UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Eduardo Costa Takeuchi

Fatores humanos em cibersegurança: uma revisão sistemática da literatura

Uberlândia, Brasil

2023

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Eduardo Costa Takeuchi

Fatores humanos em cibersegurança: uma revisão sistemática da literatura

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Sistemas de Informação.

Orientador: Renan Cattelan

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Sistemas de Informação

Uberlândia, Brasil

2023

Eduardo Costa Takeuchi

Fatores humanos em cibersegurança: uma revisão sistemática da literatura

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Sistemas de Informação.

Renan Cattelan
Orientador

Professor

Uberlândia, Brasil
2023

Agradecimentos

Agradeço a todos os professores da Universidade Federal de Uberlândia que me ensinaram e ajudaram a me desenvolver ao longo de todo o curso de Sistemas de Informação. Meus agradecimentos ao professor Renan Cattelan pelo excelente trabalho com a orientação, disposição de tempo e condução desta monografia. Por fim, agradeço aos meus amigos e pais pelo apoio e encorajamento.

Resumo

A cibersegurança está presente em diversos cenários, mas é uma prática pouco explorada pela maioria dos usuários de computadores. Ela pode estar presente para os usuários domésticos, em empresas, bancos, universidades, hospitais, em inteligências artificiais e diversas áreas e setores. Para garantir que haja um bom funcionamento dos sistemas e não haja invasões pelos cibercriminosos, será necessário aplicar boas práticas no uso de sistemas para que os métodos de mitigação sejam eficazes e evitem diversos outros problemas relacionados, e por isso diversas diretrizes podem ser seguidas e colocadas em prática a partir de treinamentos efetivos. Com o passar dos anos a tecnologia vai evoluindo e novas ameaças vão surgindo. Os usuários precisam se adaptar às evoluções, tanto da tecnologia quanto de ameaças. Muitas deles conseguem entender possíveis cenários de ataque, mas grande parte não sabe como se defender. Este trabalho visa investigar, a partir de uma Revisão Sistemática da Literatura, a relação existente entre os fatores humanos com a cibersegurança, mostrando as situações que podem causar vulnerabilidades de sistemas e elencando diversas boas práticas para combater crimes cibernéticos e mitigar riscos.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

O sucesso (ou falha) de qualquer ataque cibernético depende de fatores técnicos, principalmente, mas também de fatores humanos. Muitos usuários que, de fato, se preocupam com a segurança da informação estão suscetíveis a diversas vulnerabilidades desconhecidas. Existem diversos softwares de defesa para usuários domésticos, estudantes ou pessoas que trabalham com o computador, o mais comum é o software de antivírus, porém, eles podem ser burlados ou contornados devido a ações equivocadas dos usuários. Existe um número significativo de pesquisas focadas em aspectos técnicos e tecnológicos de ataques maliciosos.

Quando se fala em segurança cibernética, ações e eventos causados pelo fator humano podem aumentar a taxa de vulnerabilidade nos sistemas ou aplicações. Devemos considerar as empresas como um ponto de atenção, pois nelas estão os usuários que podem ter diversas características físicas e psicológicas capazes de afetar diretamente a produtividade, podendo, como consequência, facilitar a exploração de vulnerabilidades nos sistemas. Treinar, educar e capacitar os colaboradores das empresas são pontos fundamentais para mitigar os ataques cibernéticos, principalmente os provindos de fontes externas.

Alguns estudos de campo foram desenvolvidos para examinar as interações dos usuários com programas de antivírus (AV) e vulnerabilidades à medida que ocorrem nos sistemas implantados. Esses experimentos de segurança caminham para uma intersecção com a área de Interação Humano-Computador (RAY, 2022) e geralmente envolvem a participação de pessoas, visando analisar, por exemplo, o comportamento do usuário e sua interação com softwares instalados, como antivírus, configurações do host e ambientes. Um dos estudos tinha como objetivo avaliar o desempenho de software AV e os fatores de riscos humanos de ataque de malware (LéVESQUE et al., 2018).

Outro estudo teve duração de 4 meses e envolveu 50 usuários de sistemas computacionais domésticos que concordaram em usar laptops que foram instrumentados para monitoramento de possíveis ataques de malware para coletar dados sobre o comportamento dos usuários. O estudo forneceu alguns *insights* interessantes e intuitivos sobre a eficácia do software de antivírus e fatores de riscos humanos. O estudo mostrou que o desempenho do antivírus foi considerado inferior em condições de vida real em comparação com testes realizados em condições controladas. Para os testes foram considerados conhecimentos de informática, o volume de uso da rede e atividade ponto a ponto.

Os computadores de mesa e laptops não podem ser os únicos mencionados neste estudo, há também os dispositivos móveis que atualmente tem crescido bastante na socie-

dade. Esses dispositivos, baseados em um sistema operacional específico, permitem que os usuários instalem uma grande variedade de aplicativos provindos de uma ou mais fontes como, as lojas de aplicativos oficiais de grandes empresas ou de fontes desconhecidas. Por um lado, esses aplicativos enriquecem as funcionalidades dos dispositivos, melhorando o cotidiano de seus usuários. Por outro lado, mercados de aplicativos, principalmente as fontes desconhecidas, podem prover uma fonte de diferentes tipos de malware disfarçados de aplicativos normais (LI, 2020).

Um dos tipos de ataques mais comuns atualmente e que vem causando prejuízos empresariais em larga escala são os ataques de *ransomware*, que cresceram dez vezes entre julho de 2020 e julho de 2021, sendo que cerca de 51% das organizações sofreram ataques de tecnologia operacional (OT) que afetaram a produtividade e 45% sofreram ataques de OT que colocaram em risco a segurança física de um funcionário (FORTIFIREWALL, 2022). Muitas organizações estão vulneráveis a diferentes tipos de ataques cibernéticos, apesar de se esforçarem para proteger suas redes e ainda terão de enfrentar diversos riscos, pois os invasores aprimoram o tipo de ataque em força, dificuldade de detecção e número. As organizações sempre serão alvo desse tipo de ataque, pois a quantidade de informações que são geradas todos os meses é de extrema importância para os invasores. E, apesar de todos os esforços, não basta apenas instalar um sistema de segurança, mas sim gerenciar e acompanhar constantemente as mudanças, que sempre virão ao longo dos anos, pois as principais causas vem de uma má programação e baixa manutenção nos sistemas, erros humanos e outros fatores. Ainda serão descobertas novas ameaças, pois novas tecnologias impactam no cenário de cibersegurança.

Como mencionado, aplicar treinamentos aos colaboradores para conter ameaças cibernéticas pode garantir uma camada a mais de segurança para a organização, pois o fator humano tem um grande peso sobre a cibersegurança, e deve-se ter muita atenção nesse ponto quando se fala em cibersegurança. Com todos esses cenários negativos, de ameaças, invasões e roubo de informações, é possível, contudo, extrair um lado positivo, pois a comunidade de segurança cibernética tem a capacidade de tomar iniciativas para conscientização e ações contra ameaças. Por exemplo, todos os anos são realizadas diversas conferências sobre cibersegurança, como a conhecida Conferência RSA, que reúne aproximadamente 45 mil pessoas e aborda diversos programas educacionais, palestras de profissionais de redes de computadores, programas acadêmicos e competições para estudantes de tecnologia. A existência de conferências como a RSA colabora para que as informações e conhecimentos sobre cibersegurança possam ser aproveitadas melhor pelos profissionais de cibersegurança, organizações e usuários comuns.

Os estudos dos artigos selecionados trouxeram uma visão mais clara de que invasões acontecem cotidianamente, e que os profissionais de segurança da informação, muitas vezes, não estão preparados para as ameaças, sejam as já existentes e conhecidas ou

as que ainda estão por vir. A partir desses estudos, também foi possível constatar que quase todas as empresas já sofreram algum tipo de ataque cibernético, seja por e-mail, acesso em alguma página infectada ou por downloads de arquivos infectados que foram realizados por algum colaborador. Todos esses tipos de ataques geram prejuízos para qualquer organização, muitas delas não estão preparadas e não sabem o que fazer, mas aquelas que receberam ataques e tiveram prejuízos, elas acabam optando por investir em segurança, montando uma infraestrutura contra a invasão, comprando sistemas de defesa e máquinas para realizar alguns tipos de bloqueios. Devemos lembrar que, montar apenas uma infraestrutura não será suficiente, devemos lembrar do fator mais crítico, que são as pessoas no meio tecnológico.

Considerando o exposto, o objetivo deste trabalho é investigar a relação entre comportamento do usuário na perspectiva conjunta das áreas de Segurança da Informação e Interação Humano-Computador, mais especificamente os fatores humanos e comportamentais que afetam a cibersegurança por meio de uma revisão sistemática da literatura. A ideia é relacionar diferentes estudos sobre fatores humanos em cibersegurança, buscando elencar os principais conceitos associados, bem como os conjuntos organizados de boas práticas, que possam ser empregados na interação com recursos de segurança computacional.

O restante desta monografia está organizado da seguinte forma: o Capítulo 2 descreve a metodologia adotada; o Capítulo 3 apresenta os resultados obtidos, com uma discussão acerca dos principais trabalhos estudados; por fim, o Capítulo 4 traz as conclusões e considerações finais sobre a pesquisa realizada.

2 Metodologia

Para atingir os objetivos propostos, foi empregada a técnica de Revisão Sistemática de Literatura em Ciência da Computação (RSL) (NEIVA; SILVA, 2016). Trata-se de uma metodologia específica para a área de Computação, voltada para identificar, analisar e interpretar trabalhos relacionados com uma ou mais questões específicas de pesquisa.

Segundo (NEIVA; SILVA, 2016), uma RSL envolve os seguintes passos:

1. **Definir as questões de pesquisa principais da revisão.**

   Nesse passo, (NEIVA; SILVA, 2016) explicam que precisam ser definidas as perguntas que balizarão a pesquisa.

   Então, foram definidas, no contexto deste trabalho, as seguintes questões de pesquisa (QPs):

   - QP01. Quais os principais conceitos associados ao tema proposto (fatores humanos em segurança da informação)?
   - QP02. Quais os principais fatores humanos e sociais que influenciam a cibersegurança e como esses fatores se relacionam?
   - QP03. Existem conjuntos consolidados de boas práticas (usabilidade, guidelines) que podem ser aplicados na interação com a tecnologia para melhorar a segurança da informação com relação à prevenção de ciberataques?

