outras medidas de segurança da informação.	Normas subjetivas
8. Acredito que softwares para proteção e segurança possam causar problemas em outros programas no meu computador.	Custo da resposta
9. Tenho o hábito de tomar medidas de proteção na internet	Força do hábito
10. Consigo instalar softwares de proteção mesmo não havendo ninguém para me ensinar	Suporte de segurança percebido

Fonte: Autor, adaptado de (TSAI et al, 2016).

4.2 Execução da pesquisa

4.2.1 Questionário

No questionário aplicado, o pesquisador utilizou variáveis na escala qualitativa, sendo categóricas e ordinais. Foram criadas variáveis na escala de *likert* (discordo parcialmente, discordo totalmente, não sei responder, concordo parcialmente e concordo totalmente).

No questionário on-line, houve a ocorrência de valores faltantes (*missing values)*, uma vez que todas as questões foram elaboradas de forma que não fosse exigida resposta obrigatória no instrumento de coleta.

Para solucionar a ocorrência de valores faltantes (*missing values)*, o pesquisador teve quatro opções:

1) substituir os valores pela média dos dados;
2) utilizar o método de imputação múltipla - multiple imputation (RANGEL, 2013);
3) utilizar a técnica de expectativa-maximização - expected maximization (DEMPSTER et al, 1977); e
4) descartar os itens obtidos.

O pesquisador optou por descartar os itens com valores faltantes (*missing values)*.

Os respondentes no contexto presencial durante a etapa de aplicação de *questionário* foram abordados em interações pessoais, antes da pandemia de COVID-19, os quais foram convidados a responder o instrumento de coleta, independentemente de mostrar interesse ou preocupação com o tema.

No contexto presencial durante a aplicação do questionário, realizado antes da pandemia de COVID-19, não houve a ocorrência de valores faltantes (*missing values),* mas houve no contexto on-line*.*

4.2.1.2 Estatística descritiva dos resultados obtidos

Nesta seção, são explorados os dados que descrevem as variáveis da *Teoria da Motivação para a Proteção*, no tocante à segurança da informação, que mais pesam na tomada de decisão do usuário em adotar ou não medidas protetivas na internet.

O questionário teve 26 respondentes idosos com 70 anos ou mais. Após a limpeza dos dados, restaram vinte respondentes.

TABELA 5 - FREQUÊNCIA RELATIVA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 1 A 5)

	Grupo Etário - Terceira Idade				
	Discordo Totalmente	Discordo Parcialmente	Não sei responder	Concordo Parcialmente	Concordo Totalmente
Eu troco as minhas senhas com frequência.	40,00%	25,00%	0,00%	20,00%	15,00%
Um vírus pode ser prejudicial.	0,00%	0,00%	0,00%	10,00%	90,00%
As minhas chances de ser infectado por vírus são altas.	15,00%	45,00%	15,00%	15,00%	10,00%
Minhas informações pessoais já foram violadas.	55,00%	20,00%	20,00%	5,00%	0,00%
Considero fácil tomar as medidas de segurança da informação necessárias.	45,00%	25,00%	20,00%	5,00%	5,00%

Fonte: levantamento de dados.

TABELA 6 - FREQUÊNCIA RELATIVA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 6 A 10)

	Grupo Etário - Terceira Idade				
	Discordo Totalmente	Discordo Parcialmente	Não sei responder	Concordo Parcialmente	Concordo Totalmente
Acredito que um software de proteção possa ser útil para detectar e remover vírus.	5,00%	10,00%	15,00%	25,00%	45,00%
Acato a opinião das pessoas do meu círculo social sobre os cuidados que devem ser tomados ao conversar com desconhecidos na internet, ou tomar outras medidas de segurança da informação.	5,00%	20,00%	5,00%	25,00%	45,00%
Acredito que softwares para proteção e segurança possam causar problemas em outros programas no meu computador.	10,00%	5,00%	45,00%	15,00%	25,00%
Tenho o hábito de tomar medidas de proteção na internet.	25,00%	25,00%	5,00%	30,00%	15,00%
Consigo instalar softwares de proteção mesmo não havendo ninguém para me ensinar.	65,00%	20,00%	10,00%	5,00%	0,00%

Fonte: levantamento de dados.

TABELA 7 - FREQUÊNCIA ABSOLUTA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 1 A 5)

	Grupo Etário - Terceira Idade				
	Discordo Totalmente	Discordo Parcialmente	Não sei responder	Concordo Parcialmente	Concordo Totalmente
Eu troco as minhas senhas com frequência.	8	5	0	4	3
Um vírus pode ser prejudicial.	0	0	0	2	18
As minhas chances de ser infectado por vírus são altas.	3	9	3	3	2
Minhas informações pessoais já foram violadas.	11	4	4	1	0
Considero fácil tomar as medidas de segurança da informação necessárias.	9	5	4	1	1

Fonte: levantamento de dados.

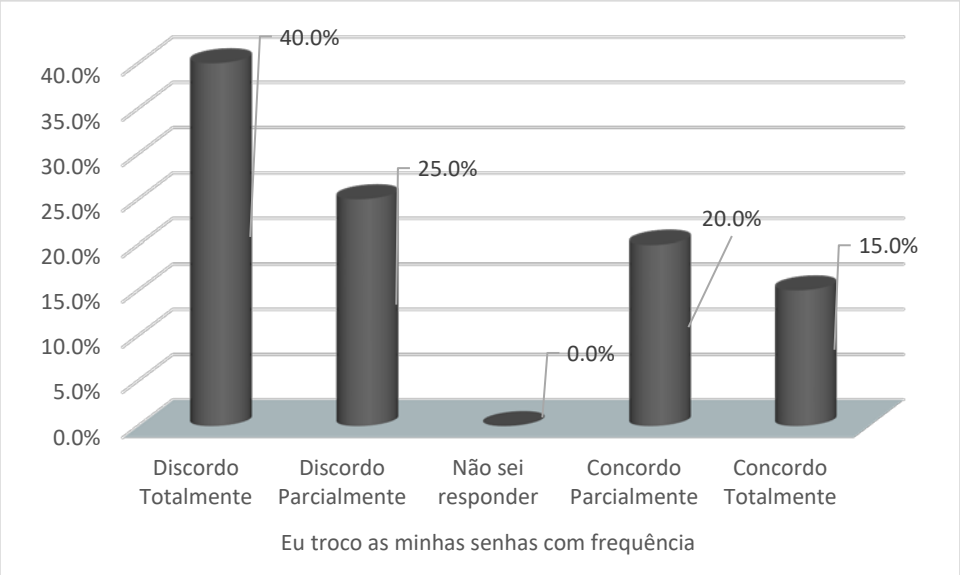
TABELA 8 - FREQUÊNCIA ABSOLUTA DO RESULTADO DO QUESTIONÁRIO (QUESTÕES DE 6 A 10)

	Terceira Idade				
	Discordo Totalmente	Discordo Parcialmente	Não sei responder	Concordo Parcialmente	Concordo Totalmente
Acredito que um software de proteção possa ser útil para detectar e remover vírus.	1	2	3	5	9
Acato a opinião das pessoas do meu círculo social sobre os cuidados que devem ser tomados ao conversar com desconhecidos na internet, ou tomar outras medidas de segurança da informação.	1	4	1	5	9
Acredito que softwares para proteção e segurança possam causar problemas em outros programas no meu computador.	2	1	9	3	5
Tenho o hábito de tomar medidas de proteção na internet.	5	5	1	6	3
Consigo instalar softwares de proteção mesmo não havendo ninguém para me ensinar.	13	4	2	1	0

Fonte: levantamento de dados.

Com o intuito de facilitar a visualização, foram geradas dez figuras com a descrição das respostas dadas pelos respondentes de terceira idade, a partir dos itens do questionário.

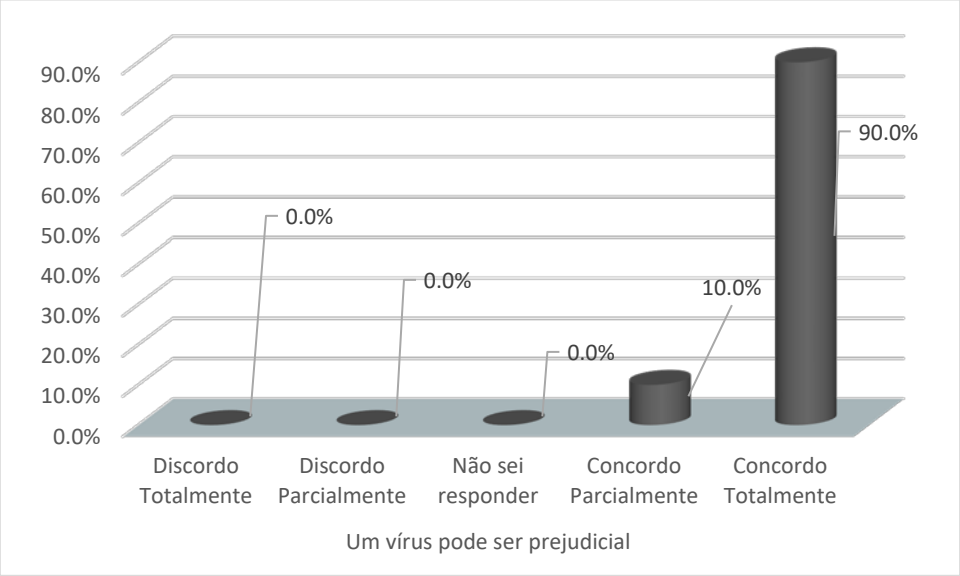
FIGURA 1 - DADOS DA ASSERTIVA “EU TROCO MINHAS SENHAS COM FREQUÊNCIA”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

Conforme se extrai da figura 2, as alternativas *Discordo Totalmente* e *Discordo Parcialmente* somadas respondem por 65% do total das respostas no público de terceira idade, indicando uma possível disposição das pessoas a não trocarem as suas senhas, fato que pode fragilizar a segurança da informação desses respondentes.

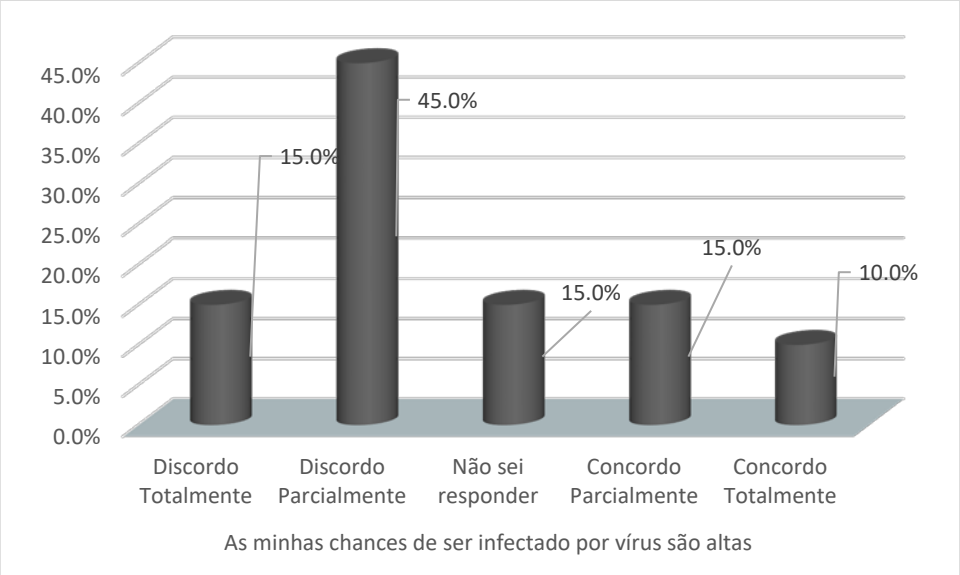
FIGURA 2 - DADOS DA ASSERTIVA “UM VÍRUS PODE SER PREJUDICIAL”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

Atente-se que, com relação à figura 3, é possível observar que o reconhecimento do potencial ofensivo de um vírus é consenso entre os respondentes da terceira idade.

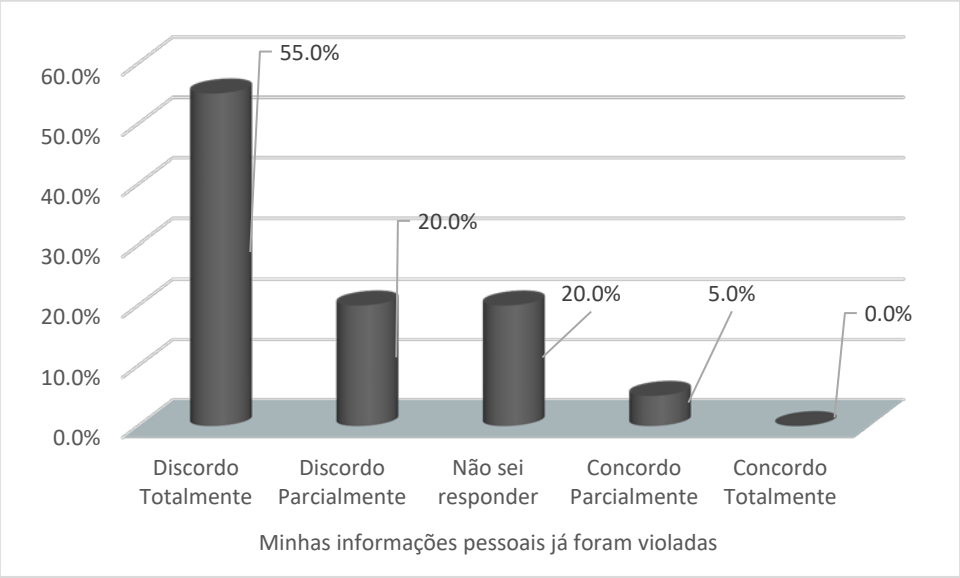
FIGURA 3 - DADOS DA ASSERTIVA “AS MINHAS CHANCES DE SER INFECTADO POR VÍRUS SÃO ALTAS”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

No que concerne à figura 4, observa-se que as respostas apresentam um aspecto equilibrado entre quatro das cinco assertivas; todavia, 60% dos respondentes da terceira idade acreditam totalmente ou parcialmente que as suas chances de serem infectados não são altas, o que pode ser um pensamento equivocado.

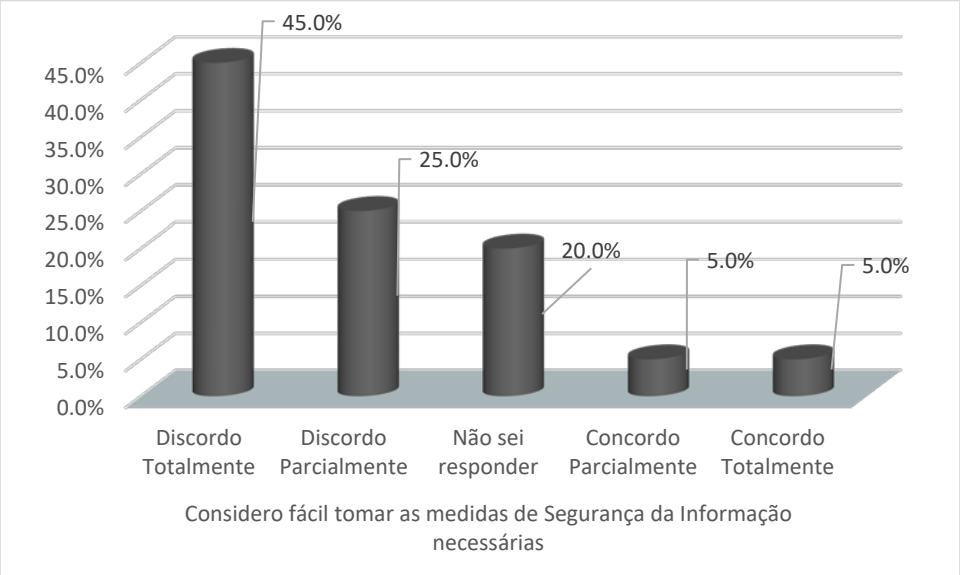
FIGURA 4 - DADOS DA ASSERTIVA “MINHAS INFORMAÇÕES PESSOAIS JÁ FORAM VIOLADAS”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

Na figura 5, 75% dos respondentes da terceira idade discordam totalmente ou parcialmente de que já tiveram as suas informações violadas. Vale ressaltar que grande parte dos usuários não têm conhecimento sobre as políticas de privacidade dos sites sob o qual registram as suas informações pessoais, e simplesmente clicam em “*Concordo com a política*” sem ao menos lê-la (MASOODA et al, 2016).