2. **Devem ser definidas as palavras-chave.**

   As palavras-chave foram baseadas utilizando as QPs e sinônimos. Portanto, com base nessa verificação, foram selecionadas as seguintes palavras-chave:

   - "cyber attack";
   - "privacy invasion";
   - "cyber security";
   - "psychology human factors";
   - "security and human factors";
   - "malware warnings";
   - "persuasion in technology system";
   - "risk communication";
   - "human computer interaction";

- "computer information security";
- "malware persuasion";
- "people interaction with machines and technology";
- "human factors and engineering psychologist";
- "social-psychological techniques the scammers themselves use";
- "concrete threats and vague threats";
- "users turned off browser malware warnings";
- "computer security";
- "safety and security measures cybersecurity";
- "cybercrime";
- "behavioral cybersecurity";
- "human-systems integration";
- "human and societal aspects of security and privacy";
- "social aspects of security and privacy";
- "vulnerability assessment";
- "cybersecurity behavior";
- "cybersecurity Metrics";
- "cyber risk";
- "human errors"; e
- "data privacy".

3. **Definir a string de busca.**

   O próximo passo é definir uma busca completa, em que cada palavra-chave foi combinada, gerando a seguinte string:

   (cyber OR attack) AND (privacy OR invasion) AND (cyber OR security) AND (psychology OR human OR factors) AND (security OR human OR factors) AND (malware OR warnings) AND (computers OR security OR human OR behavior) AND (persuasion OR technology OR system) AND (risk OR communication) AND (human OR computer OR interaction) AND (computer OR information OR security) AND (malware OR persuasion) AND (people OR interaction OR machines OR technology) AND (human OR factors OR engineering OR psychologist) AND (social OR psychological OR techniques OR scammers OR themselves OR use) AND (concrete OR threats OR vague) AND (computer OR security) AND (safety OR security OR measures OR cybersecurity) AND (cybercrime) AND (behavioral

OR cybersecurity) AND (human OR systems OR integration) AND (human OR societal OR aspects OR security OR privacy) AND (vulnerability OR assessment) AND (cybersecurity OR behavior) AND (cybersecurity OR metrics) AND (Cyber OR risk) AND (human OR errors) AND (data OR privacy).

4. **Definir as bases de busca.**

   De acordo com (NEIVA; SILVA, 2016), como essa definição depende da área da revisão sistemática, foram utilizadas as seguintes bases de dados para encontrar pesquisas:

   - Portal Periódico CAPES.
   - Google Scholar.

5. **Refinamento de string.**

   Para esse item, as strings definidas no item anterior foram utilizadas no Portal Periódico CAPES e no Google Scholar. Após a execução da string de busca, foi verificado se os artigos eram ou não relevantes, observando se os artigos relacionados tinham títulos chamativos relacionados ao tema. Se os resultados não forem satisfatórios, a string deve passar por melhorias, o que não foi o caso.

6. **Execução da string de busca nas bases.**

   Após a definição da string de busca e a utilização nas bases de dados, foram retornadas as informações referentes às buscas nas bases.

7. **Baixar e armazenar o resultado das buscas.**

   Todas as principais bases de busca permitem exportar um conjunto de resultados obtidos das pesquisas nas buscas de dados. O principal formato utilizado neste trabalho foi o Bibtex, para o gerenciamento de referências.

8. **Definir os critérios de inclusão e exclusão.**

   (NEIVA; SILVA, 2016) mencionam que nessa etapa, os artigos devem passar por critérios de exclusão e inclusão antes de irem para a próxima etapa de revisão. Assim, um dos critérios utilizados foi o idioma, sendo selecionados apenas artigos escritos em Inglês e Português. Outro critério adotado foi o de cunho temporal, sendo selecionados somente artigos publicados entre os anos de 2005 e 2022, que foi considerado pelo autor um intervalo suficiente para realizar a análise ora proposta.

9. **Seleção de artigos - Primeira Etapa - Análise por título e abstract.**

   Na primeira seleção, foram observados os títulos dos artigos, para ver se estavam mencionando fatores humanos com cibersegurança e se tinham algo relacionado

com as questões de pesquisa. Neste caso foram analisados 75 artigos e 50 deles conseguiram passar pela análise de título (veja em Figura 1, Passo 9).

10. **Seleção de artigos - Segunda Etapa - Análise por Introdução e Conclusão.**

    Na segunda seleção, que foi combinada com a primeira etapa de sobre seleção de artigos, analisando-se as introduções e conclusões dos artigos. Na Tabela 1, esse item se refere à coluna de "Analisados". Neste passo, os critérios analisados foram verificados se as informações contidas na Introdução e Conclusão dos artigos tinham informações relevantes. Foram analisados 50 artigos obtidos no Passo 9, dos quais 25 foram selecionados, pois seus conteúdos eram os que mais se aproximavam de responder às questões de pesquisa. (veja em Figura 1, Passo 10).

11. **Seleção de artigos - Terceira Etapa - Leitura completa e checklist de qualidade.**

    Na terceira seleção, foram realizadas leituras completas dos artigos selecionados no Passo 10, verificando se as informações contidas eram relevantes para a monografia. Conforme a Tabela 1, foram selecionados 25 artigos que passaram por uma análise mais aprofundada, verificando se conseguiam responder ao menos uma das questões de pesquisa e se continham informações importantes para abordar neste trabalho. (veja em Figura 1, Passo 11).

Tabela 1 – Artigos disponíveis nas bases de dados.

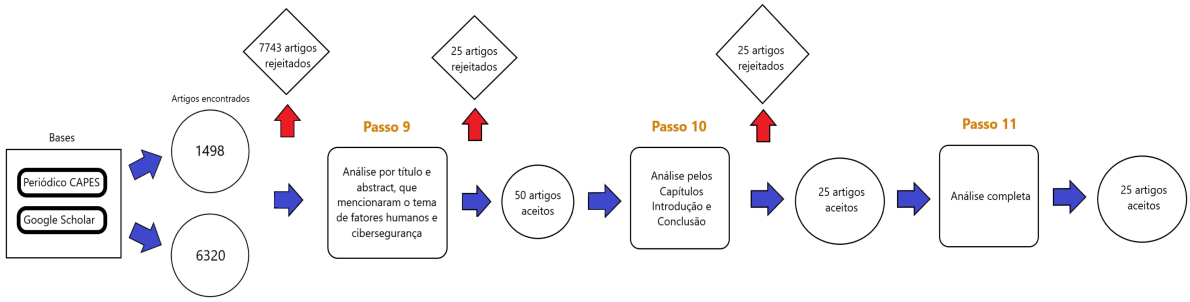
Base de dados	Quantidade total	Analisados	Selecionados
Portal Periódico CAPES	1498	25	11
Google Scholar	6320	50	14

12. **Extração das respostas relacionadas às questões de pesquisa.**

    Uma vez selecionados os artigos, referentes aos Passos 9 a 11, procedeu-se então com as extrações das respostas, que são apresentadas, dentro de uma discussão mais ampla no Capítulo 3.

Ainda, para ajudar nas análises e trazer informações mais ricas para este trabalho, a metodologia adotada foi complementada com ideias baseadas no trabalho de (PABLOS; FEITOSA, 2020). Essa adaptação da técnica de RSL contém características muito próximas da técnica apresentada por (NEIVA; SILVA, 2016) e, quando combinadas, tornam possível mostrar as informações com mais clareza. No trabalho de (PABLOS; FEITOSA, 2020), foram aplicados alguns critérios de qualidade para os artigos analisados, em seguida o autor realiza uma somatória da qualidade geral (QG) baseando-se se as questões de pesquisa foram correspondidas com os artigos analisados. A qualidade geral dos trabalhos consiste em uma avaliação dos artigos estudados, que tem uma relação no mínimo

Figura 1 – Procedimento geral de pesquisa para filtragem de literatura.



Adaptado de: (RAHMAN et al., 2021)

indireta com as questões de pesquisas, sendo atribuídas as notas: 1 (pouco), 2 (médio) e 3 (muito) para cada questão de pesquisa respondida. E essas notas significam o quanto o artigo pode apresentar dados relevantes e precisos para responder às QPs. Então, os artigos foram avaliados e foram feitas as somatórias, que serão apresentadas em uma tabela de qualidade geral das literaturas no próximo capítulo.

3 Resultados

As interações humanas com os computadores podem nos trazer ricas informações sobre as ações e comportamentos dos usuários, que estão relacionadas aos ataques mal intencionados. O resultado dessas ações pode ajudar os usuários a se protegerem mais contra esses tipos de ataques. Alguns estudos apresentados nesta pesquisa demonstram que as ações dos usuários podem afetar de maneira direta e indireta os sistemas de computadores. Por exemplo, um usuário pode acessar um site, que pode conter algum script malicioso e não saber que a página está coletando seus dados. Há também o tipo de usuário que sabe dos riscos e, mesmo assim, ignora os alertas, desativando as proteções do computador para acessar determinado conteúdo que pode conter uma ameaça. Não só as ações dos usuários são os principais conceitos abordados, mas também os resultados posteriores, como por exemplo, o comportamento de um computador após ser invadido por um programa malicioso. E esses dados são importantes fontes de informações para conseguir dados relacionados às ações dos usuários.

As tecnologias de informação e comunicação tornaram-se essenciais para que organizações e indivíduos mantenham altos níveis de produtividade. A adoção dessas tecnologias vem, em contrapartida, acompanhada por uma infinidade de novas vulnerabilidades e, portanto, novas ameaças à confidencialidade e à integridade dos dados pessoais e organizacionais. No entanto, especialistas concordam que as pessoas são o elo mais fraco na proteção do sistema de segurança da informação de uma organização (PARSONS et al., 2017).