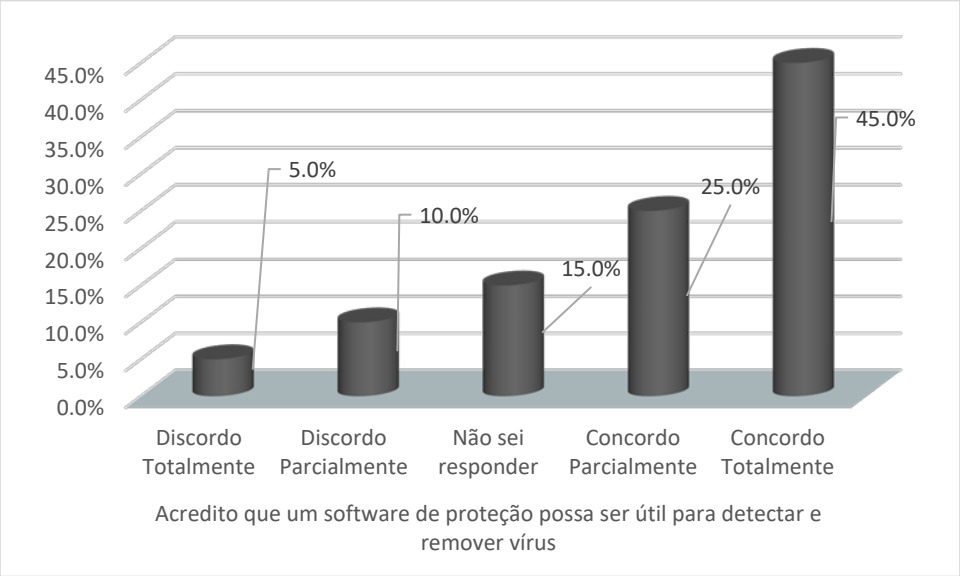
FIGURA 5 - DADOS DA ASSERTIVA “CONSIDERO FÁCIL TOMAR AS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO NECESSÁRIAS”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

No que diz respeito a figura 6, ressalta-se que o público de terceira idade externou dificuldades para tomar medidas de segurança da informação na internet, com apenas 10% dos usuários alegando *concordar totalmente ou parcialmente* que é fácil tomar medidas de segurança da informação na internet.

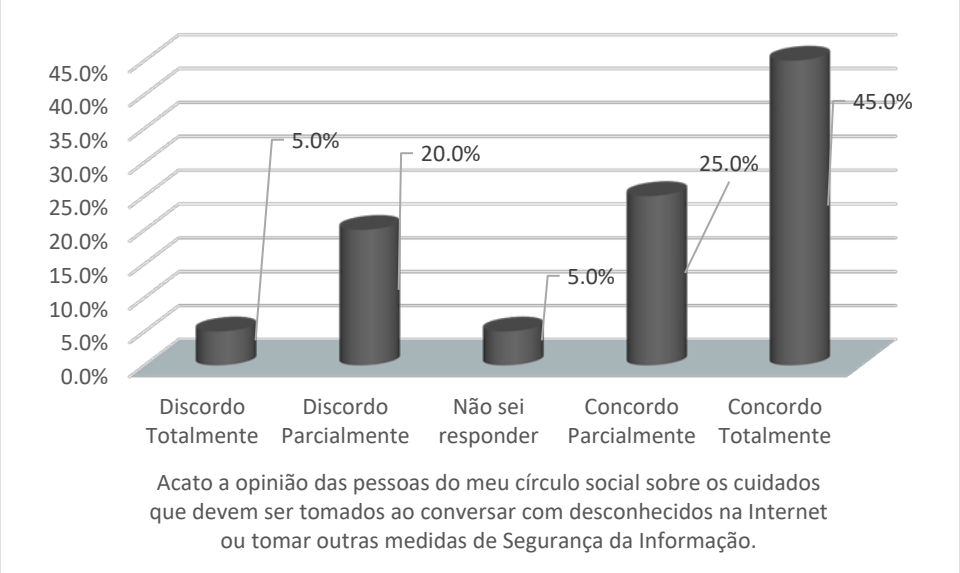
FIGURA 6 - DADOS DA ASSERTIVA “ACREDITO QUE UM SOFTWARE DE PROTEÇÃO POSSA SER ÚTIL PARA DETECTAR E REMOVER VÍRUS”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

A figura 7, que está associada à variável denominada “eficácia da resposta” tem o intuito de verificar se os respondentes creem que um software de proteção possa ser útil para detectar e remover vírus. Nesse sentido, parte majoritária dos respondentes de terceira idade acredita na eficácia de um software de proteção para fazer frente a vírus e pragas digitais. Fazer um usuário acreditar que softwares de segurança são eficazes em combater pragas digitais estimula a sua tomada de decisão nesse sentido, isso porque a variável “eficácia da resposta” é uma das que pesam na decisão do usuário em tomar uma medida de segurança da informação, conforme pesquisa realizada por (TSAI et al, 2016);

FIGURA 7 - DADOS DA ASSERTIVA “ACATO A OPINIÃO DAS PESSOAS DO MEU CÍRCULO SOCIAL SOBRE OS CUIDADOS QUE DEVEM SER TOMADOS AO CONVERSAR COM DESCONHECIDOS NA INTERNET, OU TOMAR OUTRAS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO”, DO PÚBLICO DE TERCEIRA IDADE

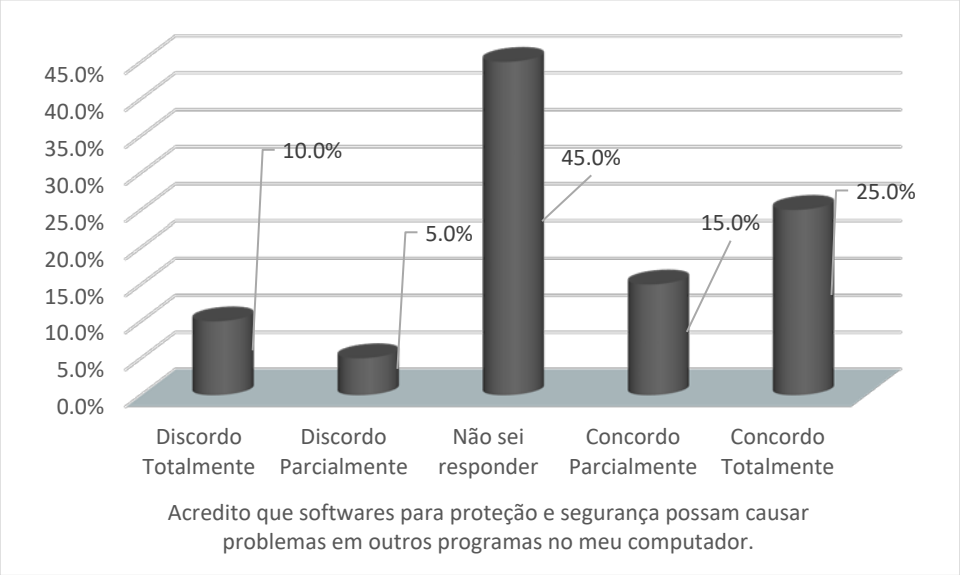


Fonte: levantamento de dados.

A partir da figura 8, infere-se que a maior parte do público respondente tende a considerar a opinião das pessoas de seu círculo social sobre os cuidados a serem tomados na internet. Nesse ponto, cabe uma ressalva, de que a *Engenharia Social* é um dos ataques empreendidos contra os usuários de internet, e que, em determinados critérios, o público da terceira idade está

mais vulnerável nesse quesito, e a pesquisa de (VIANA, 2017) corrobora essa afirmação.

FIGURA 8 - DADOS DA ASSERTIVA “ACREDITO QUE SOFTWARES PARA PROTEÇÃO E SEGURANÇA POSSAM CAUSAR PROBLEMAS EM OUTROS PROGRAMAS NO MEU COMPUTADOR”, DO PÚBLICO DE TERCEIRA IDADE

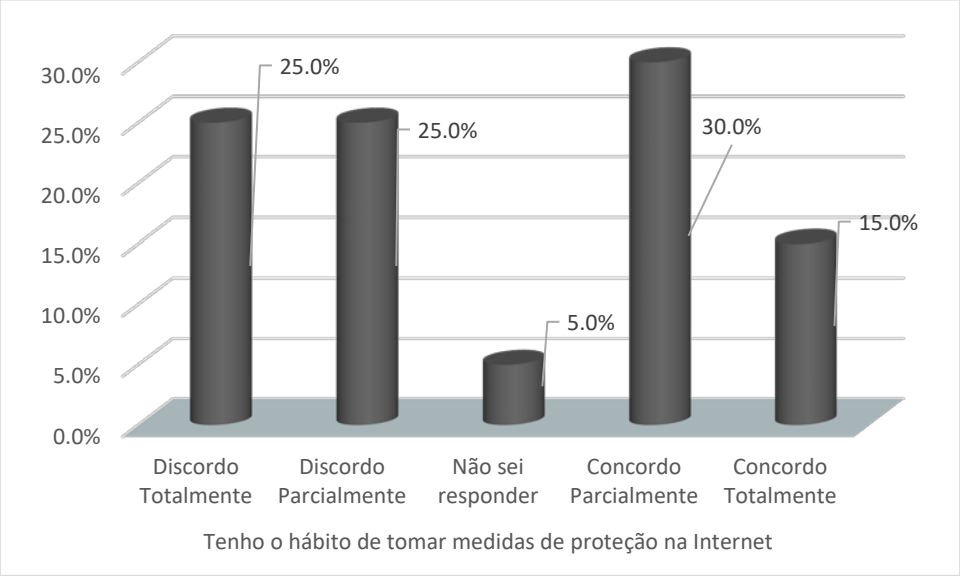


Fonte: levantamento de dados.

As respostas à assertiva exibida por meio da figura 9, se relacionam com a variável da *Teoria da Motivação Para a Proteção* denominada “custo da resposta”; se a resposta à ameaça de segurança da informação demandar um alto custo, ou seja, trouxer algum prejuízo a outras ferramentas do computador, o usuário tenderá a não tomar a medida de segurança da informação requerida.

A percepção desse baixo custo em tomar uma resposta, conforme mostrado na figura 9, pelo público idoso, é um indicador positivo, já que tal fato não será um entrave no momento da tomada de decisão de aderir a um comportamento mais seguro.

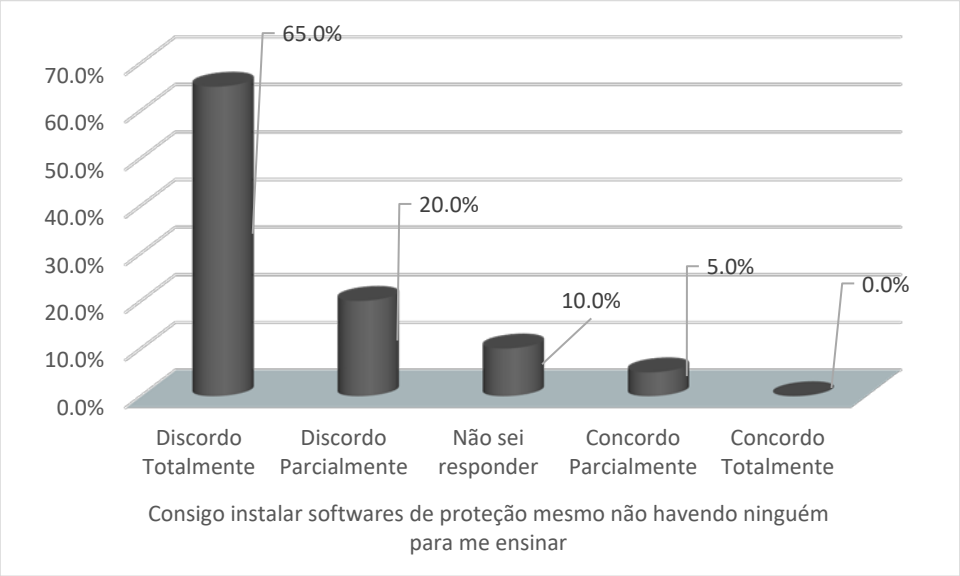
FIGURA 9 - DADOS DA ASSERTIVA “TENHO O HÁBITO DE TOMAR MEDIDAS DE PROTEÇÃO NA INTERNET”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

Em alusão à figura 10, tratando-se de hábitos na internet, metade do público de terceira idade *discorda total* ou *parcialmente* sobre manter um hábito seguro na internet.

FIGURA 10 - DADOS DA ASSERTIVA “CONSIGO INSTALAR SOFTWARES DE PROTEÇÃO MESMO NÃO HAVENDO NINGUÉM PARA ME ENSINAR”, DO PÚBLICO DE TERCEIRA IDADE



Fonte: levantamento de dados.

Na figura 11, o público de terceira idade afirma não conseguir instalar softwares de segurança da informação sem que haja alguém para auxiliá-los.

TABELA 9 - MEDIDAS DE TENDÊNCIA CENTRAL

Afirmação	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Média	2,45	4,9	2,6	1,75	2	3,95	3,85	3,4	2,85	1,55
Mediana	2	5	2	1	2	4	4	3	2,5	1
Moda	1	5	2	1	1	5	5	3	4	1

Afirmação

1. Eu troco as minhas senhas com frequência;
2. Um vírus pode ser prejudicial;
3. As minhas chances de ser infectado por vírus são altas;
4. Minhas informações pessoais já foram violadas;
5. Considero fácil tomar as medidas de segurança da informação necessárias;
6. Acredito que um software de proteção possa ser útil para detectar e remover vírus;
7. Acato a opinião das pessoas do meu círculo social sobre os cuidados que devem ser tomados ao conversar com desconhecidos na internet, ou tomar outras medidas de segurança da informação;
8. Acredito que softwares para proteção e segurança possam causar problemas em outros programas no meu computador;
9. Tenho o hábito de tomar medidas de proteção na internet;
10. Consigo instalar softwares de proteção mesmo não havendo ninguém para me ensinar.

Assertivas na escala likert

1. Discordo totalmente
2. Discordo parcialmente
3. Não sei responder
4. Concordo parcialmente
5. Concordo totalmente

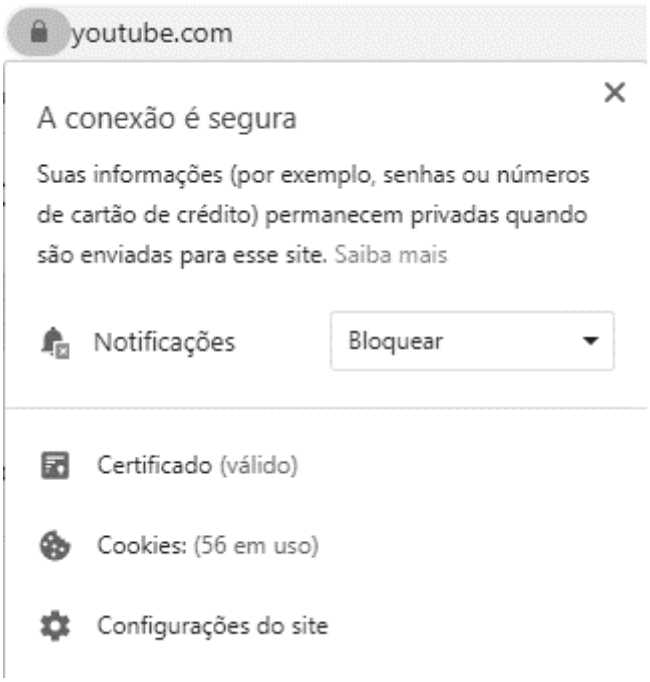
Fonte: levantamento de dados

4.2.2 Observação de usuários

Nesta seção, o processo de Observação Direta com os usuários será melhor detalhada, a fim de fornecer um entendimento de como o usuário doméstico interage com os itens de segurança da informação selecionados.

4.2.2.1 Imagem e descrição dos itens de segurança em que os usuários interagiram

FIGURA 11 - AÇÃO 1 – VERIFICAR CADEADO



Fonte: levantamento de dados.

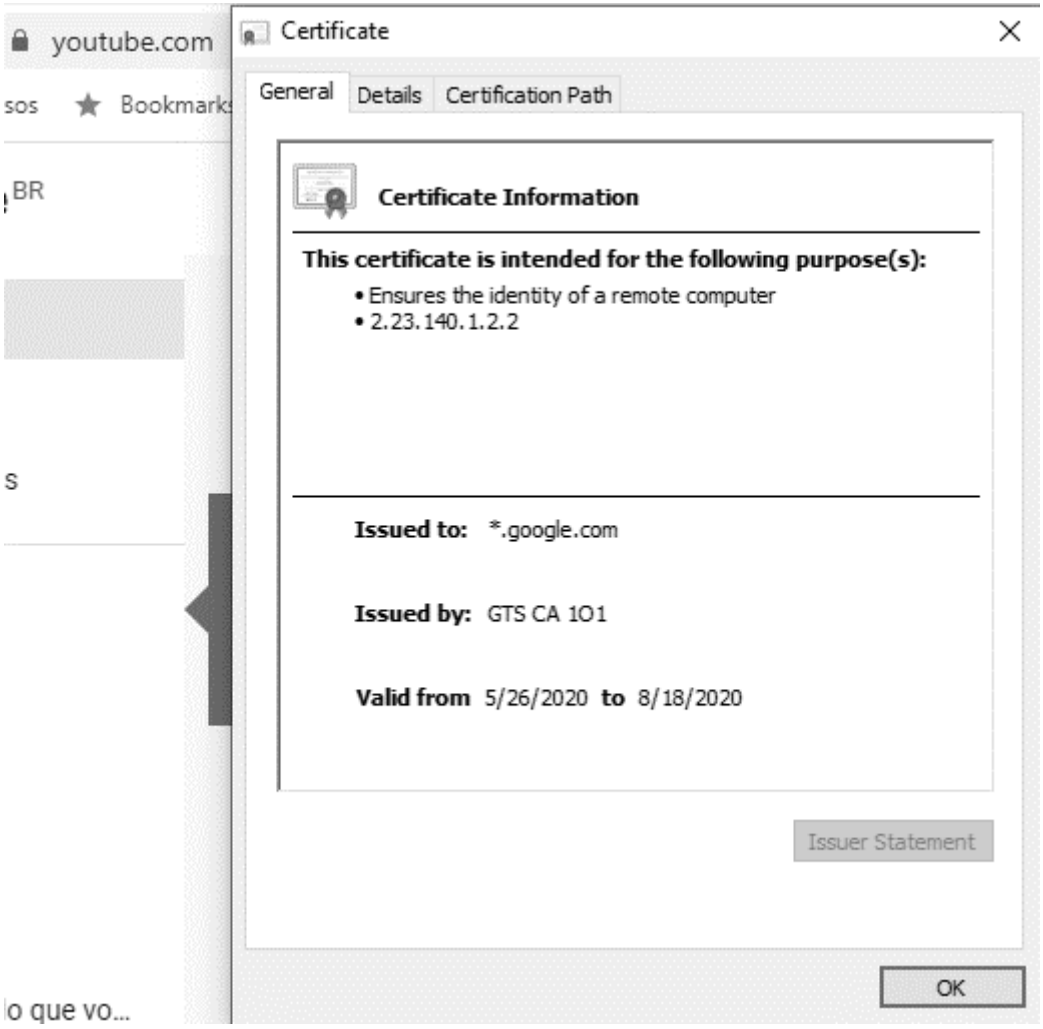
Nesta atividade foi solicitado aos voluntários que localizassem o cadeado que é exibido no navegador e explicasse a sua função.

FIGURA 12 - AÇÃO 2 – VERIFICAR HTTPS

Fonte: levantamento de dados.

Nesta ação foi solicitado aos voluntários que identificassem se o site utilizava o protocolo *https*. Muitos usuários sentiram dificuldades nessa etapa em razão de que o *https* é mostrado somente quando o usuário clica duas vezes, na sequência, no campo de busca do navegador.

FIGURA 13 - AÇÃO 3 – VERIFICAR CERTIFICADO DE SEGURANÇA



Fonte: levantamento de dados.

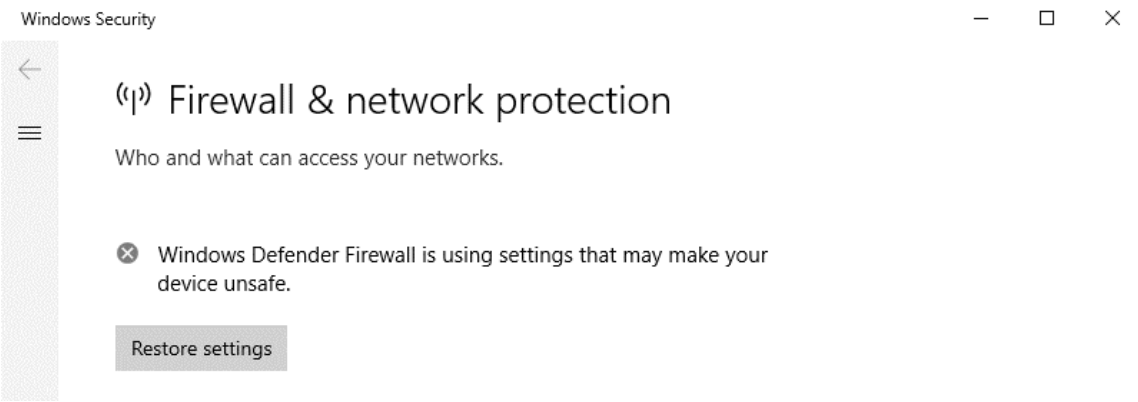
Nesta ação foi solicitado aos voluntários que localizassem o certificado de segurança do site e verificasse se é válido.

FIGURA 14 - AÇÃO 4 – VERIFICAR DOMÍNIO

Fonte: levantamento de dados.

Nesta ação foi questionado ao usuário sobre o que é nome de domínio e como ele faria para localizar esse nome.

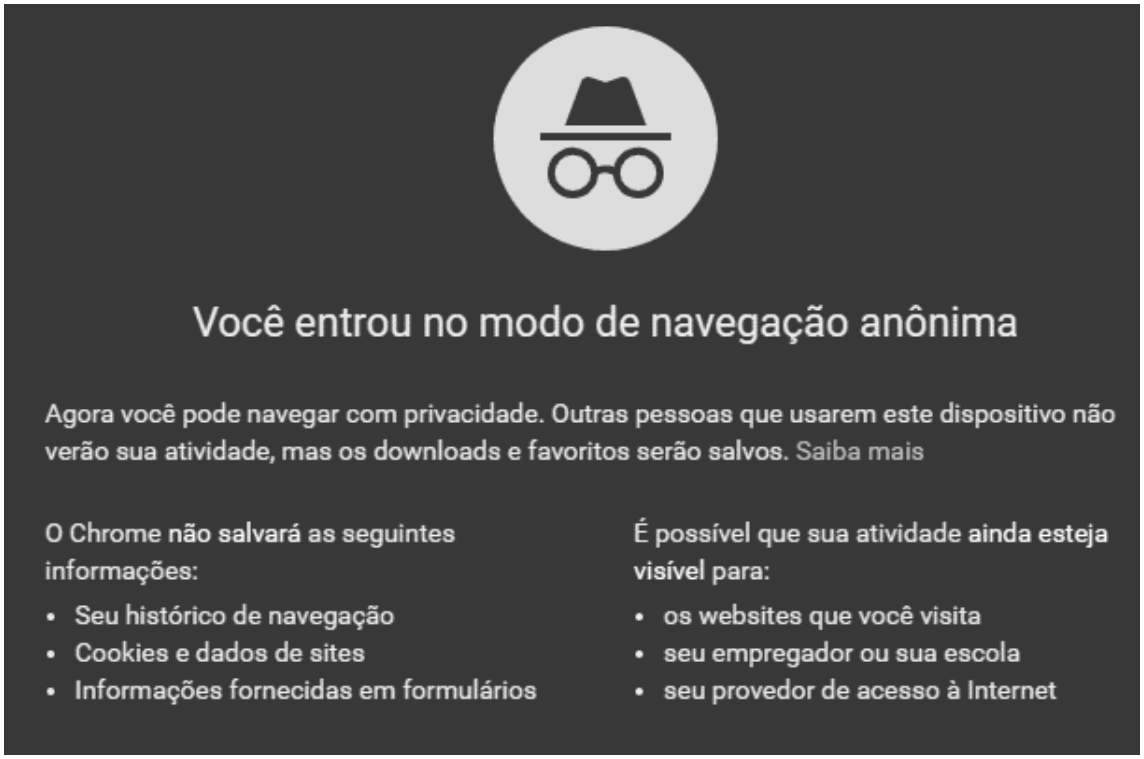
FIGURA 15 - AÇÃO 5 – VERIFICAR FIREWALL



Fonte: levantamento de dados.

Nesta ação, foi solicitado aos voluntários que verificassem a situação de seu firewall.

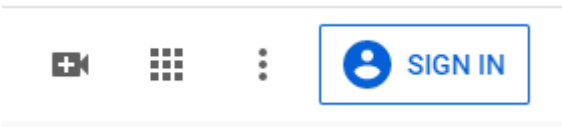
FIGURA 16 - AÇÃO 6 – NAVEGAR ANÔNIMO

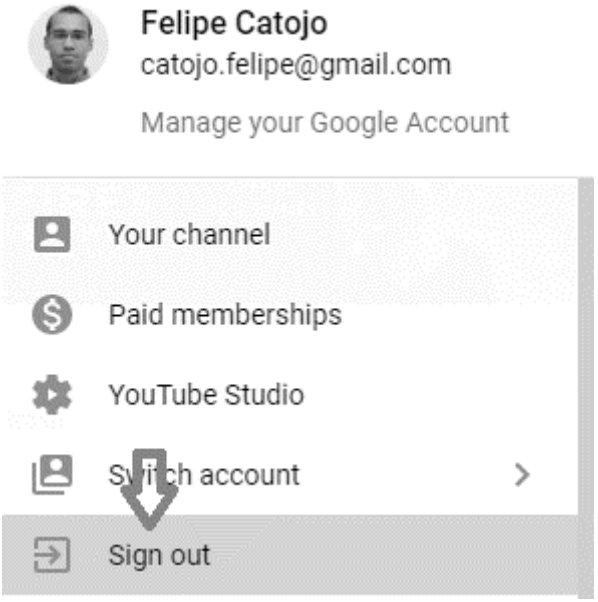


Fonte: levantamento de dados.

Nesta ação foi solicitado aos voluntários que navegassem anonimamente. Alguns usuários nunca tinham ouvido falar desse recurso.

FIGURA 17 - AÇÃO 7 – REALIZAR *LOGIN* E *LOGOUT*





Fonte: levantamento de dados.

Nesta ação, foi questionado se os usuários sabiam o que era *login* e *logout*. Muitos usuários conseguiram realizar a atividade, mas não souberam descrever corretamente o ato de *logar* e de *deslogar* de uma plataforma, pois conheciam apenas como "*entrar*" e "*sair*" da plataforma.

FIGURA 18 - AÇÃO 8 – IDENTIFICAR DESTINO DE URL ANTES DE CLICAR

Fonte: levantamento de dados.

Nesta ação, foi solicitado que os voluntários identificassem o destino de uma *url* antes de clicar na mesma. Houve uma dificuldade maior nos testes quando realizados por meio de *smartphone*, em que o usuário para completar essa ação precisava tocar na tela em cima de um rótulo durante alguns

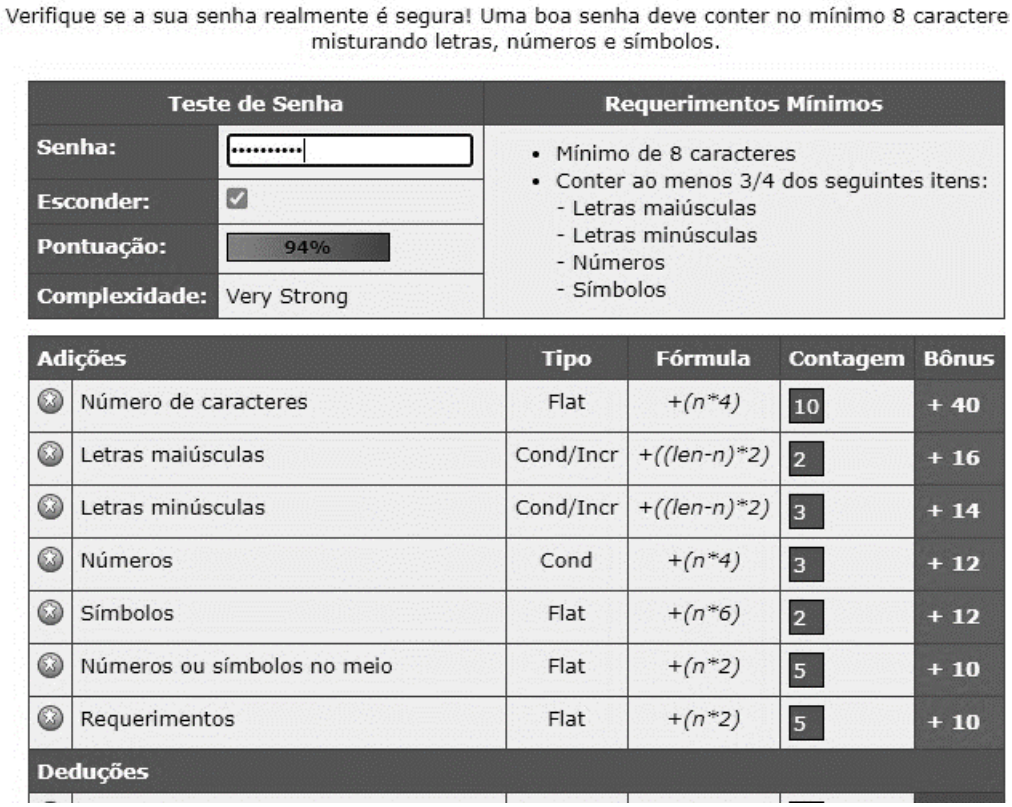
segundos até que aparecesse a opção “Copiar URL”, o usuário precisaria então colar essa URL em algum editor de texto para que ela ficasse visível.

FIGURA 19 - AÇÃO 9 – IDENTIFICAR PHISHING

Fonte: levantamento de dados.

Nesta atividade, foi solicitado aos voluntários que analisassem a imagem com o intuito de identificar anormalidades no que se refere à segurança da informação. Alguns usuários apontaram para o endereço colocado de maneira inadequada antes do domínio do site, outros usuários apontaram a ausência de cadeado que indica que a conexão é segura.

FIGURA 20 - AÇÃO 10 – DEFINIR SENHA FORTE



Fonte: levantamento de dados.

Nesta atividade, os usuários foram solicitados a inserirem uma senha inédita, da qual nunca haviam utilizado anteriormente, com o intuito de testar a força de senha.

4.2.2.2 Usuários selecionados para os testes

Nessa etapa da pesquisa, foram registrados os atributos mais importantes do Grupo Idoso (GI). Os voluntários também receberam codinomes para garantir o anonimato, sendo Idoso1 até Idoso10. As características desse grupo podem ser visualizadas na tabela a seguir:

TABELA 10 - USUÁRIOS SELECIONADOS PARA OS TESTES

Grupo	Usuário	Sexo	Idade	Ocupação	Escolaridade
GI	**Idosa1**	F	72	Psicóloga	Superior
	Idoso2	M	72	Suboficial de Mar. Mercante	Médio
	Idosa3	F	75	Técnica Administrativa	Superior
	Idoso4	M	83	Engenheiro Mecânico	Superior
	Idoso5	M	84	Militar da Reserva	Médio
	Idoso6	M	75	Técnica Administrativa	Médio
	Idoso7	M	70	Gráfico	Médio
	Idosa8	F	70	Contadora	Superior
	Idosa9	F	70	Pedagoga	Superior
	Idosa10	F	70	Técnica Administrativa	Superior

Fonte: levantamento de dados.

Usuários de terceira idade

Devido à pandemia de COVID-19 anunciada pela OMS em 11 de março de 2020 (UNA-SUS, 2020), os testes com os usuários idosos não puderam ser realizados presencialmente. Dessa forma, procedeu-se com a realização dos testes remotamente.

Com isso, seis dos dez usuários de terceira idade precisaram contar com o apoio de algum familiar para a preparação do ambiente de testes. Esse apoio de um familiar foi necessário na maior parte dos casos para:

1) estabelecer a reunião por *Google Meet*;

2) instalar o navegador *Google Chrome*;

3) realizar o compartilhamento remoto da tela.

Quando algum familiar prestava apoio na preparação do ambiente ao usuário de terceira idade, este já sabia de antemão que não poderia dar sugestões quanto ao objeto do teste, portanto, foi estabelecido como premissa

que qualquer interferência do familiar, que pudesse resultar na conclusão com sucesso da atividade não seria considerada para fins de computo do percentual de sucesso.

Usuária Idosa1

A usuária Idosa1, mulher, 72 anos, psicóloga, executou as ações em uma tarde do dia 27/11/2019. A voluntária utilizou seu próprio computador para efetuar a pesquisa e se mostrou bastante animada em contribuir. Ela foi convidada a participar por meio do *Whatsapp*, pois fazia parte do círculo social do pesquisador. A participante não necessitou de auxílio de familiar para preparação do ambiente, apenas do pesquisador por meio de chamada telefônica.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", a voluntária conseguiu localizar o item, e comentou: "*é pra informar que estou num site seguro, né?*" e também mencionou "*mexo mais no celular, acho que eu teria mais facilidade lá*". Na atividade 2, "*Analisar prefixo de HTTPS*", ela não conseguiu encontrar esse prefixo, e comentou: "*essas letras estão tão pequenas*", e apesar de ter tentado localizar o item, não teve sucesso nessa ação. Na atividade 3, "*Verificar certificados de segurança*", durante a atividade, ela comentou: "*eu sei mais acessar a internet, mas tem uma menina que trabalha lá em casa que resolve isso pra mim*", e não localizou o certificado. Na atividade 4, "*Analisar nome de domínio*", a usuária soube responder bem a atividade, e disse que sabia discernir os sites que visitava, e comentou com um tom de indagação: *"é quando tem edu.com, gov.com?".* Na atividade 5, "*Verificar firewall*", a participante tentou executar a ação, mas sem sucesso, ela informou: "*sou usuária básica, e também tenho meus filhos que me ajudam nessas questões*". Na atividade 6, "*Navegar anônimo*" a usuária disse: "*não me preocupo em navegar anônimo, porque uso mais o telefone para ler notícias, falar no whatsapp e fazer e receber ligações*". Na atividade 7, "*Realizar logout após o término das atividades*", a participante conseguiu realizar a atividade normalmente, pois já utilizava essa função no *Facebook*. Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" a voluntária

conseguiu realizar a ação pelo computador e disse: “*é aquele endereço que fica pequenininho no cantinho?*”. Na ação 9, “*Identificar conteúdo phishing*”, ela não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, mas informou que só acessa sites de confiança e também comentou: “*geralmente acesso os links do grupo da família pelo Whatsapp, mas não acesso o que não conheço, e às vezes também pergunto aos meus filhos se o endereço é seguro”*. Na última ação, 10, “*Definir senha forte*”, a usuária digitou uma senha inédita, mas que carecia de força, ela comentou: "*costumo utilizar senhas fáceis de lembrar, porque senão esqueço*".