As ações dos usuários estão relacionadas a diversos fatores sobre a cibersegurança, pois cada ação tomada pode trazer diferentes efeitos e resultados, como por exemplo, abrir brechas de seguranças em uma máquina em rede e afetar um servidor. Essas brechas de seguranças de um computador pessoal ou empresarial podem ter diferentes impactos. Por exemplo, após uma invasão, pode ser que o programa malicioso seja imperceptível ao usuário, com o intuito apenas de roubar informações, ou também com um nível de complexidade maior, como criar túneis de acesso para alguém com más intenções, causar lentidão do sistema, executar outros programas em segundo plano com diferentes ações, ter acesso a diferentes contas de e-mails importantes, ou a contas bancárias, dados pessoais, possibilitando redefinir cadastros de sites, alter e-mail, senhas, números de celulares, fazendo com que o usuário mal intencionado possa prejudicar a vida de uma ou várias pessoas.

É por esses e outros motivos que a cibersegurança se encaixa no tema quando falamos de fatores humanos, mas será mesmo possível se proteger de diversos ataques em

um ambiente conectado à Internet? Diversos estudos tentam responder essa pergunta. Por exemplo, o trabalho de (LéVESQUE et al., 2018) menciona que, mesmo os usuários que são conscientes a respeito de segurança computacional, são suscetíveis a vulnerabilidades desconhecidas e que até os melhores mecanismos de segurança podem ser contornados como resultado de ações do usuário.

Já em outra pesquisa, (GRATIAN et al., 2018) mencionam que existem cinco categorias principais de traços de personalidade, conhecidas como "Big Five" amplamente aceito, são elas:

- Abertura à experiência;
- Consciência;
- Extroversão;
- Amabilidade; e
- Neuroticismo.

Os autores (GRATIAN et al., 2018) alegam que os traços de personalidade citados podem causar interferência na segurança e são bem explorados na literatura da psicologia, mas pouco estudados no âmbito tecnológico. Vale lembrar que, no caso de suscetibilidade de phishing, o traço de personalidade é bem utilizado para esse fim. Portanto, nesse caso, há um número maior de estudos. De acordo com os autores (HALEVI; LEWIS; MEMON, 2013), mulheres com alto neuroticismo eram excelentes vítimas de phishing, além de permitirem brechas e terem configurações de privacidade fracas. Sabemos então que os usuários ou colaboradores são o elo mais fraco da cibersegurança. Mas devemos também pensar do outro lado, o lado em que criminosos utilizam indivíduos como meio para atingir um fim, esse é o ataque de Engenharia Social, entre os quais estão os ataques de phishing. Esses tipos de ataques manipulam o indivíduo, causam desorientação e criam falsas informações, aproveitando a situação e invadindo o dispositivo alvo, causando algum prejuízo, roubando dinheiro e ou informações sensíveis, podendo utilizar telas clones que direcionam para páginas falsas e que, ao tentar realizar algum tipo de ação a página falsa rouba as informações do usuário (Figura 2). Ataques de phishing têm uma forte presença no tema Fatores Humanos em Cibersegurança, pois envolvem diretamente os usuários e os cibercriminosos. (DIAS, 2021) aborda o tema de cibersegurança com phishing e menciona alguns comportamentos que causam riscos e suas possíveis prevenções.

Para os comportamentos que causam riscos de ataques, o autor cita:

- Utilização de *e-mails* profissionais para fins pessoais;

- Acesso a *websites* não fidedignos;
- Abertura de anexos ou links de *e-mail* de spam e/ou fontes não fidedignas; e
- Compartilhamento de senhas e de informações privadas ou corporativas.

Para a prevenir um ataque de phishing, o autor cita:

- **Não abrir quaisquer links, arquivos ou anexos suspeitos, recebidos de fontes desconhecidas**;
- **Não baixar e/ou instalar aplicação a partir de fontes não fidedignas**;
- **Utilizar senhas únicas e com combinações de caracteres não óbvios**;
- **Utilizar a autenticação de multi fatores**;
- **Manter os sistemas atualizados**; e
- **Utilizar sistemas de segurança e software antivírus adequados aos diversos dispositivos**.

Figura 2 – Representação de cibercrime com interação do usuário.

Com todas essas informações de diferentes artigos e autores, podemos notar que, os seres humanos são o ponto de partida para diferentes tipos de invasões, sendo assim, um dos lados mais fracos da segurança cibernética. Entender as características humanas, as suas diferenças, técnicas e habilidades, irão influenciar e ajudar pesquisadores e profissionais da área a melhorarem e desenvolverem métodos de mitigação contra ameaças. (GRATIAN et al., 2018) mencionam que os estilos das tomadas de decisões, preferências de riscos, traços de personalidade e fatores demográficos podem ajudar nas pesquisas contra ameaças.

Muitos usuários passam por diversos avisos dos softwares de segurança. Na maioria dos casos, eles ignoram completamente ou desligam as notificações. (MODIC; ANDERSON, 2014) mencionam cenários como esse, mas reforçam que **os avisos de advertência**

deveriam ser mais claros, mais fáceis de serem entendidos. A fala do autor tem significados importantes, pois, depois de diversos experiências com softwares de antivírus testados em máquinas virtuais entre os anos de 2019 e 2022, foi constatado que as mensagens não eram tão claras e que na maioria das vezes os softwares de antivírus mostravam as notificações de ameaça e logo em seguida a mensagem desaparecia e, ao ir nos logs do software, foi constatado também que era complicado encontrar as mensagens de aviso, além de, não sabermos se o programa tinha sido enviado ou não para a quarentena. Por isso é **importante que os softwares sejam mais fáceis de serem compreendidos**. Baseado nessas informações dos autores, e através de outros estudos, chega-se ao achado de que os softwares deveriam conter mais informações do problema, induzir o usuário a ler o que está acontecendo, mostrar uma descrição detalhada e precisa, entregar exemplos do que o problema detectado pode causar, pois avisos bem definidos e estruturados são muito mais eficazes do que os avisos simples de 'ameaça detectada'.

Existem conjuntos consolidados de boas práticas que se aplicam na interação com a tecnologia, por exemplo, há locais que parecem ser seguros, mas devemos ficar atentos, um exemplo comum são os computadores de uso público, eles podem estar infectados com algum tipo de ameaça, por exemplo, nesses computadores pendrives e memórias são bem comuns de serem utilizados nas portas USB e são fontes causadoras de vulnerabilidades. Se alguma ameaça infecta o dispositivo portátil é capaz de que outras máquinas sejam afetadas por aquele mesmo software invasor ao utilizar o mesmo dispositivo infectado. Então **devemos ficar atentos aos computadores públicos**, pois não são seguros, as pessoas que utilizaram esses computadores podem não ter tido boas práticas, principalmente por não ser um sistema pessoal e por isso, os cuidados podem ser quase nulos. Também é importante **ter muita atenção ao digitar senhas nos smartphones em locais públicos e evitar que outras pessoas vejam**, isso pode comprometer a segurança e a vítima pode acabar sendo invadida por uma maneira bem simples.

Os autores (LéVESQUE et al., 2018) concluíram que os computadores sem um sistema de segurança eram mais infectados e também mencionam boas práticas similares para melhorar a cibersegurança:

- **Não ignorar as mensagens de segurança que aparecem dos softwares de defesa**; e
- **Utilizar software de antivírus para proteger o computador**.

Já os autores (SIKDER et al., 2020) mencionam que, para haver boas práticas de segurança para uso de smartphones e evitar vulnerabilidades indesejadas, devem ser seguidas as seguintes práticas:

- Os usuários devem **manter somente em seu telefone os aplicativos que são importantes** para suas atividades diárias relacionadas ao smartphone;
- Antes de instalar um aplicativo, **deve-se entender sobre seus recursos, permissões e classificações para verificar se não é prejudicial**;
- **Deve-se desligar as funcionalidades de consumo de bateria como NFC, Bluetooth, Wi-FI, GPS etc. se desnecessário**;
- Deve-se verificar os aplicativos de manutenção padrão e as notificações dos serviços do Google Play para detectar aplicativos e otimizá-los;
- Os usuários de smartphones devem **desinstalar os aplicativos desnecessários para evitar o uso extra de bateria e vazamentos de privacidade**.

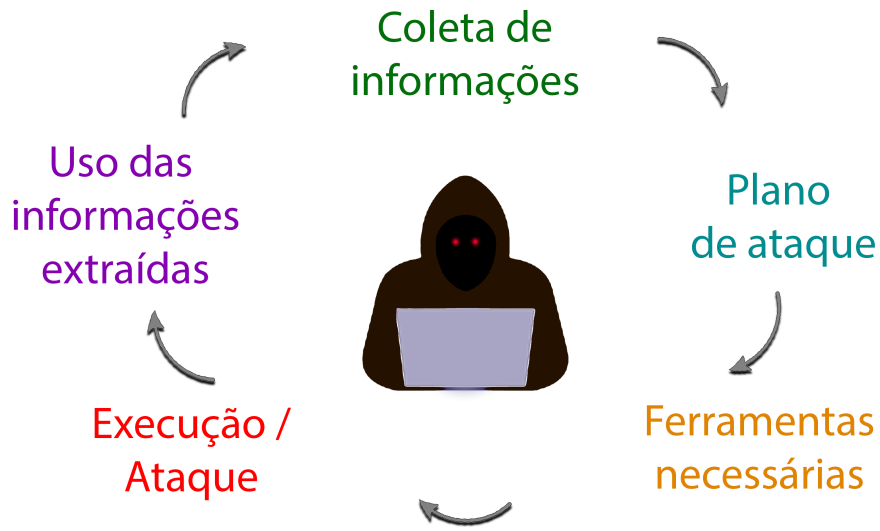
As melhores práticas de segurança de um dispositivo são diretrizes e salvaguardas para proteger os dados dos usuários, nesse caso, (WEICHBROTH; ŁYSIK, 2020), mencionam a importância de **manter os dispositivos bloqueados por algum tipo de autenticação**, isso evita invasões referentes aos roubos ou furtos, desde que a senha tenha um nível alto de complexidade, pois a quantidade de fatores de autenticação não é necessariamente sinônimo de boa qualidade de senha. **Atualizar os sistemas operacionais e aplicativos para a última versão**, pois a maioria das atualizações podem resolver algum tipo de problema de vulnerabilidade e de outras ameaças. É importante **realizar backups dos dados regularmente** de fotos, vídeos, documentos e outros arquivos importantes, com o backup o usuário pode se prevenir de perda ou exclusão de dados, bem como dos ataques de ransomware. Deve se **utilizar criptografia dos dados**, isso vai ajudar a tornar as senhas ou as informações ininteligíveis, ou seja, converter os dados em outro tipo de formato ou código, para que apenas as partes autorizadas possam descriptografar e ler esses dados. Normalmente o recurso pede uma senha que, se esquecida pode causar problemas para a recuperação de dados. Conexões de Wi-Fi públicas podem facilitar as invasões, e por isso, é **fortemente recomendado que não se conecte em Wi-Fi público e inseguro sem utilizar uma opção de transmissão segura, como uma rede virtual privada VPN**. É necessário habilitar a limpeza remota de dados, caso um dispositivo com dados confidenciais seja roubado e que não haja chance de recuperá-lo, então é bom que haja uma forma de realizar esse procedimento de limpeza a distância. O sistema operacional Android contém uma ferramenta do Google que é capaz de realizar a busca pela localização, bloquear o dispositivo e até mesmo realizar uma limpeza de fábrica no dispositivo, evitando assim que o invasor utilize as aplicações e tente roubar dados sensíveis. Desativar o Bluetooth e Wi-Fi quando não for necessário, pois as implementações dessas tecnologias podem estar vulneráveis.