A voluntária teve um desempenho acima da média, e seu percentual de (40%) de conclusão das atividades ficou acima da média do grupo etário (22%) do qual se enquadrava.

Usuário Idoso2

O usuário Idoso2, homem, 72 anos, nível médio, executou as ações em sua residência por meio de vídeoconferência com o pesquisador, numa tarde de sábado, do dia 30/05/2020. A sua filha realizou a preparação do ambiente para que o mesmo executasse as ações. O participante foi bastante solicito em participar da pesquisa e optou por fazê-lo por meio de um *smartphone*.

O usuário foi convidado a participar por meio do *Whatsapp*, e fazia parte do círculo social do pesquisador. Ele aceitou participar da pesquisa. Ele não era de falar muito, apenas o que lhe era perguntado.

Na preparação do ambiente, quando o pesquisador pediu para o voluntário compartilhar a sua tela, ele comentou: "compartilhar não tem não, tem apresentar tela".

Na atividade 1, “*Analisar ícone de cadeado fechado que é indicado pelo navegador*”, o voluntário conseguiu localizar o item, e comentou: *"eu tenho que colocar o dedo no cadeado, é isso?"* e também mencionou: “*é pra dizer que o site é seguro?*”. Na atividade 2, “*Analisar prefixo de HTTPS*”, o participante não conseguiu encontrar esse prefixo, mas perguntou: "é na parte de endereço?

Não sei não." E embora tenha tentado localizar o item, não teve sucesso nessa ação. Na atividade 3, "*Verificar certificados de segurança*", durante a atividade, ele comentou: "*é perto do cadeado? esse eu não sei não"*, e não localizou o certificado. Na atividade 4, "*Analisar nome de domínio*", o usuário conseguiu responder a atividade, e disse o nome de domínio do site em que se encontrava*".* Na atividade 5, "*Verificar firewall*", ele tentou executar a ação, mas sem sucesso, ele informou: "*sou usuário básico, isso aí já é mais difícil pra mim*". Na atividade 6, "*Navegar anônimo*" o usuário tentou localizar a função e não conseguiu, então comentou: "*não não não, isso aí eu não sei não, acesso mais whatsapp e youtube*". Na atividade 7, "*Realizar logout após o término das atividades*", o participante conseguiu realizar a atividade normalmente, mas ficou confuso quanto aos termos *login* e *logout*, e comentou: "*loginho é entrada e logout é a saída do site, é isso?*". Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" usuário não conseguiu realizar a ação pelo telefone e disse "*url é onde coloca o endereço do site, é isso? Não tenho esse hábito não, eu clico, boto o endereço e pronto".* Na ação 9, "*Identificar conteúdo phishing*", ele não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*tá muito pequeno pra enxergar, não tá dando pra identificar não"* e afirmou, logo após o pesquisador ter esclarecido a atividade: "*é uma página falsa!"*. Na última ação, 10, "Definir senha forte" o usuário digitou uma senha inédita, mas que carecia de força, ele comentou: *"eu estou acostumado a fazer de 6 dígitos".*

Seu percentual de (30%) de conclusão das atividades ficou acima da média do grupo etário (22%) do qual se enquadrava.

Usuária idosa3

A usuária Idosa3, mulher, 75 anos e de nível médio, técnica administrativa, executou as ações em sua residência por meio de vídeoconferência com o pesquisador numa manhã do dia 24/08/2020.

Ela foi convidada a participar da pesquisa por meio do *Facebook*, já que era do círculo social do pesquisador. Aceitou participar da pesquisa e ela própria preparou o ambiente para os testes.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", a voluntária não conseguiu realizar a ação, e quando perguntada sobre o objetivo do símbolo do cadeado, não conseguiu explicar e comentou: "eu sei que não consigo abrir nada quando o cadeado aparece", e também disse: "eu acho que é exatamente pra não dar acesso pra gente". Na atividade 2, "*Analisar prefixo de HTTPS*", ela não conseguiu encontrar esse prefixo. E comentou: "*aparece muito isso, mas eu não sei também não*", "*aparece lá em cima onde você pede pra abrir algum link que mandam*". Na atividade 3, "*Verificar certificado de segurança*", a usuária não conseguiu localizar o item, e comentou: "*aparece muito quando abre o banco, o site do banco", "aí ele já diz, que é uma segurança, né".* Na atividade 4, "*Analisar nome de domínio*", a participante não conseguiu explicar o que é nome de domínio de um site, e com isso, não concluiu a atividade, ela comentou: "tá fazendo umas perguntas muito difíceis", "é você ter o domínio sobre aquilo, sobre alguma coisa". Na atividade 5, "*Verificar firewall*", a usuária não conseguiu concluir a atividade, e comentou: "nunca ouvi falar em firewall, não sei não". Na atividade 6, "*Navegar anônimo*", após ter tentado sem sucesso executar essa ação, ela comentou: "já ouvi falar, mas não sei como funciona, não sei como que é". Na atividade 7, "*Realizar logout após o término das atividades*" ela conseguiu concluir a atividade e soube explicar corretamente essa função, comentando: "*login é pra quando você vai entrar em alguma coisa, aí eles pedem logo! acessar o seu login*". Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" não conseguiu realizar a ação e disse: "isso eu nunca precisei executar não". Na ação 9, "*Identificar conteúdo phishing*", ela não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*geralmente são pessoas conhecidas que me mandam coisas por e-mail, assim como você, então eu já abro direto, quando vem algum link no meu email, ou por whatsapp eu não abro".* Na última ação, 10, "*Definir senha forte*" a usuária digitou uma senha inédita, mas que era frágil, ela disse: *"geralmente eu uso só números, a não ser, por exemplo, no caso do meu e-mail, só no meu e-mail*

particular e do trabalho que não são só números, mas geralmente minhas senhas todas são seguidas de números".

A voluntária teve um desempenho abaixo da média, e seu percentual de (0%) de conclusão das atividades ficou abaixo da média do grupo etário (22%) do qual se enquadrava.

Usuário idoso4

O usuário Idoso4, homem, 83 anos, engenheiro mecânico, executou as ações em sua residência por meio de vídeo conferencia com o pesquisador, numa tarde do dia 28/08/2020.

O usuário foi convidado a participar da pesquisa por meio da sua neta, foi enviada uma mensagem por *Whatsapp,* e depois foi realizada uma ligação para alinhar a execução da pesquisa. Sua neta já era do círculo social do pesquisador. O usuário aceitou participar da pesquisa. E ele próprio preparou o ambiente para os testes.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", o voluntário não conseguiu realizar a ação, e comentou: "*Não olho cadeado e raramente acesso site de banco. Acesso mais no celular porque acredito que pelo aplicativo tem uma maior segurança do que no computador*". Na atividade 2, "*Analisar prefixo de HTTPS*", o usuário não conseguiu encontrar esse prefixo. Mas comentou: "*Nunca ouvi falar nisso, mas já ouvi falar em criptografia, pra melhorar a segurança da gente. A nossa segurança em relação ao manuseio das coisas do banco*". Na atividade 3, "*Verificar certificado de segurança*", o usuário não conseguiu localizar o item, e comentou: "*já ouvi falar em certificado de segurança - pra tu ter segurança nas coisas que vocês fazem com o computador".* Na atividade 4, "*Analisar nome de domínio*", o usuário não conseguiu explicar o que é nome de domínio de um site, e não concluiu a atividade, ele comentou: "*não, não ouvi falar*". Na atividade 5,

“*Verificar firewall*”, o usuário não conseguiu concluir a atividade, e comentou: “*Nunca ouvi falar, eu não sou dessa época. Quando eu ‘tava’ pra me aposentar é que começaram. A manutenção foi uma das últimas áreas em que colocaram computador. Aprendi aqui em casa, mexendo, fazendo; meus filhos me dão dicas, e vou fuçando, mas não sou assim, expert não; mas eu mando mensagem, recebo mensagens, uma série de coisas mais corriqueiras*”. Na atividade 6, “*Navegar anônimo*”, após o participante ter tentado sem sucesso executar essa ação, ele comentou: “*Eu nunca ouvi falar nisso não, isso é... anônimo é que você não conhece a pessoa né*”. Na atividade 7, “*Realizar logout após o término das atividades*”, o participante conseguiu concluir a atividade, mas não soube explicar corretamente essa função, e comentou: “*Login é quando você quer fazer algum contato, você faz o login do teu site... quando vai entrar, ele pede login, bota a senha...”.* Já com relação ao logout, o voluntário comentou: *“look out, significa olhar por fora*”; Na ação 8, “*Mover cursor do mouse sobre a url antes de clicar;*” usuário não conseguiu realizar a ação e comentou não saber o significado disso”. Na ação 9, “*Identificar conteúdo phishing*”, ele não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*Sou cuidadoso, não abro de qualquer um não...”.* Na última ação, 10, “*Definir senha forte*”, o usuário digitou uma senha inédita, mas que era frágil, ele disse: *"Misturo letras com números porque é mais seguro, mais difícil de você ser grampeado por alguém aí”.* Mas a senha não se mostrou com força suficiente.

O voluntário teve um desempenho abaixo da média, e seu percentual de (10%) de conclusão das atividades ficou abaixo da média do grupo etário (22%) do qual se enquadrava.

Usuário idoso5

O usuário Idoso5, homem, 84 anos, militar da reserva, nível superior, executou as ações em sua residência por meio de vídeoconferência com o pesquisador, numa tarde do dia 29/08/2020.

O usuário foi convidado a participar da pesquisa por meio da sua neta, foi enviada uma mensagem por *Whatsapp,* e depois foi realizada uma ligação

para alinhar a execução da pesquisa. Sua neta já era do círculo social do pesquisador. O usuário aceitou participar da pesquisa. E ele próprio preparou o ambiente para os testes.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", o voluntário conseguiu realizar a ação, e comentou: "*Não há dúvida, sem o cadeado eu não abro de jeito nenhum, ele serve pra bloquear alguém que queira entrar no que a gente tá falando, né? Ou que tá resolvendo, sei lá, mas assim mesmo isso aí ainda é falho"*. Na atividade 2, "*Analisar prefixo de HTTPS*", o usuário conseguiu encontrar esse prefixo, e comentou: "*aqui tem e deve ter, o que eu ouvi dizer é que ele mostra a segurança do site em que eu estou entrando. Quando não tem é coisa que não é certa, que não é seguro*". Na atividade 3, "*Verificar certificado de segurança*", o usuário não conseguiu localizar o item, e indagou: *"tem que olhar pra ver se tem o https e pra ver se tem o cadeadinho. Mas certificado é um papel escrito, isso?".* Na atividade 4, "*Analisar nome de domínio*", o usuário conseguiu explicar o que é nome de domínio de um site, e também concluiu a atividade, ele comentou: "*já no e-mail, eu acredito que é quando a gente tem uma conta lá. Consigo identificar pelo 'terminal', depois da arroba*". Na atividade 5, "*Verificar firewall*", o usuário não conseguiu concluir a atividade, e comentou: "*Nunca ouvi falar*".Na atividade 6, "*Navegar anônimo*", após o usuário ter tentado sem sucesso executar essa ação, ele comentou: "*isso aí eu nunca ouvi falar não, não sei o que é não*". Na atividade 7, "*Realizar logout após o término das atividades*", o participante conseguiu concluir a atividade, e comentou: "*login é o nome da conta*", o usuário conhecia essa função como "entrar" e "sair". Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" usuário não conseguiu realizar a ação e comentou não saber o significado disso. Na ação 9, "*Identificar conteúdo phishing*", ele não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, mas comentou: "*Normalmente eu não abro, eu deleto ou então eu pergunto ao meu filho, e ele diz: papai, não entra não que isso aí é pegadinha".* Na última ação, 10, "*Definir senha forte*" o usuário digitou uma senha inédita, mas que era frágil, ele disse: *"Prefiro comprar no boleto, não coloco número de cartão. Eles recomendaram, quando eu comecei a aprender isso, que sejam letras e números e no mínimo 8*

caracteres. Sigo isso, com algumas exceções, quando é coisa boba". Mas a senha não tinha força suficiente para ser reputada como segura.

O voluntário teve um desempenho acima da média, e seu percentual de (40%) de conclusão das atividades ficou acima da média do grupo etário (22%) do qual se enquadrava.

Usuária idosa6

A usuária Idosa6, mulher, 75 anos e de nível médio, técnica administrativa, executou as ações em sua residência por meio de vídeoconferência com o pesquisador, numa manhã do dia 31/08/2020.

A usuária foi convidada a participar da pesquisa por *Facebook*, já que era do círculo social do pesquisador. A usuária aceitou participar da pesquisa. E ela própria preparou o ambiente para os testes.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", a voluntária não conseguiu realizar a ação, e quando perguntada sobre o objetivo do símbolo do cadeado, não conseguiu explicar e comentou: "não ok, não me atento para o cadeado." Na atividade 2, "*Analisar prefixo de HTTPS*", a usuária não conseguiu encontrar esse prefixo. E comentou: "*nunca ouvi falar*". Na atividade 3, "*Verificar certificado de segurança*", a usuária não conseguiu localizar o item, e comentou: "*não sei onde fica e nem me preocupo com isso".* Na atividade 4, "*Analisar nome de domínio*", a usuária não conseguiu explicar o que é nome de domínio de um site, com isso, não concluiu a atividade. Na atividade 5, "*Verificar firewall*", a usuária não conseguiu concluir a atividade, e comentou: "nunca ouvi falar". Na atividade 6, "*Navegar anônimo*", após a usuária ter tentado sem sucesso executar essa ação, ela comentou: "nunca ouvi falar e também não sei para que serve". Na atividade 7, "*Realizar logout após o término das atividades*", a participante conseguiu concluir a atividade, mas não soube explicar os termos "*login*" e "*logout*". Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" usuária não conseguiu realizar a ação e disse: "não faço isso, clico direto". Na ação 9, "*Identificar conteúdo phishing*", ela não conseguiu detectar os

problemas de segurança que estavam na imagem que foi exibida, e comentou: "*se for e-mail do banco que estou acostumada a usar eu olho direto, senão, apago direto".* Na última ação, 10, "*Definir senha forte*", a usuária digitou uma senha inédita, mas que era frágil, e disse: *"misturo letras e números, às vezes com 8 caracteres".*

A voluntária teve um desempenho abaixo da média, e seu percentual de (10%) de conclusão das atividades ficou abaixo da média do grupo etário (22%) do qual se enquadrava.

Usuário Idoso7

O usuário Idoso7, homem, 70 anos, gráfico, executou as ações em sua residência por meio de vídeoconferência com o pesquisador, numa tarde do dia 13/06/2020.

O usuário foi convidado a participar por intermédio do seu filho, que é do círculo social do pesquisador. O usuário aceitou participar da pesquisa. O seu filho realizou toda a preparação do ambiente para o teste.

Na atividade 1, "A*nalisar ícone de cadeado fechado que é indicado pelo navegador*", o voluntário não conseguiu localizar o item, durante a tentativa de localizar o item, o usuário comentou: "*meu amigo, se você mexeu em alguma coisa, aqui não alterou nada, se tem algum cadeado aqui, ele foi parar em outro lugar*". Quando foi perguntando acerca do propósito do símbolo do cadeado, ele informou: "*serve pra abrir o Google é isso?"*. Na atividade 2, "*Analisar prefixo de HTTPS*", o usuário não conseguiu encontrar esse prefixo, e fez confusão com um ícone que estava na barra de ferramentas denominado "apps", o usuário comentou: "*tá aqui ó, apps*" e foi informado de que esse não era o ícone correto, e, apesar de continuar em sua tentativa sem sucesso, após desistir da tarefa, ele disse: "*já chegou a conclusão desse já? Ganhei zero, mas tudo bem; (risos)*". Na atividade 3, "*Verificar certificados de segurança*", apesar de não ter conseguido localizar os itens das atividades anteriores, como ele já havia mexido bastante nas opções de segurança, conseguiu localizar o certificado e comunicou que: "*certificado de segurança serve para certificar a*

segurança do site". Na atividade 4, "*Analisar nome de domínio*", o usuário não conseguiu responder a atividade, e mencionou: "não sei o que é isso". E após a atividade ter sido esclarecida para o usuário, o mesmo informou que desconhecia esse termo e conhecia apenas o nome *site*. Na atividade 5, "*Verificar firewall*", o usuário informou não saber o que é isso e desistiu da ação. Na atividade 6, "*Navegar anônimo*" o usuário informou que: "*to ouvindo isso pela primeira vez, aí começa a complicar né*", e logo depois da atividade ter sido explicada, ele disse: "*não sei se eu vou conseguir lembrar disso tudo que você falou aí*", e não conseguiu concluir a atividade. Na atividade 7, "*Realizar logout após o término das atividades*", o participante não conseguiu concluir. Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" usuário não conseguiu realizar a ação e brincou: "*quem sabe isso aí é meu filho, ele está escondendo o jogo (risos)".* Na ação 9, "*Identificar conteúdo phishing*", ele não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*eu não consegui, mas não é difícil, só que aonde você catucou eu nunca tinha visto".* Na última ação, 10, "*Definir senha forte*", o usuário digitou uma senha inédita, mas bastante frágil, ele disse: *"só uso números nas minhas senhas, uns quatro números, não passa disso".*

O voluntário teve um desempenho abaixo da média, e seu percentual de (10%) de conclusão das atividades ficou abaixo da média do grupo etário (22%) do qual se enquadrava.

Usuário idoso8

O usuário Idoso8, homem, 70 anos, contador, nível superior, executou as ações em sua residência por meio de vídeoconferência com o pesquisador numa tarde do dia 14/09/2020.

O usuário foi convidado a participar da pesquisa por meio de seu genro, foi enviada uma mensagem por *Whatsapp,* e depois foi realizada uma ligação para alinhar a execução da pesquisa. Seu genro não era do círculo pessoal do pesquisador, mas era do círculo social da esposa do pesquisador. O usuário

aceitou participar da pesquisa. E ele próprio preparou o ambiente para os testes.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", o voluntário não conseguiu realizar a ação, e comentou: "como eu não uso isso, eu suponho que é pra ver se está certo o que estou acessando". Na atividade 2, "*Analisar prefixo de HTTPS*", o usuário não conseguiu encontrar esse prefixo, e comentou: "*Quando você vai procurar um site de alguma coisa você coloca lá o https. Pra que serve eu não sei também*". Na atividade 3, "*Verificar certificado de segurança*", o usuário não conseguiu localizar o item, e comentou: "*Ouvir falar, eu já ouvi, mas a única coisa que eu uso é o antivírus, uso o AVG e pronto*". Na atividade 4, "*Analisar nome de domínio*", o usuário não conseguiu explicar o que é nome de domínio de um site, e também não concluiu a atividade, ele comentou: "*Domínio também não sei, já estou afastado, aposentando há bastante tempo. Quando tenho alguma dúvida eu ligo pro Márcio (meu genro).*"Na atividade 5, "*Verificar firewall*", o usuário não conseguiu concluir a atividade, e comentou: "*Firewall não, nunca ouvi falar*".Na atividade 6, "*Navegar anônimo*", após o usuário ter tentado sem sucesso executar essa ação, ele comentou: "*Só sei de navegação, anônima eu não sei*". Na atividade 7, "*Realizar logout após o término das atividades*", o participante conseguiu concluir a atividade e soube explicar corretamente essa função, e comentou: "*Login é pra entrar na conta. Qual que é meu login? É o meu e-mail.... quando eu vou abrir o computador eu sempre coloco o meu login, eu sei assim, tecnicamente eu não sei. Logout é 'logar' fora, sair...".* Na ação 8, "*Mover cursor do mouse sobre a url antes de clicar*;" usuário não conseguiu realizar a ação e comentou: "não faço isso não, já clico direto". Na ação 9, "*Identificar conteúdo phishing*", ele não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*Eu olho o que eu sei o que que é... Se eu recebo alguma mensagem de algo que eu participo, eu olho, o resto eu envio tudo pra lixeira. Mas normalmente são promoções que recebo, de sites de venda".* Na última ação, 10, "*Definir senha forte*", o usuário digitou uma senha inédita, mas que era frágil, ele disse: *"*Coloco oito dígitos misturados, com letras e números*".* Mas a senha não tinha força suficiente para ser reputada como segura.

O voluntário teve um desempenho abaixo da média, e seu percentual de (10%) de conclusão das atividades ficou abaixo da média do grupo etário (22%) do qual se enquadrava.

Usuária idosa9

A usuária Idosa9, mulher, 70 anos, nível superior, pedagoga, executou as ações em sua residência por meio de vídeoconferência com o pesquisador, numa noite de domingo do dia 14/06/2020.

A usuária foi convidada a participar por intermédio da sua filha, que é do círculo social do pesquisador. A usuária aceitou participar da pesquisa. A sua filha realizou toda a preparação do ambiente para o teste.

Na atividade 1, "*Analisar ícone de cadeado fechado que é indicado pelo navegador*", a voluntária conseguiu realizar a ação, e quando perguntada sobre o objetivo do símbolo do cadeado, pensou por cerca de seis segundos e respondeu: "*ah, lembrei, tem relação com a segurança do site*". Na atividade 2, "*Analisar prefixo de HTTPS*", a usuária não conseguiu encontrar esse prefixo, e desistiu da ação segundos depois. Também não soube explicar do que se tratava. Após o pesquisador explicar a atividade, a usuária comentou: "*é igual site de caixa né, de banco*?" Na atividade 3, "*Verificar certificado de segurança*", a usuária conseguiu localizar o item, e comentou: "*a maioria das pessoas não tem acesso a essas informações não, a esses detalhes*". Na atividade 4, "*Analisar nome de domínio*", a usuária não conseguiu explicar o que é domínio de um site, com isso, não foi possível concluir a atividade. Na atividade 5, "*Verificar firewall*", a usuária informou não saber o que é isso e comentou: "firewall é fogo em inglês?" E não soube realizar a atividade. Na atividade 6, "*Navegar anônimo*", após a usuária ter tentado sem sucesso executar essa ação, o pesquisador esclareceu a atividade, e ela em seguida perguntou: "*então quem usa a internet com má-fé usa sempre esse modo anônimo? Se eu quiser entrar no Tinder, devo entrar no modo anônimo? Estou viúva né...".* Apesar de ter consiguido realizar a ação, não soube explicar com clareza o propósito dessa função. Na atividade 7, "*Realizar logout após o término das atividades*", a participante conseguiu concluir a atividade e

comentou: “*login é quando eu quero acessar alguma coisa, quando eu quero acessar o yahoo eu faço login, e logout é pra sair*”, e também comentou que não costuma esquecer seus perfis logados em plataformas. Na ação 8, “*Mover cursor do mouse sobre a url antes de clicar*;” a usuária não conseguiu realizar a ação e disse: "*não, não faço isso não, talvez eu já tenha feito, mas não lembro não*", e não conseguiu realizar a atividade. Usuária informou: "*já vi esse link no canto inferior esquerdo do navegador, mas nunca me liguei*". Na ação 9, “*Identificar conteúdo phishing*”, ela conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*eu não clicaria nessa mensagem não, se recebesse, tá faltando ‘cadeadinho’, eu ficaria com o pé atrás, sempre me liguei no cadeado, ninguém nunca me falou, mas eu deduzia que era segurança*". Na última ação, 10, “*Definir senha forte*”, a usuária digitou uma senha inédita, e também frágil, ela disse: *"senha grande é mais fácil de esquecer, por isso todo mundo usa senha fraca"* e também comentou*: "Quando eu desconfio do site, eu digito uma senha falsa, se ele concordar, é porque o site é falso".*

A voluntária teve um desempenho bom e acima da média, e seu percentual de (40%) de conclusão das atividades ficou acima da média do grupo etário (22%) do qual se enquadrava.

Usuária idosa10

A usuária Idosa10, mulher, 70 anos e de nível superior, técnica administrativa, executou as ações em sua residência por meio de vídeoconferência com o pesquisador numa tarde do dia 12/06/2020.

A usuária foi convidada a participar da pesquisa por *Whatsapp*, já que era do círculo social do pesquisador. A usuária aceitou participar da pesquisa. E ela própria preparou o ambiente para os testes.

Na atividade 1, “*Analisar ícone de cadeado fechado que é indicado pelo navegador*”, a voluntária conseguiu realizar a ação, e quando perguntada sobre o objetivo do símbolo do cadeado, conseguiu informar corretamente que “*serve para indicar que o site é seguro*”. A usuária persistiu por mais de dois

minutos até conseguir realizar a ação, tendo concluído com sucesso. Na atividade 2, “*Analisar prefixo de HTTPS*”, a usuária conseguiu encontrar esse prefixo. Ela levou um tempo considerável até conseguir concluir. Também não conseguiu explicar o acrônimo, mas deduziu: “*https tem algo a ver com a segurança do site*”. Na atividade 3, “*Verificar certificado de segurança*”, a usuária não conseguiu localizar o item, e comentou: “*não sei onde fica essa opção, essa parte de segurança eu não sei muito bem”.* Na atividade 4, “*Analisar nome de domínio*”, a usuária não conseguiu explicar o que é nome de domínio de um site, com isso, não concluiu a atividade. Na atividade 5, “*Verificar firewall*”, a usuária persistiu em tentar encontrar essa opção no sistema operacional, mas não conseguiu concluir, tendo desistido da atividade e informado não ter conseguido finalizar a ação. Na atividade 6, “*Navegar anônimo*”, após a usuária ter tentado sem sucesso executar essa ação, o pesquisador esclareceu a atividade, e ela em seguida comentou: “eu já tinha ouvido falar nessa navegação anônima, mas nunca precisei fazer”. Na atividade 7, “*Realizar logout após o término das atividades*”, a participante conseguiu concluir a atividade e soube explicar corretamente essa função. Na ação 8, “*Mover cursor do mouse sobre a url antes de clicar*;” usuária não conseguiu realizar a ação e disse: "isso eu nunca precisei executar não”. Na ação 9, “*Identificar conteúdo phishing*”, ela não conseguiu detectar os problemas de segurança que estavam na imagem que foi exibida, e comentou: "*não vejo nada de diferente não, mas eu não acessaria porque não acesso nada de banco que chega no meu e-mail”.* Na última ação, 10, “*Definir senha forte*”, a usuária digitou uma senha inédita, mas que era frágil, ela disse: *"digito uma senha que eu consiga lembrar, não uso senhas muito grandes”.*

A voluntária teve um desempenho abaixo da média, e seu percentual de (30%) de conclusão das atividades ficou acima da média do grupo etário (22%) do qual se enquadrava.

4.2.2.3 Análise dos resultados

Nesta etapa os resultados do processo de teste com os usuários serão sintetizados, na Tabela 11

1. Conclusão ou não da ação;
2. Tempo de conclusão de cada ação;
3. Média de acertos por usuário;
4. Média de acertos do grupo de terceira idade;
5. Percentual de conclusão por tarefa.

Público: idosos

TABELA 11 - INFORMAÇÕES SOBRE A CONCLUSÃO DE CADA AÇÃO PELO PÚBLICO IDOSO

Tarefas	**Situação da Ação – Concluída ou Não Concluída.**										**%T**
	Idosa1	**Idoso2**	**Idosa3**	**Idoso4**	**Idoso5**	**Idosa6**	**Idoso7**	**Idoso8**	**Idosa9**	**Idosa10**	
T1 – Verificar cadeado;	Sim	Sim	Não	Não	Sim	Não	Não	Não	Sim	Sim	50%
T2 – Verificar HTTPS;	Não	Não	Não	Não	Sim	Não	Não	Não	Não	Sim	20%
T3 – Verificar certificado de segurança;	Não	Não	Não	Não	Não	Não	Sim	Não	Sim	Não	20%
T4 – Verificar domínio;	Sim	Sim	Não	Não	Sim	Não	Não	Não	Não	Não	30%
T5 – Verificar firewall;	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	0%
T6 – Navegar anônimo;	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	0%
T7 – Realizar Login e logout;	Sim	Sim	Não	Sim	Sim	Sim	Não	Sim	Sim	Sim	80%
T8 – Cursor do mouse/url;	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	10%
T9 – Identificar *phishing*;	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Não	10%
T10 – Força de senha.	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	0%
Acertos por usuário:	**40%**	**30%**	**0%**	**10%**	**40%**	**10%**	**10%**	**10%**	**40%**	**30%**	
Média de acertos (%):	**22%**										**22%**
Sim - Concluído. Não - Não concluído. %T – Percentual de conclusão da tarefa.											

Fonte: levantamento de dados.

A tabela 11, com as informações sobre o percentual de conclusão por ação pelo público *idoso***,** indica que as atividades com menor percentual de acertos foram a de *Força de senha* (0%) e *verificar firewall* (0%). Logo após a navegação anônima com (0%), verificar destino da *url* antes de clicar na mesma com (10%), identificação de *phishing* (10%) e verificação de *https* (20%). A de verificar certificado de segurança teve 20%, verificação de domínio teve 30%, e verificar cadeado de segurança teve 50% de acertos e por último a realização de *login* e *logout* com 80%. Na média, os usuários idosos conseguiram realizar 22% das atividades apresentadas.

Foi verificado, no que se refere às atividades com menor percentual de acertos (*definir senha forte* e *verificar firewall*), que este número de 0% se deve, provavelmente, ao fato de que os voluntários preferem utilizar senhas simples, porque facilita a memorização, e quanto à segunda atividade, quase todos os usuários não sabiam o que era *firewall*, e dos que sabiam, tiveram dificuldades de localizar no sistema operacional.

No que se refere à atividade de navegação anônima, a maior parte dos usuários não sabiam do que se tratava, sendo que alguns ainda opinavam com a finalidade de tentar explicar, e alguns acertaram, dado que o próprio nome da atividade faz alusão ao significado dela. Porém, é uma funcionalidade pouco utilizada por este público, o que resultou no baixo número de acertos.

Quanto à atividade de verificar destino da *url* antes de clicar na mesma, também foi constatado que é uma atividade pouco realizada por este público, o que, de certa maneira, os torna mais vulneráveis a ameaças que buscam ocultar uma *URL* em um rótulo de endereço na internet.

A atividade de analisar prefixo *https* obteve um percentual baixo também, e um dos motivos, provavelmente, é o fato de que alguns usuários não utilizavam o *browser* para acessar serviços digitais de forma habitual, mas sim os próprios *apps* disponíveis no *Android* em seus *smartphones*, que já utilizam esse recurso por padrão.

Na atividade de *phishing,* 90% dos voluntários não conseguiram identificar itens suspeitos em uma mensagem maliciosa*.* Mas*,* apesar de não terem conseguido identificar, afirmaram não clicar em qualquer *link* que recebem por e-mail.

A atividade de verificação de domínio trouxe à tona o fato de que muitos usuários não conhecem essa denominação, porém, quando foi solicitado que localizassem o nome do site em que se encontravam, a maior parte conseguiu realizar normalmente.

A atividade de verificação de certificado de segurança trouxe um pouco de dificuldade para os voluntários, haja vista, que é um recurso que não está acessível de imediato, dessa forma, o usuário precisa executar alguns passos para acessá-lo, e esse fato foi responsável pelo baixo número de acertos.

A atividade de verificar o cadeado de segurança parece ser mais comum entre os usuários idosos do que as atividades anteriores, levando-se em conta que os voluntários que acertaram a atividade, informaram que é o primeiro ato que realizam ao acessar um serviço digital que envolve dados sensíveis.

A realização de *login* e *logout* foi a atividade que obteve o maior percentual de acertos entre elas, haja vista ser bastante corriqueiro o uso de redes sociais por parte deste público, o que acaba demandando a execução dessa atividade sucessivas vezes para o acesso aos seus perfis sociais.

TABELA 12 - INFORMAÇÕES SOBRE O TEMPO DE CONCLUSÃO DE CADA AÇÃO PELO PÚBLICO IDOSO

Tarefas	**Tempo de Conclusão (em minutos)**									
	Idosa1	**Idoso2**	**Idosa3**	**Idoso4**	**Idoso5**	**Idosa6**	**Idoso7**	**Idoso8**	**Idosa9**	**Idosa10**
T1 – Verificar cadeado;	00:32	00:50	N/A	N/A	00:09	N/A	N/A	N/A	00:24	02:38
T2 – Verificar HTTPS;	N/A	N/A	N/A	N/A	00:36	N/A	N/A	N/A	N/A	03:09
T3 – Verificar certificado de segurança;	N/A	N/A	N/A	N/A	N/A	N/A	01:03	N/A	00:20	N/A
T4 – Verificar domínio;	00:25	00:33	N/A	N/A	00:15	N/A	N/A	N/A	N/A	N/A
T5 – Verificar firewall;	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
T6 – Navegar Anônimo;	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
T7 – Realizar login e logout;	00:26	00:30	N/A	00:23	00:10	00:15	N/A	00:11	00:06	00:10
T8 – Cursor do mouse/url	00:25	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
T9 – Identificar *phishing*;	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	01:14	N/A
T10 – Força de senha.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Tarefas não concluídas (%)	60%	70%	100%	90%	60%	90%	90%	90%	60%	70%
N/A – Não aplicável: usuário não compreendeu a tarefa ou não teve sucesso na conclusão.										

Fonte: levantamento de dados.

Em relação à tabela 12 que contém o tempo demandado para execução de cada atividade, pôde-se constatar que houve bastante variação em razão do conhecimento que cada usuário tinha sobre o tema.

Em algumas atividades o tempo não foi contabilizado, pois o usuário optou por não realizar a ação, por não saber do que se tratava o item.