(WEICHBROTH; ŁYSIK, 2020) ainda reforçam que é necessário **ficar atento às técnicas de engenharia social**, como visto anteriormente, o usuário deve estar ciente da existência de pessoas maliciosas e desconfiar de ações suspeitas. **Não realizar a remoção de restrições de softwares**, técnicas conhecidas como root ou jailbreak, podem causar vulnerabilidades, expondo o sistema operacional. Outro destaque importante é **não conceder permissões desnecessárias aos aplicativos**, pois podem liberar acesso a câmera, microfone, lista de contatos, localização e outros recursos importantes do dispositivo. **Deve ser mantido nos aparelhos somente os aplicativos úteis para o uso diário e que também funcionam corretamente**, pois aplicativos desnecessários e com bugs podem permitir que invasores utilizem esse meio para invasão. Por último, é necessário **instalar aplicativos de segurança**, como antivírus, pois protegem contra aplicativos e vírus maliciosos. Seguir todos os Passos de boas práticas de defesa não irá garantir total segurança dos dispositivos, porém irá diminuir em grande parte os riscos de uma invasão no computador, violações de privacidade, os riscos de travamentos e a perda de dados importantes.

Então, como descrito, os ataques cibernéticos provindos de engenharia social são bem perigosos, pois os invasores podem estudar as suas vítimas conversando pessoalmente ou pelos meios digitais e principalmente investigando pelas redes sociais. Atualmente estar exposto em redes sociais pode trazer diferentes consequências graves, pois o cibercriminoso aproveita de todos os detalhes possíveis da vítima para aplicar ataques e golpes, ou seja, podemos definir como um meio para explorar a psicologia humana usando informações que são próximas da vítima (veja a Figura 3). Os autores (SIDDIQI; PAK; SIDDIQI, 2022) mencionam que os ataques por engenharia social normalmente não seguem padrões ou abordagens específicas para a realização de um ataque e por isso esses tipos de ataques são eficazes, eficientes e fáceis, levando prejuízos significativos aos seus alvos. Ainda reforçam que contramedidas podem ser aplicadas, são elas:

- **O uso de aprendizado de máquina** que pode desempenhar um papel importante no combate a ataques cibernéticos de engenharia social, pois podem identificar alguns tipos de padrões em e-mails, SMS, links maliciosos e em chamadas usando processamento de linguagem natural;
- **O uso de Aprendizagem Profunda** que é uma abordagem eficaz contra ameaças cibernéticas;
- **O uso de Aprendizagem por Reforço** utilizando arquiteturas de feedback para definir políticas, incluindo cenários incertos em tempo real, a ferramenta precisa ser treinada para aprender a lidar com as ameaças; e
- **O uso de Processamento de Linguagem Natural** que combinada com as técnicas de ***Machine Learning*** combate ataques de phishing.

Figura 3 – Ciclo da Engenharia Social.



Adaptado de: (DALMAZO, 2021)

Vimos que características humanas são capazes de interferir na segurança cibernética. Organizações que desejam se proteger de invasões devem dar prioridade para a proteção de dados sensíveis, seja da organização ou de clientes, mas sem esquecer dos próprios funcionários. Existem alguns tipos de estudos que verificam a correlação entre essas características humanas e os cibercrimes. No artigo de (PARSONS et al., 2017), os autores mencionam que desenvolveram o Questionário de Segurança da Informação, em inglês *Human Aspects of Information Security Questionnaire* (HAIS-Q), como instrumento eficaz para a medição da conscientização sobre segurança da informação, em inglês *Information Security Awareness* (ISA). O HAIS-Q, utiliza o modelo de conhecimento, atitude e comportamento, em inglês *Knowledge, Attitude and Behaviour* (KAB), cujas pesquisas demonstraram uma forte relação entre conhecimento, atitude e comportamento, dando indícios e provas mais concretas sobre as relações das vulnerabilidades de segurança que são causadas pelo comportamento humano e, claro, uma visão de como enfrentá-los.

O uso acentuado de computadores e dispositivos portáteis nos últimos anos trouxe facilidades em comunicações, movimentações bancárias e diversas outras ferramentas úteis ao dia-a-dia. Muitas pessoas já têm a ideia de como utilizar seus equipamentos, sabem em parte o que torna os seus dispositivos lentos e vulneráveis, também o que devem evitar abrir. Mas, ainda sim, se considerarmos a quantidade de pessoas no Brasil, por exemplo, teremos uma quantidade bem alta de pessoas que não sabem como se proteger. De acordo com o artigo de (SCHULTZ, 2005), o autor menciona que 80% das pessoas analisadas sabiam evitar abrir anexos maliciosos devido à experiência e ao conhecimento da existência de outros worms e vírus, enquanto os outros 20% das pessoas ainda não sabiam que evitar abrir esses anexos seria a melhor ação. O autor ainda reforça que,

se pegarmos esses 20% e compararmos com a população mundial, teremos um número exorbitante de pessoas que não tem conhecimento dessas ameaças. Foi observado também que as pessoas desistiram de usar um sistema de defesa, pois tinham controles e recursos muito difíceis de serem utilizados. E, por isso, farão de tudo para evitá-los ou contorná-los. Outro problema relacionado com as pessoas na segurança da informação é que, ao serem contratadas em uma empresa, recebem somente informações do que pode e o que não podem fazer, e não recebem os devidos treinamentos para se proteger do que é ruim. A maioria das organizações pedem referências durante o processo de contratação e nunca verificam, após um determinado período, se as pessoas mudam seus hábitos com o passar do tempo – algo que pode alterar drasticamente o fator de ameaça interna, dado que a maioria das organizações estendem uma quantidade muito grande de confiança para funcionários, empreiteiros e consultores – algo arriscado e que, talvez, não devesse ser assim. A segurança da informação é realmente um problema para as pessoas. Mas são as pessoas que deveriam controlar a tecnologia, não o contrário. Temos uma abundância de tecnologias em detrimento de um número insuficiente de especialistas aptos a lidar com o fator humano na segurança da informação. Um bom começo seria publicar mais artigos sobre este assunto para conscientizar os usuários.

Todos os dispositivos eletrônicos que funcionam com algum tipo de sistema e que estão sincronizados com a Internet podem sofrer diferentes tipos de ataques externos constantemente. Cibercriminosos sempre estão procurando por alguma falha de segurança. E, por isso, não podemos esquecer os dispositivos portáteis, por exemplo, os aparelhos que fazem parte da Internet das Coisas (IoT). Esses dispositivos estão mudando constantemente a sociedade, eles facilitam o dia a dia das pessoas, empreendedores, fazendeiros, profissionais de diferentes áreas. Com esse tipo de tecnologia, é possível produzir uma quantidade de dados inimaginável. E, quando falamos de produção de dados, temos que vincular automaticamente a cibersegurança, porque são esses dados que interessam aos cibercriminosos. (ALMIANI et al., 2020) cita que várias abordagens e técnicas podem ser utilizadas para proteger as plataformas da IoT, são elas:

- **O uso de Firewalls**;
- **Utilizar criptografia de dados**; e
- **Utilizar autenticação de usuários por meio do paradigma de computação em névoa**.

A cibersegurança combinada com dispositivos IoT traz diversas vantagens. É possível extrair informações importantes para serem analisadas, principalmente por terem aplicações rodando em tempo real, na maioria dos casos. As ferramentas de análises relacionadas à cibersegurança dependem de uma grande quantidade de dados atualizados,

e as fontes de IoT são excelentes para trazer essas informações. Coletar dados atualizados garantem que os especialistas e estudiosos da área possam obter dados precisos e criar técnicas para mitigar as ameaças constantes. (NIETO; RIOS, 2019) mencionam que diversos atores podem gerar diferentes interpretações de problemas e soluções, que são relacionadas à indivíduos que podem ser apresentadas na forma de perfis de cibersegurança. Nos últimos anos, as pessoas estão andando praticamente o tempo todo com seus dispositivos portáteis, levando-os para todos os lugares: trabalho, escola, lazer e outros. Esses dispositivos portáteis, como smartphones, coletam localizações, direcionam publicações de acordo com o uso, ou seja, conseguem capturar dados relevantes que podem ser explorados pelos cibercriminosos. Por isso, é muito importante seguir diretrizes com os dispositivos pessoais e as regras de cibersegurança valem para todos os dispositivos conectados na Internet. Por outro lado, é possível encontrar o lado positivo sobre esses ataques, por exemplo, será possível aproveitar as mesmas técnicas utilizadas pelos cibercriminosos, podendo aprender com as diversas variações de problemas para melhorar as técnicas de defesa da cibersegurança.