Considerando que alguns dados não puderam ser preenchidos, optou-se por não criar *rankings*, gerar totais gerais ou fazer comparações acerca do tempo das tarefas, mas tão somente registrar o tempo de conclusão de cada tarefa dos voluntários.

5 – RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO

Dados e resultados considerados para elaboração das recomendações

Para a elaboração das 25 recomendações que estão distribuídas por 13 categorias, foram considerados os resultados da análise do grupo de terceira idade na etapa qualitativa e também os resultados obtidos com a etapa quantitativa, os quais identificaram que:

1) O grupo avaliado teve dificuldades em conseguir realizar determinadas ações por conta própria;

2) O grupo avaliado teve dificuldades em conservar hábitos sobre a tomada de medidas de segurança da informação na internet;

3) O grupo avaliado teve dificuldades na instalação de ferramentas de segurança em seus dispositivos;

4) Média do percentual de conclusão das atividades foi de 22%, que é um número baixo.

Análise geral e recomendações

Categoria 1 - Fornecer informações sobre as ameaças de senhas frágeis

Grandes corporações especializadas em segurança analisam a senha com base em alguns critérios: uma senha simples composta por 6 números pode ser quebrada por um computador entre 25 microssegundos e 2 minutos (PASSWORDMETER, 2020), (KASPERSKY, 2020) e (SECURITY, 2020), além de terem uma alta probabilidade de estarem contidas em banco de dados vazados. Já uma senha um pouco mais robusta, composta de 12 caracteres, incluindo letras minúsculas e maiúsculas, bem como um caractere especial, já pode elevar o tempo de comprometimento da senha entre 3 meses e 34 mil anos, dependendo da capacidade computacional empregada (SECURITY, 2020) e (KASPERSKY, 2020).

Durante a execução da atividade, “*Definir senha forte*”, junto aos voluntários de terceira idade, nenhuma das senhas criadas por eles atingiu os critérios necessários para serem consideradas como forte, por meio da ferramenta on-line utilizada para aferição da força da senha (http://www.passwordmeter.com/).

Alguns usuários nessa etapa afirmaram só configurarem senhas fortes quando requerido pela plataforma. Além de anotá-las em pedaços de papéis, *post-its* e deixá-los sobre a mesa, e até mesmo anotá-las em ferramentas de organização de informações pessoais *on-line*.

Muitos usuários alegaram utilizar senhas que tenham algum sentido para elas, como datas de aniversário, nomes de animais de estimação, nome de entes queridos, entre outros.

Com isso, e em razão do percentual de conclusão de 0% verificado na atividade, *definir senha forte,* realizada pelos voluntários na etapa qualitativa, além das recomendações da (ABAP, 2020), no sentido de reforçar as senhas pessoais, recomenda-se que usuários sejam:

1. instruídos quanto às ameaças que permeiam senhas frágeis;
2. quanto ao risco de adoção de senhas que sejam deduzíveis facilmente por terceiros;
3. quanto à limpeza de suas mesas e eliminação de *post-its* com senhas;
4. e também, quanto a registrar dados sensíveis em bases de dados pela internet.

Categoria 2 - Fornecer informações sobre as ameaças que decorrem da ausência de ferramentas de *firewall* e *anti-malware*.

Negligenciar uma ferramenta de segurança como o *firewall* pode tornar uma organização ou um usuário mais suscetível a ataques cibernéticos. Uma situação que ilustra isso ocorreu entre o ano de 2005 e 2019, quando um atacante comprometeu e expôs 106 milhões de informações de cartões de

crédito de clientes da *Capital One*; o atacante, alegadamente, explorou um *firewall* incorretamente configurado (NTSC, 2020).

Somado a isso, os usuários ainda carecem de conhecimentos para avaliar suas ferramentas de *firewall* e *anti-malware* e, o número de ameaças digitais tem aumentado (BROADCOM, 2019) e (DHAMIJA at el. 2006).

Por não estarem sob a proteção de um *firewall* corporativo, muitos usuários que estão trabalhando via *home-office* devido a COVID-19, se tornam alvos mais fáceis para os criminosos, já que no ambiente doméstico as camadas de segurança são mais frágeis (SOPHOS, 2020).

No teste qualitativo realizado na atividade "*Verificar firewall*", nenhum voluntário conseguiu verificar a situação de seu *firewall*. Alguns voluntários achavam que essa funcionalidade era do próprio navegador *Chrome*.

Com isso, recomenda-se instruir os usuários sobre:

1. conceitos básicos de *firewall* e ferramentas *anti-malware*;
2. procedimentos de verificação de *firewall* e de ferramentas *anti-malware* em seus computadores pessoais.

Categoria 3 - Fornecer recomendações sobre ameaças que as *urls* recebidas pela internet podem trazer

Verificar o destino de uma *url* antes de acessá-la diminui o risco de segurança do usuário. Em 2017, a cada dezesseis *urls*, uma era maliciosa; em 2018, houve um salto, e uma *url* a cada dez passou a ser maliciosa, aumentando mais ainda o risco de segurança (BROADCOM, 2019).

Outro fato que corrobora isso, é que se tratando de *phishing url*, foram registradas uma a cada 170 em 2018 e também 273.782.113 *urls* maliciosas, que são aquelas *urls* que redirecionam os usuários para outras páginas nocivas, além de 24.610.126 objetos maliciosos, tais como *scripts*, arquivos executáveis, *exploits*, etc. (BROADCOM, 2019) e (KASPERSKY, 2019).

Para contornar isso, existem ferramentas que checam se uma *URL* ou um website contêm formulários nocivos, páginas ofensivas, objetos ou

conteúdos maliciosos, ajudando a reduzir o risco de segurança do usuário (GEEKFLARE, 2020).

Muitos usuários não conhecem os meios para superar essa ameaça; isso pôde ser visto durante a execução da ação "*Mover cursor do mouse sobre url antes de clicar;*" junto aos voluntários. Noventa por cento dos usuários não sabiam que ao passar o *cursor* do *mouse* sobre um *link,* receberiam uma prévia sobre o destino ao qual o *link* o levaria no canto inferior esquerdo do navegador. Com isso, muitos acessavam *links* sem saber de antemão sobre a legitimidade ou não dos endereços, tornando-os mais vulneráveis a ataques.

Um outro recurso importante, mas que nenhum usuário da amostra conhecia, eram as ferramentas de "*website malware scanning"* – ou *scanner* de *websites* - para endereços suspeitos na internet, que também ajuda a mitigar esse risco.

No total, apenas 1 voluntário conseguiu concluir essa ação; portanto, recomenda-se instruir usuários a:

1. manterem uma ferramenta *anti-malware* instalada e atualizada;
2. lançarem mão dessas ferramentas de checagem de *links* para mitigarem os riscos de ataques;
3. terem cautela ao acessar endereços na internet.

Categoria 4 - Fornecer recomendações sobre a privacidade ao navegar pela internet

A navegação anônima não garante total anonimato, mas mitiga em algum nível o risco de violação da privacidade (VARONIS, 2020). Esse tipo de navegação, em algumas situações, diminui a quantidade de informação que é exposta pelo usuário ao navegar na internet por meio de seu dispositivo, diminuindo o impacto de ataques de criminosos que buscam coletar informações pessoais e documentos para depois fazerem uso desses dados de forma ilegal (CISCO, 2016).

Buscando aferir o conhecimento dos voluntários sobre esse tópico, foi criada a atividade: “*Navegar anônimo*”, nenhum usuário conseguiu realizar essa atividade.

Considerando o percentual de insucesso na atividade de navegação anônima pelos voluntários, recomenda-se instruir os usuários, principalmente, aqueles que compartilham os seus dispositivos com outras pessoas ou utilizam computadores públicos a:

1. experimentarem essa funcionalidade, para reduzir a exposição de suas informações pessoais em computadores compartilhados.

Categoria 5 - Recomendações sobre ameaças decorrentes da ausência de protocolos seguros de hipertexto ao navegar na internet.

Aparentemente, atacantes tem como alvo protocolos mais frágeis. Entre 2018 e 2019, o protocolo *http* foi o segundo mais atacado com 6.6 pontos percentuais (6.6%), enquanto que o protocolo *https* obteve apenas 1 ponto percentual (1%) numa ordem de 100 pontos percentuais (100%), sendo que outros protocolos foram responsáveis pelos demais ataques (BROADCOM, 2019). O protocolo *http* expõe usuários a ameaças quando não combinado com uma criptografia adequada. Esse protocolo funciona por padrão na porta 80, ficando à frente da porta 443 em termos de quantidade de ataques recebidos; a porta 443 está, normalmente, associada ao *https* para fornecer criptografia à conexão (BROADCOM, 2019).

Apesar do uso da porta 443 com *https* prover criptografia, cerca de 20% dos 502 maiores sites do mundo ainda não tinham implementado essa função até 2018, colocando em risco as informações dos usuários, mesmo não havendo dados sensíveis a serem trocados com a outra ponta (WHYNOHTTP, 2020) e (AVIRA, 2018).

Para aferir o conhecimento dos voluntários sobre a verificação da criptografia de suas conexões ao navegar na internet, foi criada uma atividade denominada “*verificar https”,* que foi conduzida durantes os testes com usuários. Apenas dois usuários conseguiram concluir essa ação.

Considerando o número de 20% de sucesso obtido na etapa qualitativa sobre a atividade de verificar *https* do site no navegador pelos voluntários idosos, recomenda-se que os usuários sejam instruídos a:

1. analisarem essa opção ao acessar um site que envolva a troca de dados pela rede, mesmo que os dados a serem trocados com a outra ponta não sejam sensíveis.

Categoria 6 - Recomendações quanto às ameaças de um site sem certificado de segurança ou com certificado inválido.

O uso de certificados de segurança *SSL* são importantes pois garantem autenticação; dessa forma, apenas um receptor habilitado poderá receber a informação, mitigando o risco de violação dos dados (PARTEK, 2020).

Para aferir o conhecimento dos voluntários acerca desse tema, foi criada uma atividade denominada "*Verificar certificados de segurança*"; nesta atividade, apenas dois usuários conseguiram concluir a atividade, mas nenhum deles soube explicar com clareza a finalidade desse recurso.

A ausência de um certificado de segurança pode representar um risco para o usuário, que pode submeter suas informações a um destinatário que não seja legítimo.

Considerando o percentual de conclusão de 20% dessa atividade, recomenda-se instruir os usuários a:

1. realizarem o procedimento de verificação dos certificados nas páginas, isto é, se eles existem e se são válidos.

Categoria 7 - Recomendações quanto às ameaças de troca de dados com um *site* sem criptografia (em que o navegador não exibe o símbolo do cadeado).

O símbolo do cadeado indica que a conexão é criptografada, e isso é importante para que os dados estejam seguros. Para se ter uma ideia, quase 50% de todo o tráfego da internet não é criptografado, o que aumenta a suscetibilidade dos usuários trocarem as suas informações pessoais em texto plano com a outra ponta (SANDVINE, 2018).

Durante os testes com usuários, os voluntários foram encarregados de executar uma atividade denominada “*Verificar cadeado*”, com o intuito de aferir o conhecimento sobre o tema. Cinco voluntários conseguiram localizar esse símbolo, porém apenas dois conseguiram explicar de forma mais aprofundada a sua função.

Dessa forma, considerando o resultado de 50% de sucesso na conclusão dessa atividade, recomenda-se instruir os usuários sobre:

1. implicações que o ato de transferir informações pela rede de maneira não criptografada pode acarretar.

Categoria 8 - Recomendações quanto às ameaças de um domínio adulterado

Em 2018, diversos domínios adulterados imitando sites pertencentes a organizações políticas foram desligados, sendo que os domínios mais comprometidos foram aqueles pertencentes à categoria que utiliza "DNS Dinâmico" (BROADCOM, 2019).

Adulterar o destino de um domínio a partir da troca ou violação de servidores de DNS também é uma prática comum, e servidores de DNS comprometidos podem afetar toda a rede, já que quando afetados são configurados para entregar nomes de domínios maliciosos aos computadores clientes (KASPERSKY, 2019).

Para aferir o conhecimento dos voluntários sobre esse tema, foi criada uma atividade denominada “*Analisar nome de domínio*”. Apenas três usuários conseguiram localizar e explicar a finalidade do domínio, o que pode representar um risco, já que é um indício de que esses usuários não dispensam a atenção necessária a esse recurso.

Considerando o baixo percentual de conclusão: 30% da atividade de verificar domínio por parte dos voluntários da pesquisa, recomenda-se instruir os usuários a:

1. utilizarem apenas servidores DNS confiáveis;
2. checarem e realizarem varredura dos domínios que apresentem indícios de nocividade antes mesmo de acessá-los;
3. dispensar uma atenção maior ao domínio em si, já que atacantes tentam confundir os usuários trocando caracteres de forma quase imperceptível;
4. tentar evitar ao máximo sites que estão sob a categoria de DNS Dinâmico.

Categoria 9 - Recomendações quanto à ação de realizar *login* e *logout*

Alguns usuários durante esta pesquisa mencionaram já ter esquecido os seus perfis abertos em redes sociais ou em caixas de mensagens em computadores compartilhados, como em *LAN Houses*. É possível que um usuário receba auxílio de alguém para efetuar *login* com a sua conta para utilização de algum serviço em uma determinada plataforma e, não receba auxílio para efetuar o *logout*; além de que alguns usuários têm as suas informações de *login* violadas, por meio da prática de *formjacking*[5].

Para aferir o conhecimento dos voluntários a esse respeito, foi criada uma atividade denominada: "*Realizar logout após o término das atividades*".

Do público avaliado, oito conseguiram executar essa funcionalidade; os outros não conheciam essa atividade como *login* e *logout*, mas como *acessar*

[5] A prática de *formjacking* consiste em adulterar formulários que são preenchidos com essas credenciais pelos usuários, com o objetivo de capturar essas informações de *login* ou bancárias de forma ilegal (BROADCOM, 2019).

ou *sair* da plataforma; 20% dos usuários não conseguiram realizar essa atividade. Sendo assim, recomenda-se:

1. instruir os usuários que não possuam essa habilidade a buscarem auxílio e orientação de pessoas de confiança;
2. ter cautela com *formjacking*;
3. nunca esquecer seus perfis abertos em computadores compartilhados ou em locais públicos.

Categoria 10 - Recomendações quanto a e-mails recebidos com propósitos nocivos, *phishing*.

Phishing é uma tentativa de obter dados sensíveis dos usuários, tais como senhas, dados de cartões de crédito, entre outros, através do ato de descrever a si próprio como alguém ou algum serviço digno de confiança. (NTSC, 2020).

Por se aproveitar do fator psicológico do usuário, ataques *phishing* são muito eficazes e, em 2016, o *phishing* figurava em sétimo lugar na categoria de *malwares* mais recorrentes, sendo assim, uma ameaça de ocorrência provável, não só em caixas de e-mail, englobando também mensagens por *SMS*, redes sociais e plataforma de jogos (CISCO, 2016) e (NTSC, 2020).

Para compreender o nível de conhecimento dos voluntários idosos acerca desse tema, foi criada uma atividade denominada: “*Identificar conteúdo phishing*”.

Nesta atividade, dos dez usuários que foram encarregados com a tarefa de identificar conteúdo malicioso em uma mensagem falsa, apenas um usuário conseguiu identificar, com segurança, objetos maliciosos na imagem apresentada, o que representa um risco a segurança deste público, mesmo apesar de muitos usuários terem afirmado não acessar conteúdo que desconheçam.

Alguns usuários comentaram que se o teor da mensagem contiver estímulos adequados e suficientes ou se esses usuários estivessem distraídos,

eles poderiam decidir acessar, mesmo tendo desconfiado da mensagem, aceitando o risco.

Considerando o baixo percentual de sucesso (10%) identificado na atividade de verificar *phishing*, recomenda-se:

1. instruir os usuários a olharem com ceticismo conteúdos que recebem;
2. adotar medidas preventivas com o intuito de evitar que o ataque se concretize.

Categoria 11 - Recomendações quanto à prevenção de ataques baseados em Engenharia Social

Nessa pesquisa, os voluntários afirmaram não conseguir realizar determinadas ações de segurança por conta própria, necessitando recorrer a terceiros para concretizar essas ações, fato que possui um risco de segurança associado, já que muitos atacantes se aproveitam dessa necessidade para tirar proveito, cometendo posteriormente atos ilícitos ou moralmente incorretos.

A pesquisa de (VIANA, 2017), de caráter quantitativo e a de (BOOTHROYD, 2017), qualitativa, também corroboraram esse fato, pois identificaram maior vulnerabilidade no grupo de terceira idade a ataques baseados em Engenharia Social; foi verificado que tais usuários são mais tendentes a confiar em terceiros.

Assim sendo, recomenda-se que:

1. os usuários sejam instruídos a não confiar a segurança de seus dados a desconhecidos.

Categoria 12 - Recomendações quanto à atitude de tomar medidas protetivas

Grande parte dos voluntários afirmaram tomar uma medida de segurança apenas quando percebem algum suporte de informática para apoiá-lo. Sendo assim, recomenda-se que os usuários:

1. Assegurem-se de que antes de realizar as suas ações na internet, tomem as medidas necessárias para garantir que o seu computador não tenha sido comprometido com *malware* que possa prejudicá-lo ou afetar o dispositivo de terceiros, buscando na internet fontes de informação que possam substituir um suporte de segurança.