Vimos também que alguns comportamentos de usuários podem causar impactos diretos e indiretos, sendo de extrema importância reforçar e complementar aqueles que são baseados nas ações humanas, por exemplo, as características, conhecimentos, habilidades, experiências, responsabilidades, personalidade, etc. Avaliar todos esses pontos, é o começo para uma boa atuação contra cibercriminosos. (LAHCEN et al., 2020) mencionam que é importante realizar uma série de perguntas para analisar e mapear os usuários, incluindo seu ambiente. A avaliação pode envolver fatores conhecidos, coletar fatos sobre as capacidades e limitações do usuário e o ambiente de trabalho. Ao avaliar, pode-se reconhecer os fatores emergentes que não foram inicialmente incluídos no mapeamento e podem causar um erro humano. Existem fatores combinados que podem causar alguns problemas, por exemplo os fatores físicos combinados com ações humanas, e também os fatores psicológicos combinados com os fatores físicos. Por exemplo, a fadiga ou a distração podem contribuir para erros não intencionais, e a perda de vigilância pode causar erros intencionais. Erros humanos podem causar prejuízos para as indústrias e organizações. O usuário deve estar sempre consciente, mesmo que seu comportamento atual não cause uma violação naquele momento executado, não significa que não poderá acontecer no futuro e portanto, o usuário deve analisar os riscos no presente e no futuro.

Os colaboradores às vezes cometem erros que podem ser ou não de propósito, por exemplo, anotar senhas em papéis e deixar do lado da máquina. Esses erros podem causar uma série de problemas se um usuário mal intencionado quiser acessar a máquina. O ambiente de trabalho também pode afetar o usuário e induzir a ter fadiga, que pode ser um fator problemático, se o ambiente causar pressões psicológicas e estresses. Tudo que está em volta do funcionário deve ser analisado, incluindo a falta de comunicação com os colegas de equipe, porque, se o usuário não está a par das sequências de trabalho corretas

e ações preventivas, isso poderá ocasionar brechas de segurança. A fadiga é um sentimento muito comum no ambiente de trabalho, e pode ser ocasionada por diversos fatores. Esse tipo de cansaço e sonolência, reduz as ações dos usuários de realizarem atividades de maneira segura. Características individuais e o ambiente de trabalho contribuem muito para se ter a fadiga no trabalho, é uma das principais causas de acidades de trabalho. Ter uma diminuição da habilidade de processamento de informações pode causar problemas de segurança, pois as tomadas de ações sem atenção, podem ocasionar brechas de segurança e perda de dados. (STANTON et al., 2016) mencionam que a fadiga pode ser chamada também de fadiga de segurança, e que a resignação e perda de controle associadas a ela certamente representam um desafio aos esforços destinados a promover a segurança online e proteger a privacidade de trabalho.

As corporações têm um grande desafio, que é mitigar a fadiga de segurança dos seus colaboradores, pois a maioria delas não tem experiência para lidar com esse problema, o que resulta do aumento da perda de habilidade cognitiva e consequentemente o aumento de abertura de brechas cibernéticas. A fadiga de segurança pode ser dividida em diferentes tipos, o autor (NOBLES, 2022) menciona alguns tipos, são eles:

- A Fadiga de Autenticação é uma condição de cansaço baseada na imposição de criar senhas complexas que expiram o tempo todo e validações excessivas de acessos (credenciamento);
- A Fadiga de Decisão é o estado de exceder as habilidades cognitivas ao executar tarefas repetitivas;
- A Fadiga de Alerta que ocorre ao analisar muitos incidentes para determinar a importância dos alertas relacionados a segurança cibernética;
- A Fadiga de Treinamento acontece quando a educação é ineficaz e excessiva, deixando os funcionários frustrados e exaustos; e
- A Fadiga Regulatória acontece quando há medo de não cumprir as excessivas leis que são impostas pela corporação.

Devemos lembrar também que as características humanas mencionadas nem sempre são fáceis de predeterminar e que eventos de conscientização, por exemplo, podem não ser bem aproveitados em alguns desses casos. Existem características humanas que são distintas, mas como estão situadas em um grupo, pode ser que essas pessoas acabem sendo influenciadas a tomar boas ações de maneira iguais e automáticas. Também há casos em que o grupo não siga as diretrizes de maneira correta, influenciando os outros colaboradores que poderiam seguir corretamente as diretrizes a não faze-lá. E é aí que uma boa conscientização, treinamentos, diretrizes devem ser aplicadas de maneira repetitiva. Esses

eventos de cibersegurança devem ter um retorno, um feedback dos colaboradores, pois não adianta aplicar esses eventos se são apresentações cansativas, pois os colaboradores não irão absorver as informações de maneira positiva e não colocarão em prática as diretrizes de cibersegurança. E, como é um processo de repetição, as organizações devem analisar constantemente, levantar os riscos através de uma análise e realizar o procedimento sempre que necessário. Essas contra diretrizes mencionadas, são destacadas com uma visão mais generalizada pelos autores (RAHMAN et al., 2021) que acreditam que teorias das ciências sociais, teorias cognitivas e várias teorias psicológicas podem ser combinadas para identificar e explicar as diversas contra diretrizes observadas.

Como mencionada, os fatores psicológicos também implicam na cibersegurança, por exemplo, a impulsividade, pode ser uma ação negativa do usuário que pode causar brechas de segurança. Usuários com essa característica podem não distinguir um e-mail legítimo de um phishing, também criam senhas simples por serem facilmente lembradas e ou reutilizam as mesmas senhas em outros sistemas. (HADLINGTON, 2017) cita a relação do Transtorno do Déficit de Atenção com Hiperatividade (TDAH) junto com a cibersegurança e portanto, pessoas com TDAH tendem a falhar na identificação de um e-mail de phishing, pois a falta de atenção pode ocasionar ações erradas e implicar no aumento de cibercriminosos.

O cibercrime pode ser definido como atividades mediadas por computador que são ilegais ou consideradas ilegais por partes específicas, e essas atividades podem ser realizadas por meio de redes globais (PALMIERI; SHORTLAND; MCGARRY, 2021). Esses autores argumentam que os smartphones são, hoje, a chave de tudo. É onde a vida do indivíduo está, pois, utilizam bancos, acessam e armazenam fotos, documentos e vídeos em aplicações nas nuvens, o que significa que é possível capturar e roubar tudo o que as pessoas digitam, como números de cartão de crédito, números de contas bancárias e senhas de diversas aplicações. E, como essas tecnologias estão em constante fase de mudança, sempre evoluindo, aumentando o desempenho, tendo novas melhorias e novas tecnologias embarcadas, por exemplo diferentes tipos de sensores para o hardware, e uma série de programas que podem salvar a localização, habilitar microfone e câmera. Imagine o quão valioso é para os cibercriminosos a quantidade de informações que um smartphone não pode gerar. Com o passar dos anos, o termo "crime cibernético" vai se tornando mais complexo, a tecnologia muda, as ameaças mudam (BUTTON; WHITTAKER, 2021).

Após diversos temas de cibersegurança tratados aqui, sabemos sobre a adequação da segurança, mesmo que esteja sendo usada por várias organizações para proteger suas operações, ela não oferece proteção completa. Existem cibercriminosos com diferentes propósitos de ataque, os autores (RAZAQUE et al., 2021) citam que, alguns cibercriminosos querem invadir contas bancárias, outros querem roubar informações de documentos pessoais e ou empresariais. De fato, as informações são extremamente valiosas para ambos

os lados, mas vemos que o lado que está vencendo é dos cibercriminosos, devido às diferentes técnicas de invasões que surgem toda semana e que são informadas pelos portais de softwares de antivírus.

(DELCHER, 2021) questiona: "estamos perdendo a luta contra o crime cibernético?". Segundo o autor, para que as empresas sejam mais resilientes aos ataques de segurança cibernética, a resposta é confiar no conhecimento atual das pessoas sobre segurança cibernética e sua proteção contra crimes cibernéticos. Ainda menciona que, um estudo recente, realizado durante a pandemia do SARS-CoV-2 (Covid-19), descobriu que três quartos dos trabalhadores domésticos não tinham recebido nenhum treinamento de segurança para o trabalho remoto. E, reforçando, os números de ataques cibernéticos estão subindo a cada ano e podem acabar acelerando mais o processo de invasão com os trabalhos remotos de colaboradores, pois, nesse cenário, é dada uma máquina para cada colaborador poder acessar de casa os sistemas organizacionais, podendo manipular arquivos, alterar, ter acesso aos arquivos de rede e outros. Se a conexão está feita, é possível que invasores também possam ter acesso, se houver vulnerabilidades.

Os esforços para abordar efetivamente a questão do crime online podem ser prejudicados pela falta de estabilidade e continuidade organizacional (YAR; STEINMETZ, 2019). Uma das principais questões, é se é possível prevenir qualquer crime cibernético entendendo os fundamentos da segurança cibernética na vida cotidiana. As tecnologias modernas são usadas em todo o mundo e quase universalmente na Internet, então esse problema afeta todas elas. O cibercrime que tinha um vínculo muito grande com aparelhos desktops agora está migrando em alta velocidade para dispositivos portáteis, como smartphones, tablets e VoIPs.

Os malwares de dispositivos móveis aumentaram acentuadamente nos últimos anos, resultando em golpes inteligentes de engenharia social e outros tipos de ataques (BORKOVICH; SKOVIRA, 2019). E é possível prevenir esses tipos de crimes cibernéticos, porém é muito importante melhorar as práticas de privacidade. Também é necessário aplicar regulamentos mais definitivos, para conduzir melhor protocolos de segurança, ter uma reforma da cultura de segurança organizacional que muitas das vezes é ignorada. Mitigar ataques, requer esforços coordenados apoiados e defendidos pelos profissionais de níveis mais altos de gerência. Para reforçar e destacar as ideias anteriores foi extraída algumas boas práticas mencionadas pelos autores (BORKOVICH; SKOVIRA, 2019), são elas:

- **Incorporar missões de cibersegurança/engenharia social no Código de Conduta e Ética do Funcionário**;
- **Desenvolver e implantar treinamentos de conscientização de segurança**;
- **Desenvolver políticas de classificação de dados e informações**;

- **Desenvolver programas de treinamento de funcionários projetado para identificar e resistir a ataques de engenharia social**;
- **Testes de resistências dos funcionários a aberturas de engenharia social, simulando os eventos**;
- **Incentivar os funcionários a adotar e praticar as políticas de segurança com prêmios**;
- **Divulgar as políticas de segurança com pôsteres, protetores de tela, anúncios por e-mail, vídeos e boletins informativos**;
- **Convidar especialistas para realizar palestras sobre segurança e comportamentos**;
- **Modificar a cultura de segurança corporativa com maior consciência, sensibilidade e ceticismo saudável**.