Categoria 13 - Recomendações quanto à adoção de hábitos seguros na internet

Mudar um hábito é uma tarefa difícil, e para que isso ocorra, é necessário que o usuário possua os estímulos necessários que o farão tomar essa decisão e o manterão na conduta correta. A maior parte das respostas do grupo de terceira idade sobre a variável *suscetibilidade à ameaça,* foi no sentido de que *discordam parcialmente* que estão suscetíveis a ameaças. Já na assertiva referente a *normas subjetivas*, a maior parte das respostas foi no sentido de *se importarem com a opinião de pessoas próximas sobre os cuidados que devem ser tomados*. Sendo assim, recomenda-se:

1. Nos avisos de segurança, utilizarem essas premissas como um gatilho para estimular os usuários a mudarem o seu comportamento em relação a algum aspecto de segurança da informação, como por exemplo: afirmar que a atitude deste usuário pode influenciar na segurança da informação de um outro usuário próximo; um exemplo corriqueiro é quando um usuário compartilha um *link* malicioso com um familiar ou uma pessoa próxima, que acarreta na contaminação do computador deste familiar com vírus.

6 - CONCLUSÃO

A presente pesquisa, de caráter exploratório, baseou-se em uma parte quantitativa com idosos de 70 anos ou mais, e em uma parte qualitativa, realizada também com voluntários de terceira idade, com o objetivo de compreender o comportamento em segurança da informação dos usuários de internet, tendo como resultado a proposta de recomendações de segurança da informação.

Foram consultados conceitos da literatura sobre segurança da informação, teorias comportamentais e contexto de uso das TICs e como os mesmos têm sido relacionados ao comportamento dos usuários no contexto doméstico.

Para a conclusão do objetivo da pesquisa foi utilizada a *Teoria da Motivação Para a Proteção,* que foi escolhida em razão de uma pesquisa conduzida por (JANSEN & VAN SCHAIK, 2017), que constatou que essa teoria explicou até 64% da variância no comportamento dos usuários em segurança da informação. Também foi aplicado um questionário para a coleta de dados e para a posterior descrição dos resultados obtidos, tendente a identificar diferenças no comportamento entre os voluntários envolvidos.

Para se chegar ao objetivo principal foi necessário também analisar as variáveis que influenciam o comportamento em segurança da informação no uso das TICs à luz da Teoria da Motivação para a Proteção, foram construídos alguns gráficos, descrevendo, estatisticamente, o comportamento dos usuários em relação às variáveis da teoria estudada.

Para identificar as principais vulnerabilidades comportamentais relacionadas à segurança da informação dos usuários, foi conduzida uma etapa de observação dos participantes, com o objetivo de aferir qualitativamente o comportamento do usuário em diversas ações de segurança da informação.

Durante a etapa de *observação dos participantes* foram identificadas as fragilidades dos usuários ao interagir com os itens de segurança da informação apresentados, o que possibilitou a elaboração de recomendações de

segurança da informação adequadas ao comportamento identificado. Essa etapa contou com entrevistas e testes com voluntários, que foram incumbidos de executar diversas ações em seus próprios computadores sob a observação do pesquisador.

Na aplicação do questionário, que contou com vinte respondentes, os resultados indicaram que o público de terceira idade negligenciou três questões: 1) Consigo instalar softwares de proteção mesmo não havendo ninguém para me ensinar, 2) Minhas informações pessoais já foram violadas e 3) Considero fácil tomar as medidas de segurança da informação necessárias; sendo uma associada à variável “Suporte de Segurança Percebido”, outra associada à “Experiência prévia com riscos de segurança” e a outra associada a variável “Autoeficácia”, respectivamente. Portanto, a identificação desses comportamentos foi importante, pois estimula a adoção de medidas direcionadas para o público do estudo.

A seção do questionário referente às perguntas sobre o perfil do usuário, trouxe à tona o fato de que o motivo de o usuário não utilizar a internet está associado a “*ter dificuldades para utilizar*” e não por “*não possuir internet*”, ou “*ter receio de que haja violação nos dados*”, ou outro motivo, considerando que a principal queixa do público idoso acima de setenta anos foi referente a dificuldades para utilização.

Já a *observação de usuários,* que contou com dez voluntários de terceira idade*,* possibilitou a construção de tabelas com o desempenho dos voluntários acerca das atividades de segurança, bem como, a obtenção de outros parâmetros importantes para compreensão das vulnerabilidades associadas ao uso da internet e, concluiu que esses voluntários ainda carecem de conhecimentos de conceitos básicos de segurança.

Foi conduzida uma análise geral para que as recomendações fossem mais apropriadas ao comportamento identificado na presente pesquisa. Como resultado, foram geradas 25 recomendações de segurança da informação, distribuídas por treze categorias. A quantificação do percentual de sucesso ou não das atividades executadas, permitem conhecer os pontos fracos dos usuários que mais demandam atenção, o que possibilita que as

recomendações, treinamentos ou orientações sejam mais reforçadas nesses pontos. Normalmente, as recomendações encontradas no mercado não levam em conta fatores que estimulam os usuários a tomarem as suas decisões de segurança, no momento de elaborar as orientações sobre o tema; nessa pesquisa, certos fatores que estimulam os usuários a mudarem o seu comportamento foram levados em conta para a elaboração de algumas recomendações.

Essas recomendações são importantes porque conscientizam os usuários e possuem potencial para ajudar na adoção de comportamentos mais seguros, o que poderá reduzir ocorrências relacionadas a crimes virtuais, violação de dados e outras condutas eticamente incorretas.

Como trabalhos futuros, sugere-se que na etapa de questionário, sejam envolvidos mais respondentes, com o intuito de refletir melhores resultados; também é recomendável utilizar todos os itens de mensuração da teoria para cada variável medida, isso fará com que a pesquisa seja fiel à proposta original do seu modelo.

Também é interessante, no que se refere a um estudo qualitativo, preparar mensagens e avisos de segurança para que sejam exibidos aos usuários durante uma seção simulada em uma página na internet ou intranet, para tornar as interações mais dinâmicas e ter percepções mais ricas acerca da efetividade que certos avisos e, mensagens de segurança podem trazer às atitudes dos usuários em tempo real.

A presente pesquisa teve limitações, uma delas é relativa ao fato de o pesquisador ter encontrado dificuldades para reunir respondentes idosos acima de setenta anos. O número de pessoas acima de setenta anos que faz uso da internet é baixo, e este parece ser um fato corriqueiro em outras pesquisas dessa mesma natureza.

Uma outra limitação diz respeito ao fato de que a etapa de *observação de usuários* não pôde ser realizada presencialmente em função da pandemia de COVID-19; dessa forma, todas as atividades relacionadas a essa etapa precisaram ser realizadas remotamente, sendo que alguns usuários tinham dificuldades na preparação do ambiente, já que era a primeira vez de muitos

voluntários em uma chamada de vídeo pela internet, alguns outros tiveram problemas em razão da oscilação de suas conexões, que ocorreu algumas vezes ao longo das sessões.

Apesar disso, a preocupação com as políticas públicas e privadas, no que se refere ao público da terceira idade e as tecnologias devem ser levadas em conta porque, possivelmente, todos faremos parte desse grupo etário futuramente.

Ter o entendimento dessas vulnerabilidades e comportamentos é importante para manutenção da segurança da informação desses usuários por meio de práticas adequadas.

7 - REFERÊNCIAS BIBLIOGRÁFICAS

AJZEN, I. (1985). **From intentions to actions: A theory of planned behavior**. In J. Kuhl & J. Beckmann (Eds.), Action control: From cognition to behavior. Berlin, Heidelber, New York: Springer-Verlag. (pp. 11-39).

APUKE, OBERIRI. (2017). **Quantitative Research Methods : A Synopsis Approach**. Arabian Journal of Business and Management Review (kuwait Chapter).. 6. 40-47. 10.12816/0040336.

ASSOCIAÇÃO BRASILEIRA DE AGÊNCIAS DE PUBLICIDADE. **Cartilha Institucional de Segurança da Informação e Prevenção a Fraudes**. 2020. Disponível em: http://www.abap.com.br/pdfs/seguranca_informacao.pdf/, Acesso novembro. 2020.

AVIRA. **20% of the world 502 largest websites do not use HTTPS**. 2018. Disponível em: https://www.avira.com/en/blog/20-of-the-world-502-largest-websites-do-not-use-https/. Acesso novembro. 2020.

BADA. M., SASSE. A., NURSE J.R.C. **Cyber security awareness campaigns: Why do they fail to change behaviour?**, International Conference on Cyber Security for Sustainable Society 2015 Conference paper; 2015. 118–31. 2015.

BARBER, NELSON. **How Self-Confidence and Knowledge Effects the Sources of Information Selected During Purchase Situations**. Graduate Faculty of Texas Tech University, Texas, 2008.

BECCARIA, C. (1963). **On Crimes and Punishments** (Introduction by H. Paolucci, Trans.). New York, NY: Macmillan.

BECKERS K, PAPE S. **A serious game for eliciting social engineering security requirements**, in: Proceedings of the 24th IEEE International Conference on Requirements Engineering, RE 16, IEEE Computer Society; 2016, pp. 16–25. 2015.

BENDOVSCHI, ANDREEA. **Cyber-Attacks – Trends, Patterns and Security Countermeasures**. Procedia Economics and Finance. 28. 24-31. 10.1016/S2212-5671(15)01077-1. 2015.

BILJON, JUDY., RENAUD, KAREN. **A Qualitative Study of the Applicability of Technology Acceptance Models to Senior Mobile Phone Users**. Multimodal Human Computer Interaction and Pervasive Services. 228-237. 10.1007/978-3-540-87991-6_28. 2008.

BLEEPINGCOMPUTER. **Brazil's court system under massive RansomExx ransomware attack**. 2020. Disponível em: https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/. Acesso novembro. 2020.

BOLFARINE, HELENO. Instituto de Matemática e Estatística (IME-USP). **Testes Qui-quadrado - Aderência e Independência**. 2012. Disponível em: https://www.ime.usp.br/~hbolfar/aula_2013/Aula11-QuiquadradoA12012.pdf, Acesso set. 2019.

BOOTHROYD, VANESSA., PATRICK, ANDREW., CHIASSON, SONIA. **Older adults' perception of online risk**. 2014.

BORITZ, J. **IS practitioners' views on core concepts of information integrity**. International Journal of Accounting Information Systems. 6. 260-279. 10.1016/j.accinf.2005.07.001. 2005.

BRASIL, 2000. Lei nº 10.097 de 19 de dezembro de 2000. Altera dispositivos da **Consolidação das Leis do Trabalho – CLT**, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Leis/L10097.htm>. Acesso em: 17 fev. 2020.

BRASIL, 2003. **Estatuto do idoso**. Lei nº 10.741, de 01 de outubro de 2003. Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm>. Acesso em: 10 jan. 2020.

BRASIL. **Constituição**. 1988, Seção II, Art. 40, § 1º, Inciso II. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 2 de jul. 2019.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, Acesso novembro. 2020.

BRASIL. **Planos de Benefícios da Previdência Social**. 1991. Seção V, Subseção II, Art. 51. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8213cons.htm. Acesso em 2 de jul. 2019.

BROADCOM. **Internet Security Threat Report**, 2019. Disponível em: https://docs.broadcom.com/doc/istr-24-executive-summary-en , Acesso jul. 2019.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros**. 2017. Disponível em: https://www.cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2017/ , Acesso jul. 2020.

CHANG, B. L., BAKKEN, S., BROWN, S. S., HOUSTON, T. K., KREPS, G. L., KUKAFKA, R., ... STAVRI, P. Z. **Bridging the digital divide: Reaching vulnerable populations**. Journal of the American Medical Informatics Association, 11, 448–457. 2004.

CHARNESS, N., BOOT, W. R. **Aging and information technology use: Potential and barriers**. Current Directions in Psychological Science, 18, 253–258. 2005.

CHEN, Y.R, SCHULZ, P.J. **The Effect of Information Communication Technology Interventions on Reducing Social Isolation in the Elderly: A Systematic Review**. J Med Internet Res. 2016;18(1):e18. Published 2016 Jan 28. doi:10.2196/jmir.4596, 2016.

CHERDANTSEVA, YULIA., HILTON, JEREMY. **A Reference Model of Information Assurance & Security**. Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013. 546-555. 10.1109/ARES.2013.72. 2013.

CISCO. **Cisco® 2016 Midyear Cybersecurity Report**. 2016. Disponível em: https://www.cisco.com/c/dam/m/en_ca/never-better/assets/files/midyear-security-report-2016.pdf. Acesso novembro. 2020.

CYBIS, W. **Ergonomia e usabilidade: conhecimentos, métodos e aplicações**. 2. ed. São Paulo: Novatec, 2010.

DANIELSSON, KARIN., LINDGREN, HELENA., MULVENNA, MAURICE., NILSSON, INGEBORG., WATERWORTH, JOHN. **Digital technology in healthcare and elderly care**. 188-190. 10.1145/3121283.3121425. 2017.

D'ARCY, JOHN., HERATH, TEJASWINI. **A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings**, European Journal of Information Systems, 20:6, 643-658, DOI: 10.1057/ejis.2011.23. 2011.

DEMPSTER, A. P.; LAIRD, N. M.; RUBIN, D. B. **Maximum Likelihood from Incomplete Data Via the EM Algorithm**. Journal of the Royal Statistical Society: Series B Methodological. 39 (1): 1–22. doi:10.1111/j.2517-6161.1977.tb01600.x. 1977.

DHAMIJA, RACHNA., TYGAR, J., HEARST, MARTI. **Why phishing works**. Conference on Human Factors in Computing Systems - Proceedings. 1. 581-590. 10.1145/1124772.1124861. 2006.

DUPUIS, MARC & CROSSLER, ROBERT. **The Compromise of One's Personal Information: Trait Affect as an Antecedent in Explaining the Behavior of Individuals**. 10.24251/HICSS.2019.584. 2019.

ECKERT, CORNELIA & ROCHA, ANA. (2008). **Etnografia: Saberes e Práticas**. ILUMINURAS. 9. 10.22456/1984-1191.9301.

EMC CORPORATION. **The year in phishing**. Technical report, EMC Corporation, 2013.

EMINAĞAOĞLU, M., UÇAR, E., EREN, S. **The positive outcomes of information security awareness training in companies – A case study**", Information Security Technical Report, Vol. 14 No. 4, pp. 223–229. 2009.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. INFORMATION SECURITY INDICATORS. **A security event classification model and taxonomy**. 2015. Disponível em: https://www.etsi.org/deliver/etsi_gs/ISI/001_099/002/01.02.01_60/gs_ISI002v010201p.pdf, Acesso dez. 2019.

FÁVERO ET AL. **Análise de dados: modelagem multivariada para tomada de decisões**. Rio de Janeiro: Elsevier, 2009.

FÁVERO, LUIZ PAULO LOPES; BELFIORE, PATRÍCIA PRADO. **Manual de análise de dados: estatística e modelagem multivariada com excel, SPSS e stata**. [S.l: s.n.], 2017.

FILIPPO, DENISE & PIMENTEL, MARIANO & WAINER, JACQUES. (2011). **Metodologia de pesquisa científica em sistemas colaborativos**.

FISHBEIN, M., & AJZEN, I. (1975). **Belief, attitude, intention and behavior: An introduction to theory and research**. Reading, MA: Addison-Wesley.

FLOYD, D. L., PRENTICE-DUNN, S., ROGERS, R. W. **A meta-analysis of research on protection motivation theory**. Journal of Applied Social

Psychology, 30(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x. 2000.

GEEKFLARE. **9 Awesome Tools for Website Malware Scanning**. 2020. Disponível em: https://geekflare.com/website-malware-scanning/, Acesso novembro. 2020.

GLOBAL HEALTH DATA EXCHANGE., **Global Burden of Disease Study**, 2017. Disponível em: http://ghdx.healthdata.org/gbd-2017, Acesso ago. 2019.
Grenade L, Boldy D. Social isolation and loneliness among older people: issues and future challenges in community and residential settings. Aust Health Rev. 2008;32(3):468-478. doi:10.1071/ah080468. 2008.

HOWE, ADELE & RAY, INDRAJIT & ROBERTS, MARK & URBANSKA, MALGORZATA & BYRNE, ZINTA. **The Psychology of Security for the Home Computer User**. Proceedings - IEEE Symposium on Security and Privacy. 209-223. 10.1109/SP.2012.23. 2012.

IBOPE NIELSEN. **Brasileiros Com Internet No Smartphone Já São Mais De 70 Milhões**. 2015. Disponível em: https://www.nielsen.com/br/pt/press-releases/2015/brasileiros-com-internet-no-smartphone-ja-sao-mais-de-70-milhoes/, Acesso outubro. 2019.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATISTICA - IBGE. **Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua**, 2018. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/trabalho/17270-pnad-continua.html?edicao=27138&t=downloads , Acesso jul. 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Projeção da População das Unidades da Federação por sexo e idade: 2000-2030**, revisão 2013. Disponível em: https://www.ibge.gov.br/, Acesso mar. 2020.