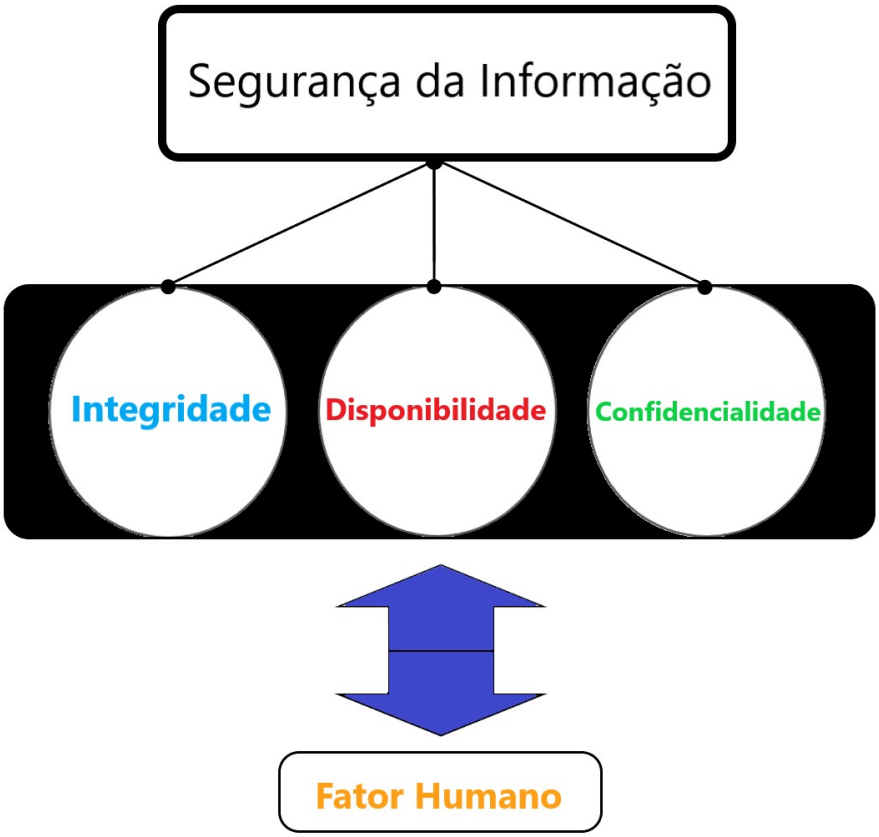
Os ciberataques vão evoluindo à medida que os anos passam, vão se tornando mais avançados e são espalhados rapidamente pela Internet. Mesmo com diversas técnicas de análise de dados e aprendizado para construir modelos de cibersegurança, um modelo de segurança baseado na descoberta efetiva de insights de segurança e padrões de segurança mais recentes poderiam ser mais úteis. Para resolver essa questão, (SARKER et al., 2020) citam que é necessário desenvolver mecanismos de segurança mais flexíveis e eficientes que possam responder a ameaças e atualizar políticas de segurança para mitigá-las de forma inteligente em um tempo curto. Analisar uma quantidade enorme de dados relevantes e de diferentes fontes ajudam a enriquecer as defesas, isso inclui redes e sistemas, e realizar políticas de seguranças com uma intervenção mínima, ou seja tentar realizar o máximo de forma automatizada para garantir que a precisão aumente. Para conseguir extrair insights efetivos será necessário utilizar várias técnicas de aprendizado de máquina, técnicas de deep learning baseadas em rede neural. Muitas dessas técnicas de aprendizagem são capazes de encontrar problemas incomuns ou comportamentos maliciosos. (SARKER et al., 2020) ainda mencionam que as técnicas de aprendizado de máquina, podem ser capazes de encontrar anomalias, ameaças e padrões nos dados, podendo fornecer soluções de segurança correspondentes.

Como visto, a cibersegurança deveria ser um assunto sério, mas muitas organizações ignoram, talvez por não ter acontecido nenhum problema ou por não quererem investir em segurança e conscientização por acharem inviável. As organizações que menosprezam a segurança cibernética só investem em segurança quando algum tipo de prejuízo lhe é apresentado. (GONÇALVES, 2019) mencionam que, essa ideia de menosprezo das organizações é como a desvalorização sobre as questões de saúde humana. Ou seja, nada

é feito enquanto nada der errado. A preocupação dos responsáveis só aumenta quando acontece algum tipo de prejuízo, isso significa que não houve uma prevenção e é aí que entra o investimento em segurança, quando os gastos para tentar recuperar os dados são superiores aos gastos com segurança. (GONÇALVES, 2019) mencionam ainda que a proteção eficaz de uma organização se dá pelo conhecimento, competências, compreensão e aceitação que são relativos a tecnologia e cibersegurança. Sabemos que realizar treinamentos, educar o colaborador em cibersegurança é um esforço que leva muito tempo, não é simplesmente citar diversas regras e pronto, deve ser um estudo teórico e prático. E a organização deve estar, de maneira contínua, coletando dados de erros cometidos pelos colaboradores para um possível treinamento. Além disso, os colaboradores devem passar por uma conscientização em cibersegurança, para que eles saibam dos riscos e que estejam comprometidos em estar de acordo com a segurança da organização. Mas devemos sempre estar atentos, pois por mais que a organização adquira softwares de segurança, coloquem bloqueios nos sistemas e adquiram firewalls ou outras máquinas relacionadas à segurança, ainda sim, a organização continuará vulnerável, pois o fator humano é uma das chaves principais.

Na segurança da informação existem pilares principais que devem ser seguidos pelas organizações se quiserem manter os seus dados seguros e livre de problemas, são eles: integridade, disponibilidade e confidencialidade (veja a Figura 4). A integridade é para garantir que não haja interferência externa que poderá corromper ou roubar os dados de uma empresa. A disponibilidade está ligada ao acesso dos dados e sistemas da empresa, ou seja, ter uma determinada aplicação disponível e não bloqueada para a utilização. E, por último, a confidencialidade garante que os dados da empresa não sejam acessíveis para qualquer pessoa ou aplicação sem algum tipo de autorização. Como exposto anteriormente, o fator humano é uma das principais causas de ciberataques e também um dos principais conceitos para a Segurança da Informação, por isso, a visão mais técnica dos pilares pode ser complementada pelos aspectos associados aos fatores humanos e por isso foi inserida na Figura 4.

Figura 4 – Fator humano como um complemento para os pilares da Segurança da Informação.



A partir da Tabela 2, é possível observar uma boa cobertura das QPs, que foram satisfatoriamente abordadas dentre os artigos estudados. Artigos esses que mostraram conhecimentos diversos sobre a cibersegurança, também foram mostradas técnicas de mitigação de ameaças e fatores que podem causar vulnerabilidades. Baseado nessas análises foi criada a Tabela 2, nas quais as questões de pesquisa que tiveram respostas diretas (abordando de maneira rápida) e indiretas (levando uma discussão mais lenta, gerando testes e analisando casos mais longos) foram consideradas. Ou seja, menções de assuntos relacionados, fatores que trouxeram ou irão trazer problemas e mitigações foram considerados.

Tabela 2 – Relacionamentos com as questões de pesquisas.

Artigos	Questões de pesquisas atendidas
(NOBLES, 2022)	QP1, QP2 e QP3
(SIDDIQI; PAK; SIDDIQI, 2022)	QP1, QP2 e QP3
(RAHMAN et al., 2021)	QP1 e QP2
(ALMIANI et al., 2020)	QP1, QP2 e QP3
(DIAS, 2021)	QP1, QP2 e QP3
(RAZAQUE et al., 2021)	QP1, QP2 e QP3
(PARSONS et al., 2017)	QP1 , QP3
(GRATIAN et al., 2018)	QP1 e QP2
(HALEVI; LEWIS; MEMON, 2013)	QP1, QP2
(SCHULTZ, 2005)	QP2 e QP3
(MODIC; ANDERSON, 2014)	QP1, QP2 e QP3
(HADLINGTON, 2017)	QP1, QP2
(LéVESQUE et al., 2018)	QP1, QP2 e QP3
(SIKDER et al., 2020)	QP1, QP2 e QP3
(WEICHBROTH; ŁYSIK, 2020)	QP1, QP2 e QP3
(NIETO; RIOS, 2019)	QP1, QP2 e QP3
(LAHCEN et al., 2020)	QP1, QP2 e QP3
(STANTON et al., 2016)	QP1, QP2
(PALMIERI; SHORTLAND; MCGARRY, 2021)	QP1 e QP2
(BUTTON; WHITTAKER, 2021)	QP1, QP2
(DELCHER, 2021)	QP1 e QP2
(YAR; STEINMETZ, 2019)	QP1 e QP2
(BORKOVICH; SKOVIRA, 2019)	QP1, QP2 e QP3
(SARKER et al., 2020)	QP1, QP2 e QP3
(GONÇALVES, 2019)	QP1, QP2 e QP3

Os artigos foram analisados verificando se haviam correspondências com as questões de pesquisas. Assim, para dar mais destaque aos artigos analisados, foram atribuídas pontuações para a qualidade geral dos artigos e, no final foi gerada uma somatória, para determinar se/como conseguiram responder as questões de pesquisas, de forma complementar, conforme a abordagem de (PABLOS; FEITOSA, 2020)

Tabela 3 – Qualidade geral das literaturas (QG).

Artigos	QG
(NOBLES, 2022)	4
(SIDDIQI; PAK; SIDDIQI, 2022)	5
(RAHMAN et al., 2021)	4
(ALMIANI et al., 2020)	5
(DIAS, 2021)	5
(RAZAQUE et al., 2021)	5
(PARSONS et al., 2017)	4
(GRATIAN et al., 2018)	4
(HALEVI; LEWIS; MEMON, 2013)	4
(SCHULTZ, 2005)	3
(MODIC; ANDERSON, 2014)	5
(HADLINGTON, 2017)	3
(LéVESQUE et al., 2018)	5
(SIKDER et al., 2020)	5
(WEICHBROTH; ŁYSIK, 2020)	5
(NIETO; RIOS, 2019)	5
(LAHCEN et al., 2020)	5
(STANTON et al., 2016)	4
(PALMIERI; SHORTLAND; MCGARRY, 2021)	3
(BUTTON; WHITTAKER, 2021)	3
(DELCHER, 2021)	3
(YAR; STEINMETZ, 2019)	3
(BORKOVICH; SKOVIRA, 2019)	5
(SARKER et al., 2020)	5
(GONÇALVES, 2019)	5

Como visto na Tabela 2, há casos em que somente uma questão de pesquisa foi atendida, indicando que o artigo abordou o assunto, porém se desviou para casos de testes, abordagens ou outras metodologias correspondente ao tema. Os artigos que tiveram duas questões de pesquisas atendidas puderam receber mais atenção do que só com uma questão atendida, pois conseguiram se aproximar mais do tema deste trabalho e conseguiram trazer informações mais relevantes. Os artigos que conseguiram responder as três questões de pesquisas foram os que conseguiram trazer quantidades de informações mais relevantes e ricas para a mitigação de ameaças na cibersegurança.

Os artigos passaram por uma análise, como mencionado no parágrafo anterior, e foram verificados quais questões de pesquisa eles conseguiram responder. Ao decorrer das análises, os artigos foram observados e pontuados de acordo com as três questões de pesquisa deste trabalho. Note que todos os artigos analisados são excelentes, todos contém estudos e evoluções de análises de várias semanas, meses ou anos. O que foi abordado neste trabalho ao analisar os artigos através de uma pontuação geral foi a qualidade na entrega das respostas para as três questões de pesquisas que foram mencionadas anteriormente.

Ao longo deste capítulo, foram relatados estudos relacionados ao fator humano, tanto de maneira positiva como negativa. De maneira negativa, temos que, invasões, perda de dados e roubos de dados associados a ações e comportamento do usuário podem gerar muitos prejuízos. E, de maneira positiva, temos que os estudiosos têm realizado pesquisas e procurado entender diversos fatores, tanto psicológicos quanto físicos, podendo chegar em conclusões de como deve ser realizada a mitigação do problema.

A partir de inúmeros estudos, pode-se concluir que os principais conceitos associados ao tema deste trabalho são que, os fatores humanos influenciam as tomadas de decisões e é importante que eles sejam avaliados para que se evite problemas ou minimize os riscos. É necessário aumentar os esforços de prevenção e mitigação para que cibercriminosos não tenham êxito em seus ataques, porque eles estão sempre procurando brechas, explorando informações, coletando dados para suas próximas investidas.

E ainda, alguns dos principais fatores humanos e sociais que influenciam a cibersegurança são:

- As pessoas são o elo mais fraco na proteção do sistema.
- Características psicológicas como: neuroticismo, estresse, fadiga de trabalho, falta de atenção, impulsividade e outros;
- A falta de comunicação com a equipe de trabalho, podendo gerar ações erradas;
- A falta de treinamentos em cibersegurança em organizações;
- Não seguir as diretrizes organizacionais;

- Ignorar alertas de softwares de defesa, fechando as mensagens sem dar atenção ou desligá-las;
- Cair em golpes por engenharia social; e
- Abrir arquivos maliciosos recebidos por e-mail;

Esses fatores se relacionam, pois no fim, qualquer uma dessas ações podem gerar vulnerabilidades em algum sistema, e o cibercriminoso poderá aproveitar de cada uma das falhas.

Assim, como visto ao longo deste capítulo, boas práticas são necessárias para mitigar os problemas, tendo sido possível obter a seguinte lista compilada a partir dos estudos realizados:

- **Não abrir quaisquer links, arquivos ou anexos suspeitos, recebidos de fontes desconhecidas**;
- **Não baixar e/ou instalar aplicação a partir de fontes não fidedignas**;
- **Utilizar senhas únicas e com combinações de caracteres não óbvios**;
- **Utilizar a autenticação de multi fatores**;
- **Manter os sistemas atualizados**;
- **Utilizar sistemas de segurança e software antivírus adequados aos diversos dispositivos**;
- **Os avisos de advertência devem ser mais claros, mais fáceis de serem entendidos**;
- **Ter muita atenção ao digitar senhas nos smartphones em locais públicos e evitar que outras pessoas vejam**;
- **Devemos ficar atentos aos computadores públicos**;
- **Não ignorar as mensagens de segurança que aparecem dos softwares de defesa**;
- Os usuários devem **manter somente em seu telefone os aplicativos que são importantes** para suas atividades diárias relacionadas ao smartphone;
- Antes de instalar um aplicativo, **deve-se entender sobre seus recursos, permissões e classificações para verificar se não é prejudicial**;

- **Deve-se desligar as funcionalidades de consumo de bateria como NFC, Bluetooth, Wi-FI, GPS etc. se desnecessário**;
- Deve-se **verificar os aplicativos de manutenção padrão e a notificação dos serviços** do Google Play para detectar aplicativos de drenagem de massa e otimizá-los;
- Os usuários de smartphones devem **desinstalar os aplicativos desnecessários para evitar vazamentos de privacidade**;
- **Manter os dispositivos bloqueados por algum tipo de autenticação e utilizar criptografia dos dados**;
- **Realizar backups dos dados regularmente**;
- **Fortemente recomendado que não se conecte em Wi-Fi público e inseguro sem utilizar uma opção de transmissão segura, como uma rede virtual privada VPN**;
- **Ficar atento às técnicas de engenharia social**;
- **Não realizar a remoção de restrições de softwares**;
- **Não conceder permissões desnecessárias aos aplicativos**;
- **O uso de *Machine Learning*** que pode desempenhar um papel importante no combate a ataques cibernéticos de engenharia social, pois podem identificar alguns tipos de padrões em e-mails, SMS, links maliciosos e em chamadas usando processamento de linguagem natural;
- **O uso de Aprendizagem Profunda** que é uma abordagem eficaz contra outros tipos de ameaças;
- **O uso de Aprendizagem por Reforço** utilizando arquiteturas de feedback para definir políticas, incluindo cenários incertos em tempo real, a ferramenta precisa ser treinada para aprender a lidar com as ameaças;
- **O uso de Processamento de Linguagem Natural** que combinada com as técnicas de ***Machine Learning*** combate ataques de phishing;
- **O uso de Firewalls**;
- **Utilizar autenticação de usuários por meio do paradigma de computação em névoa**;
- **Incorporar missões de cibersegurança/engenharia social no Código de Conduta e Ética do Funcionário**;

- **Desenvolver e implantar treinamentos de conscientização de segurança**;
- **Desenvolver políticas de classificação de dados e informações**;
- **Desenvolver programas de treinamento de funcionários projetado para identificar e resistir a ataques de engenharia social**;
- **Testes de resistências dos funcionários a aberturas de engenharia social, simulando os eventos**;
- **Incentivar os funcionários a adotar e praticar as políticas de segurança com prêmios**;
- **Divulgar as políticas de segurança com pôsteres, protetores de tela, anúncios por e-mail, vídeos e boletins informativos**;
- **Convidar especialistas para realizar palestras sobre segurança e comportamentos**; e
- **Modificar a cultura de segurança corporativa com maior consciência, sensibilidade e ceticismo saudável**.

4 Conclusões

Este trabalho aplicou a metodologia de RSL para investigar a intersecção entre as áreas de Interação Humano-Computador e Cibersegurança. Foi feito um levantamento de 25 artigos que tratavam do tema, os quais foram comentados e relacionados às questões de pesquisa definidas. Com base na metodologia adotada, a maioria dos artigos selecionados e estudados conseguem responder a primeira questão de pesquisa, sobre os principais conceitos associados ao tema (Fatores humanos em cibersegurança), explicando bem o que é a cibersegurança, os cibercrimes e suas relações existentes com as pessoas. Os fatores humanos têm relações diretas e indiretas sobre a segurança dos dispositivos (computadores, dispositivos portáteis e outros relacionados), podendo aumentar proporcionalmente os riscos de vulnerabilidade devido às ações e ao comportamentos das pessoas envolvidas.

Grande parte dos artigos estudados também conseguem responder a segunda questão de pesquisa e descrevem muito bem sobre os fatores humanos e sociais que influenciam a cibersegurança. Nesta área, foram analisadas as características psicológicas humanas e fatores externos relacionados, como o estresse, a fadiga de trabalho, falta de atenção, a falta de comunicação entre os colegas de equipe causando divergências no trabalho ou falhas, a facilidade de utilização e avisos de um software de segurança, se é importante ou não utilizar um antivírus e sobre pessoas que tinham conhecimentos de vírus em anexos enviados por e-mail.

Para a terceira questão, foram analisados os artigos selecionados e se puderam responder sobre as boas práticas de usabilidade ou guidelines. Os fatores principais analisados foram se os artigos puderam explicar o problema e propor uma solução ou se mencionaram pelo menos uma ideia curta para a solução dos problemas apresentados. Muitos dos artigos apresentaram ideias curtas sobre a solução dos problemas de cibersegurança e foram considerados como resposta para a terceira questão.

A aplicação da metodologia de (NEIVA; SILVA, 2016) trouxe uma facilidade para o desenvolvimento do tema sobre fatores humanos em cibersegurança, além de ser voltado para a área da computação, o que ajudou bastante nas buscas para a revisão sistemática dos artigos apresentados. Também foram utilizados elementos da metodologia proposta por (PABLOS; FEITOSA, 2020), e, a partir desse estudo mais amplo, foi extraída a base de análise para aplicar nesta RSL, por exemplo, a tabela de Qualidade Geral (QG), atribuindo somatórias de notas baseando as questões de pesquisas (QPs). Essas notas de QG tiveram o intuito de trazer uma relevância para este trabalho referenciando as QPs. As notas mais baixas atribuídas para os artigos, de maneira geral, significa que a explicação para as questões de pesquisas não foi muito relevante, mas que contiveram

exemplos de informações úteis para a construção das ideias. E as notas médias e mais altas foram para os artigos que exploraram os três pontos das QPs, mostrando melhores informações e soluções para tentar mitigar os problemas da cibersegurança.