INSTITUTO QUALIBEST. **Hábitos da Terceira Idade na Internet**. 2012. Disponível em: https://www.institutoqualibest.com/, Acesso set. 2019.

INTERNATIONAL BUSINESS MACHINES CORPORATION - IBM. **Cost of a Data Breach Report**, 2019. Disponível em: https://www.ibm.com/security/data-breach , Acesso jun. 2020.

JAHANKHANI, HAMID., AL-NEMRAT, A., HOSSEINIAN-FAR, AMIN. **Cyber crime Classification and Characteristics**. 10.1016/B978-0-12-800743-3.00012-8. 2014.

JIANPING, LIU., WANG, JIAN., ZHOU, GUOMIN., ZHANG, GUILAN., YUNPENG, CUI., LIU, JUAN. **User's Scientific Data Retrieval Behavior Study Based on the Model of TPB**. CSAE 2019: Proceedings of the 3rd International Conference on Computer Science and Application Engineering. 1-6. 10.1145/3331453.3360951. 2019.

JOHNSTON, ALLEN., WARKENTIN, MERRILL., MCBRIDE, MARANDA., CARTER, LEMURIA. **Dispositional and situational factors: Influences on information security policy violations**. European Journal of Information Systems. 25. 10.1057/ejis.2015.15. 2016.

KASPERSKY. **Check your password**. 2020. Disponível em: https://password.kaspersky.com/. Acesso novembro. 2020.

KPOLOVIE, PETER., EWANSIHA, S., ESARA, M. **Continental Comparison of Human Development Index (HDI)**. 4. 9-27. 10.20431/2349-0381.0401002, 2017.

KUZEL, A.J. (1999). **Sampling in Qualitative Inquiry. In: Crabtrree**, B.F. and Miller, W.L., Eds., Doing Qualitative Research, 2nd Edition, Sage Publications, Thousand Oaks, 33-45.

LARSEN, K. R., EARGLE, D. (EDS.) (2015). **Theories Used in IS Research Wiki**. Disponível em: http://IS.TheorizeIt.org. Acesso em 2 de jul. 2019.

LEE, WAN-LIN., CHAN, DELPHINE. **Consumption Intention of Online Game based on Motivation Theory**. 10.2991/ichssd-17.2018.16. 2018.

LI, YING & SIPONEN, MIKKO. **A Call For Research On Home Users' Information Security Behaviour**. PACIS 2011 - 15th Pacific Asia Conference on Information Systems: Quality Research in Pacific. 112. 2011.

LI, YING. **Users' information systems (IS) security behavior in different contexts**. University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering Acta Univ. Oul. A 655, 2015.

M. JAMAL DEEN. **Information and communications technologies for elderly ubiquitous healthcare in a smart home**. Personal Ubiquitous Comput. 19, 3–4 (July 2015), 573–599. DOI:https://doi.org/10.1007/s00779-015-0856-x. 2015.

MADDUX, J. E., ROGERS, R. W. **Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change**. Journal of Experimental Social Psychology, 19(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9. 1983.

MALGARINOU M., GOULIA E. **The nurse close the elderly**. Ed. Tavitha, 4th edition, Athens, 1997.

MALTERUD, KIRSTI & SIERSMA, VOLKERT & GUASSORA, ANN DORRIT. (2015). **Sample Size in Qualitative Interview Studies: Guided by Information Power**. Qualitative Health Research. 1. 10.1177/1049732315617444.

MARTIN N MARSHALL. Sampling for qualitative research, Family Practice, Volume 13, Issue 6, 1996, Pages 522–526, https://doi.org/10.1093/fampra/13.6.522

MEDALERTHELP. **The Elderly and the World Wide Web**. 2018. Disponível em: https://medalerthelp.org/elderly-the-world-wide-web-infographic/, Acesso mar. 2020.

MIRANDA. JORGE MIGUEL PEREIRA COUTADA. **Sensing Technologies in Pervasive Healthcare: Evaluation and Design for Senior Citizens and Continuous Care**. 2019.

NARDI, CAROLINA CHRISTINA DO SACRAMENTO. **Recomendações Para Construção De Redes Sociais Inclusivas Ao Público Idoso**. 2016. 186 f. Dissertação (Mestrado em Informática) - Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

NEOGY, SARMISTHA. **Information security: course**. 1-8. 10.1145/3109761.3158397. 2017.

NEUMANN, LYCIA TRAMUJAS VASCONCELLOS, ALBERT, STEVEN M, **Aging in Brazil, The Gerontologist**, Volume 58, Issue 4, August 2018, Pages 611–617, https://doi.org/10.1093/geront/gny019, 2018.

OLIVEIRA, MARIA MARLY DE. **Como fazer pesquisa qualitativa**. 2ª ed. Petrópolis, RJ: Editora Vozes, 2008.

OMIDOSU, JOSEPH & OPHOFF, JACQUES. **A theory-based review of information security behavior in the organization and home context**. 225-231. 10.1109/ICACCE.2016.8073752. 2016.

PAK, RICHARD., PRICE, MARGAUX., THATCHER, JASON. **Age-Sensitive Design of Online Health Information: Comparative Usability Study**. Journal of medical Internet research. 11. e45. 10.2196/jmir.1220. 2009.

PARTEK. **Are websites without an SSL Certificate 'not secure' ?**. 2019. Disponível em: https://partek.ca/website-ssl-certificate/, Acesso novembro. 2020.

PASSWORDMETER. **The Password Meter**. 2020. Disponível em: http://www.passwordmeter.com/. Acesso novembro. 2020.

PATTON, M. Q. (2015). **Qualitative Evaluation and Research Methods**. Thousand Oaks, CA: Sage.

PEEK, S. T. M., LUIJKX, K. G., RIJNAARD, M. D., NIEBOER, M. E., VAN DER VOORT, C. S., AARTS, S., VAN HOOF, J., VRIJHOEF, H. J. M., WOUTERS, E. J. M. **Older Adults' Reasons for Using Technology while Aging in Place**. Gerontology, 62(2), 226–237. https://doi.org/10.1159/000430949. 2016.

PETER MAYER, ALEXANDRA KUNZ, AND MELANIE VOLKAMER. **Reliable Behavioural Factors in the Information Security Context**. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 9, 1–10. DOI:https://doi.org/10.1145/3098954.3098986. 2017.

PEWRESEARCH. **Tech Adoption Climbs Among Older Adults. Technology use among seniors**, 2017. Disponível em: https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors/, Acesso mar. 2020.

PORTAL ACTION. **Teste Exato De Fisher**. 2019. Disponível em: http://www.portalaction.com.br/tabela-de-contingencia/teste-exato-de-fisher, Acesso ago. 2019.

RAINIE L, KIESLER S, KANG R, MADDEN M. **Anonymity, privacy, and security online**. Pew Research Center, <http://pewinternet .org/Reports/2013/Anonymity-online.aspx>; 2013.

RANGEL, THAÍS DE PAULO. **Imputação multipla de dados faltantes: exemplo de aplicação no Estudo Pró-Saúde**. 2013.

RIPPETOE, P. A., ROGERS, R. W. **Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat**. Journal of Personality and Social Psychology, 52(3), 596–604. https://doi.org/10.1037/0022-3514.52.3.596. 1987.

ROUPA, ZOE., NIKAS, MARIOS., GERASIMOU, ELENA., ZAFEIRI, VASILIKI., GIASYRANI, LAMPRINI., KAZITORI, EUNOMIA., SOTIROPOULOU, PINELOPI. **The use of technology by the elderly**. Health Sci J. 4. 2010.

SCHAIK, PAUL., JANSEN, JURJEN., ONIBOKUN, JOSEPH., CAMP, L., KUSEV, PETKO. **Security and privacy in online social networking: Risk perceptions and precautionary behaviour**. Computers in Human Behavior. 78. 10.1016/j.chb.2017.10.007. 2017.

SECURITY.ORG. How Secure Is My Password?. 2020. Disponível em: https://www.security.org/how-secure-is-my-password/. Acesso novembro. 2020.
Se-Hoon J. **Visual metaphor in advertising: is the persuasive effect attributable to visual argumentation or metaphorical rhetoric**?. Journal of Marketing Communications, 14(1), 59-73. 2008.

SENIORLIVING. **Technology for Seniors and the Elderly**. 2020. Disponível em: https://www.seniorliving.org/tech/, Acesso mar. 2020.

SHAJARI, MEHDI., ARBABI, SALAR. **Decentralized and secure delivery network of IoT update files based on ethereum smart contracts and blockchain technology**. 2019.

SILVA, EDENILDO MENDES. **Aceitação De Serviços De Saúde Móvel Por Idosos: Aplicação De Um Modelo No Cenário Brasileiro**. 2019. 125 f. Dissertação (Mestrado em Informática) - Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2019.

SLEGERS, KARIN., BOXTEL, MARTIN., JOLLES, JELLE. **Computer use in older adults: Determinants and the relationship with cognitive change over a 6 year episode**. Computers in Human Behavior. 28. 1-10. 10.1016/j.chb.2011.08.003. 2012.

SOPHOS. **Keeping You Secure Through the Coronavirus Pandemic**. 2020. Disponível em: https://www.sophos.com/en-us/content/coronavirus-pandemic.aspx, Acesso novembro. 2020.

STALLINGS, WILLIAN. **Cryptography and Network Security: Principles and Practice**, 6th Edition. 2014.

TAHERDOOST, H. **Understanding of e-service security dimensions and its effect on quality and intention to use**, Information and Computer Security, Vol. 25 No. 5, pp. 535-559. https://doi.org/10.1108/ICS-09-2016-0074. 2017.

TAYLOR, SHIRLEY., TODD, PETER. **Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions**. International Journal of Research in Marketing, Volume 12, Issue 2, Pages 137-155, ISSN 0167-8116, https://doi.org/10.1016/0167-8116(94)00019-K. http://www.sciencedirect.com/science/article/pii/016781169400019K. 1995.

TELECOM ITALIA MOBILE (TIM). **Youtube E Google São Queridinhos Dos Avós**. 2018. Disponível em: https://www.tim.com.br/sp/sobre-a-tim/sala-de-imprensa/press-releases/comercial-e-marketing/youtube-e-google-sao-queridinhos-dos-avos_, Acesso dez. 2019.

THE NATIONAL TECHNOLOGY SECURITY COALITION (NTSC). **CYBER SECURITY REPORT**. 2020. Disponível em: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf. Acesso novembro. 2020.

THOMPSON, N., MCGILL, TANYA., WANG, XUEQUN. **“Security begins at home”: Determinants of home computer and mobile device security behavior**. Computers & Security. 70. 376-391.10.1016/j.cose.2017.07.003. 2017.

TOKUDA, YASUHARU., HINOHARA, SHIGEAKI. (2008). **Geriatric Nation and Redefining The Elderly in Japan. International Journal of Gerontology** - INT J GERONTOL. 2. 154-157. 10.1016/S1873-9598(09)70003-1, 2008.

UNITED NATIONS. **World Population Ageing**, 2019. Disponível em: https://www.un.org/en/development/desa/population/publications/pdf/ageing/WorldPopulationAgeing2019-Highlights.pdf, Acesso fev. 2020.

VAPORTZIS E., CLAUSEN M.G., GOW A.J. **Older Adults Perceptions of Technology and Barriers to Interacting with Tablet Computers: A Focus Group Study**. Front Psychol. 2017;8:1687. doi:10.3389/fpsyg.2017.01687. 2017.

VARONIS. **Browsing Anonymously: Is It Really Anonymous?**. 2020. Disponível em: https://www.varonis.com/blog/browsing-anonymously/, Acesso novembro. 2020.

VIANA, JOSÉ AUGUSTO LOPES. **O uso das tecnologias de informação e comunicação na terceira idade e a vulnerabilidade à engenharia social**. 2017. 107 f. Dissertação (Mestrado em Administração) - Universidade Federal da Paraíba, João Pessoa, 2017.

VOGT, W. P. **Dictionary of Statistics and Methodology: A Nontechnical Guide for the Social Sciences**, London: Sage, 1999.

WALLACE, SARAH & GRAHAM, CHRISTIN & SARACENO, AMY. **Older Adults' Use of Technology. Perspectives on Gerontology**. 18. 50-59. 10.1044/gero18.2.50. 2013.

WHITMAN, MICHAEL & MATTORD, HERB. **Principles of Information Security**, 5th Edition. 2015.

WHY NO HTTPS. **Why No HTTPS?**. 2020. Disponível em: https://whynohttps.com/, Acesso novembro. 2020.

WORLD HEALTH ORGANIZATION. **Ageing and health. Factors influencing Healthy Ageing**, 2018. Disponível em: https://www.who.int/news-room/fact-sheets/detail/ageing-and-health, Acesso mar. 2020.

WORLD HEALTH ORGANIZATION. **World Report on Aging and Health**, 2015. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/186463/9789240694811_eng.pdf?sequence=1, Acesso mar. 2020.

ZHU, XINGZHEN., ZHU, PENG., QIU, YANMEI. **Research on the influence of fear appeals on APP users' privacy protection behavior**. IMMS '18: Proceedings of the 2018 International Conference on Information Management & Management Science. 200-205. 10.1145/3277139.3277172. 2018.

EMKE-POULOPOULOU I. **Greek elderly citizens**. Past, Present and Future. Ed Ellin, Athens, 1999.

APÊNDICE 1 - TERMO DE CONSENTIMENTO

Prezado voluntário, convidamos você a participar de um estudo sobre comportamento em segurança da informação na internet.

O estudo ocorrerá da seguinte maneira: você realizará algumas tarefas em um site da internet. Antes de começar cada tarefa, o observador dará a você algumas instruções. O observador fará a leitura das instruções remotamente sobre cada tarefa para tirar suas dúvidas. As tarefas poderão ser gravadas para que os dados possam ser analisados depois.

A sua participação é voluntária. Você pode desistir de participar a qualquer momento, sem sofrer penalidades.

Para garantir sua privacidade, a sua identidade não será revelada. Os resultados do estudo serão divulgados exclusivamente pelo pesquisador e por sua orientadora na literatura especializada ou em congressos e eventos científicos.

Quaisquer dúvidas a respeito dessa pesquisa, entre em contato com o pesquisador ou com a orientadora por e-mail:

Pesquisador: Felipe Saulo Rodrigues de Souza Catojo: felipecatojo@uniriotec.br

Curriculum Lattes: http://lattes.cnpq.br/9599317560014203

Orientadora: Simone Bacellar Leal Ferreira: simone@uniriotec.br

Curriculum Lattes: http://lattes.cnpq.br/0926018459123736

Declaração de Consentimento

Li as informações contidas neste documento antes de assinar este Termo de Consentimento. Declaro que toda a linguagem utilizada na descrição do estudo foi explicada e que recebi respostas para todas as minhas dúvidas. Confirmo que recebi uma cópia deste Termo de Consentimento. Compreendo que posso me retirar do estudo a qualquer momento, sem sofrer qualquer penalidade. Dou meu consentimento de livre e espontânea vontade para participar deste estudo.

_____ ____/_____/_____ Data

Assinatura do Participante

_____ ____/_____/_____ Data

Assinatura do Observador

APÊNDICE 2 - QUESTIONÁRIO

1a. parte do questionário - Dados gerais e uso da internet

1) Você acessa a internet?

( ) Masculino

( ) Feminino

2) Marque o motivo de você NÃO utilizar a internet

( ) Não tenho conexão com a internet

( ) Tenho receio de que meus dados sejam violados

( ) Tenho dificuldades para utilizar

( ) Outro

Descreva o motivo

_____

Levantamento de perfil

3) Qual a sua idade?

_____

4) Qual é o seu sexo?

( ) Feminino

( ) Masculino

( ) Prefiro não responder

2a. parte do questionário - Segurança da Informação

5) Eu troco as minhas senhas com frequência

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

6) Um vírus pode ser prejudicial

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

7) As minhas chances de ser infectado por vírus são altas

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

8) Minhas informações pessoais já foram violadas

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

9) Considero fácil tomar as medidas de segurança da informação necessárias

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

10) Acredito que um software de proteção possa ser útil para detectar e remover vírus

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

11) Acato a opinião das pessoas do meu círculo social sobre os cuidados que devem ser tomados ao conversar com desconhecidos na internet ou tomar outras medidas de segurança da informação.

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

12) Acredito que softwares para proteção e segurança possam causar problemas em outros programas no meu computador.

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

13) Tenho o hábito de tomar medidas de proteção na internet

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

14) Consigo instalar softwares de proteção mesmo não havendo ninguém para me ensinar

( ) Discordo totalmente

( ) Discordo parcialmente

( ) Não sei responder

( ) Concordo parcialmente

( ) Concordo totalmente

APÊNDICE 3 - AÇÕES DE SEGURANÇA

Ações de segurança da informação	
1	Analisar ícone de cadeado fechado que é indicado pelo navegador;
2	Analisar prefixo de *HTTPS*;
3	Verificar certificados de segurança;
4	Analisar nome de domínio;
5	Verificar *firewall*;
6	Navegar anônimo;
7	Realizar *logout* após o término das atividades;
8	Mover cursor do *mouse* sobre *url* antes de clicar;
9	Identificar conteúdo *phishing;*
10	Definir senha forte;