Quando usamos o termo "segurança da informação", estamos automaticamente falando sobre atacantes e defensores. Com o aumento de usuários de smartphone, também vieram um aumento na quantidade de aplicativos para estes dispositivos. Consequentemente, a segurança tanto desses dispositivos, quanto de computadores desktops, continuarão oferecendo uma infinidade de problemas relacionados à segurança. Para tentar combater os cibercriminosos, boas práticas são necessárias e muitas delas são negligenciadas, devemos mudar o pensamento, pensar estrategicamente para tentar mitigar os problemas de segurança, pois há estudos como o de (CREESE et al., 2020), que mencionam: "A menos que medidas sejam tomadas agora, até 2025, a tecnologia da próxima geração, na qual o mundo confiará cada vez mais, terá o potencial de sobrecarregar as defesas da comunidade de segurança global".

Referências

ALMIANI, M.; ABUGHAZLEH, A.; AL-RAHAYFEH, A.; ATIEWI, S.; RAZAQUE, A. Deep recurrent neural network for iot intrusion detection system. **Simulation Modelling Practice and Theory**, Elsevier, v. 101, p. 102031, 2020. Citado 3 vezes nas páginas 23, 31 e 32.

BORKOVICH, D. J.; SKOVIRA, R. J. Cybersecurity inertia and social engineering: Who's worse, employees or hackers? **Issues in Information Systems**, v. 20, n. 3, 2019. Citado 3 vezes nas páginas 27, 31 e 32.

BUTTON, M.; WHITTAKER, J. Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation. **International Journal of Law, Crime and Justice**, Elsevier, v. 66, p. 100482, 2021. Citado 3 vezes nas páginas 26, 31 e 32.

CREESE, S.; SAUNDERS, J.; AXON, L.; DIXON, W. Future series: Cybersecurity, emerging technology and systemic risk. In: **World Economic Forum**. [S.l.: s.n.], 2020. Citado na página 38.

DALMAZO. **Os perigos da engenharia social e como se proteger - Globalmind**. 2021. <https://www.globalmind.com.br/engenharia-social-sua-empresa-esta-protegida/>. (Accessed on 01/22/2023). Citado na página 22.

DELCHER, P. Are we losing the fight against cybercrime? **Computer Fraud & Security**, Elsevier, v. 2021, n. 5, p. 18–19, 2021. Citado 3 vezes nas páginas 27, 31 e 32.

DIAS, P. R. S. **Prevenir um Ataque de Phising**. Tese (Doutorado), 2021. Citado 3 vezes nas páginas 17, 31 e 32.

FORTIFIREWALL. **Cinco ciberataques a serem observados em 2022 | Blog Forti Firewall**. 2022. <https://fortifirewall.com.br/Blog/Cinco-Ciberataques-A-Serem-Observados-Em-2022/b/74/>. (Accessed on 10/19/2022). Citado na página 9.

GONÇALVES, R. S. **O fator humano da cibersegurança nas organizações**. Tese (Doutorado) — Universidade de Lisboa (Portugal), 2019. Citado 4 vezes nas páginas 28, 29, 31 e 32.

GRATIAN, M.; BANDI, S.; CUKIER, M.; DYKSTRA, J.; GINTHER, A. Correlating human traits and cyber security behavior intentions. **Computers Security**, v. 73, p. 345–358, 2018. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404817302523>. Citado 4 vezes nas páginas 17, 18, 31 e 32.

HADLINGTON, L. Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. **Heliyon**, Elsevier Ltd, England, v. 3, n. 7, p. e00346–e00346, 2017. ISSN 2405-8440. Citado 3 vezes nas páginas 26, 31 e 32.

HALEVI, T.; LEWIS, J.; MEMON, N. A pilot study of cyber security and privacy related behavior and personality traits. In: **Proceedings of the 22nd international conference on world wide web**. [S.l.: s.n.], 2013. p. 737–744. Citado 3 vezes nas páginas 17, 31 e 32.

LAHCEN, R. A. M.; CAULKINS, B.; MOHAPATRA, R.; KUMAR, M. Review and insight on the behavioral aspects of cybersecurity. **Cybersecurity**, Springer Singapore, Singapore, v. 3, n. 1, p. 1–18, 2020. ISSN 2523-3246. Citado 3 vezes nas páginas 24, 31 e 32.

LéVESQUE, F. L.; CHIASSON, S.; SOMAYAJI, A.; FERNANDEZ, J. M. Technological and human factors of malware attacks: A computer security clinical trial approach. **ACM Trans. Priv. Secur.**, Association for Computing Machinery, New York, NY, USA, v. 21, n. 4, jul 2018. ISSN 2471-2566. Disponível em: <https://doi-org.ez34.periodicos.capes.gov.br/10.1145/3210311>. Citado 5 vezes nas páginas 8, 17, 19, 31 e 32.

LI, Q. **Mobile Security: Threats and Best Practices**. 2020. <https://www.hindawi.com/journals/misy/2020/8828078/#discussion>. (Accessed on 07/30/2022). Citado na página 9.

MODIC, D.; ANDERSON, R. Reading this may harm your computer: The psychology of malware warnings. **Computers in Human Behavior**, v. 41, p. 71–79, 2014. ISSN 0747-5632. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0747563214004658>. Citado 3 vezes nas páginas 18, 31 e 32.

NEIVA, F.; SILVA, R. **Revisão Sistemática da Literatura em Ciência da Computação - Um Guia Prático**. 2016. Citado 4 vezes nas páginas 11, 13, 14 e 37.

NIETO, A.; RIOS, R. Cybersecurity profiles based on human-centric iot devices. **Human-centric computing and information sciences**, Springer Berlin Heidelberg, Berlin/Heidelberg, v. 9, n. 1, p. 1–23, 2019. ISSN 2192-1962. Citado 3 vezes nas páginas 24, 31 e 32.

NOBLES, C. Stress, burnout, and security fatigue in cybersecurity: A human factors problem. **Holistica : Journal of business and public administration**, Sciendo, v. 13, n. 1, p. 49–72, 2022. ISSN 2067-9785. Citado 3 vezes nas páginas 25, 31 e 32.

PABLOS, F. D. Y.; FEITOSA, M. D. Acessibilidade em métodos ágeis: uma revisão sistemática da literatura. **Research, Society and Development**, v. 9, n. 3, p. e133932419–e133932419, 2020. Citado 3 vezes nas páginas 14, 31 e 37.

PALMIERI, M.; SHORTLAND, N.; MCGARRY, P. Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. **Computers in human behavior**, Elsevier, v. 120, p. 106745, 2021. Citado 3 vezes nas páginas 26, 31 e 32.

PARSONS, K.; CALIC, D.; PATTINSON, M.; BUTAVICIUS, M.; MCCORMAC, A.; ZWAANS, T. The human aspects of information security questionnaire (hais-q): Two further validation studies. **Computers Security**, v. 66, p. 40–51, 2017. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404817300081>. Citado 4 vezes nas páginas 16, 22, 31 e 32.

RAHMAN, T.; ROHAN, R.; PAL, D.; KANTHAMANON, P. Human factors in cybersecurity: a scoping review. In: **The 12th International Conference on Advances in Information Technology**. [S.l.: s.n.], 2021. p. 1–11. Citado 4 vezes nas páginas 15, 26, 31 e 32.

RAY, J. **Amazon.com.br eBooks Kindle: Papel da Interação Humano Computador, RAY, JOY**. 2022. <https://www.amazon.com.br/Papel-Intera%C3%A7%C3%A3o-Humano-Computador-JOY-ebook/dp/B09V3F3RT9/ref=monarch_sidesheet>. (Accessed on 12/27/2022). Citado na página 8.

RAZAQUE, A.; AJLAN, A. A.; MELAOUNE, N.; ALOTAIBI, M.; ALOTAIBI, B.; DIAS, I.; OAD, A.; HARIRI, S.; ZHAO, C. Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system. **Applied Sciences**, v. 11, n. 17, 2021. ISSN 2076-3417. Disponível em: <https://www.mdpi.com/2076-3417/11/17/7880>. Citado 3 vezes nas páginas 26, 31 e 32.

SARKER, I. H.; KAYES, A. S. M.; BADSHA, S.; ALQAHTANI, H.; WATTERS, P.; NG, A. Cybersecurity data science: an overview from machine learning perspective. **Journal of big data**, Springer International Publishing, Cham, v. 7, n. 1, p. 1–29, 2020. ISSN 2196-1115. Citado 3 vezes nas páginas 28, 31 e 32.

SCHULTZ, E. The human factor in security. **Computers Security**, v. 24, n. 6, p. 425–426, 2005. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404805001045>. Citado 3 vezes nas páginas 22, 31 e 32.

SIDDIQI, M. A.; PAK, W.; SIDDIQI, M. A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. **Applied sciences**, MDPI AG, Basel, v. 12, n. 12, p. 6042, 2022. ISSN 2076-3417. Citado 3 vezes nas páginas 21, 31 e 32.

SIKDER, R.; KHAN, M. S.; HOSSAIN, M. S.; KHAN, W. Z. A survey on android security: development and deployment hindrance and best practices. **TELKOMNIKA (Telecommunication Computing Electronics and Control)**, v. 18, n. 1, p. 485–499, 2020. Citado 3 vezes nas páginas 19, 31 e 32.

STANTON, B.; THEOFANOS, M. F.; PRETTYMAN, S. S.; FURMAN, S. Security fatigue. **It Professional**, IEEE, v. 18, n. 5, p. 26–32, 2016. Citado 3 vezes nas páginas 25, 31 e 32.

WEICHBROTH, P.; ŁYSIK, Ł. Mobile security: Threats and best practices. **Mobile Information Systems**, Hindawi, v. 2020, 2020. Citado 4 vezes nas páginas 20, 21, 31 e 32.

YAR, M.; STEINMETZ, K. F. **Cybercrime and society**. [S.l.]: Sage, 2019. Citado 3 vezes nas páginas 27, 31 e 32.