PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO - REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

ANÁLISE DOS IMPACTOS DOS CRIMES CIBERNÉTICOS NA SOCIEDADE BRASILEIRA: DESAFIOS E PERSPECTIVAS DE COMBATE

ORIENTANDO: JOÃO PEDRO CAMPOS DE ARAÚJO
ORIENTADORA: PROF. MA. ISABEL DUARTE VALVERDE

GOIÂNIA/GO
2023

JOÃO PEDRO CAMPOS DE ARAÚJO

ANÁLISE DOS IMPACTOS DOS CRIMES CIBERNÉTICOS NA SOCIEDADE BRASILEIRA: DESAFIOS E PERSPECTIVAS DE COMBATE

Artigo Científico apresentado à disciplina apresentado à disciplina Trabalho de Curso I, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).

Orientadora Profa. Ma. Isabel Duarte Valverde.

GOIÂNIA/GO
2023

JOÃO PEDRO CAMPOS DE ARAÚJO

ANÁLISE DOS IMPACTOS DOS CRIMES CIBERNÉTICOS NA SOCIEDADE BRASILEIRA: DESAFIOS E PERSPECTIVAS DE COMBATE

Data da Defesa: de de 2023

BANCA EXAMINADORA

_____

Orientador: Profa. - Ma. Isabel Duarte Valverde. NOTA

_____

Examinador Convidado: NOTA

GOIÂNIA/GO
2023

Sumário

ANÁLISE DOS IMPACTOS DOS CRIMES CIBERNÉTICOS NA SOCIEDADE BRASILEIRA: DESAFIOS E PERSPECTIVAS DE COMBATE

João Pedro Campos de Araújo[1]

RESUMO

Os crimes cibernéticos, também conhecidos como crimes virtuais, são uma ameaça crescente e complexa na era digital. Eles abrangem atividades maliciosas direcionadas a sistemas de informática e dados. Os tipos de crimes incluem ataques a computadores e violações de dados, afetando áreas como patrimônio, liberdade individual e propriedade intelectual. A impunidade é um problema devido à falta de especialização legal na área. Enfrentar essa ameaça requer cooperação internacional, regulamentações atualizadas e investimentos em tecnologia e cibe segurança. A formação de profissionais especializados é essencial. Em resumo, os crimes cibernéticos são multifacetados, refletindo conflitos sociais e exigindo uma abordagem multidisciplinar para mitigar seus impactos.

Palavras-chave: crimes cibernéticos, cibe segurança, regulamentação, impunidade, formação profissional.

[1] Acadêmico João Pedro Campos de Araújo do Curso de Direito da Pontifícia Universidade Católica de Goiás, e-mail joaoo1966@hotmail.com

INTRODUÇÃO

Os crimes cibernéticos, também conhecidos como crimes virtuais, representam uma ameaça crescente e complexa no mundo contemporâneo. Este fenômeno em constante evolução é caracterizado por uma ampla gama de atividades maliciosas que têm como alvo sistemas de informática e dados armazenados em dispositivos eletrônicos. A definição abrangente de Ferreira (2005) sobre crimes cibernéticos fornece uma base sólida para a compreensão da complexidade desse problema. Vamos tratar nesse artigo o que é os crimes cibernéticos e quais são as suas formas de ataque. Iremos abordar como as pessoas podem se prevenir desses ataques que estão cada vez maiores.

A escolha desse tema se dá ao fato do grande crescimento desse crime em nosso país, pois de fato muitas pessoas tem sofrido com esses crimes, principalmente os idosos que não possuem tanto conhecimento de tecnologias.

A linha de pesquisa adotada será **ESTADO, RELAÇÕES E TRANSFORMAÇÕES CONSTITUCIONAIS.**

O objetivo geral dessa pesquisa é atentar a sociedade que o tema está cada vez mais predominante em nosso país, para que quando por acaso for acontecer com as mesmas possam estar completamente por dentro do assunto e poderem se prevenir de tal crime que já tirou tanto de muitas pessoas inocentes.

Diante do cenário apresentado foi estabelecido que o que a questão prolema é a falta de informação e educação que se tem hoje em dia. Os mais jovens são mais preparados devido a sempre terem convivido com tecnologias, que não é o caso dos mais velhos que por falta de conhecimento são mais vulneráveis a esses criminosos.

A estrutura do trabalho será dividida em 3 capítulos que começará no primeiro explicando o que é os crimes, depois seguirá para os tipos de crimes cibernéticos e finalizará explicando como as pessoas possam se prevenir desses ataques.

Dentro desse contexto, é fundamental compreender que os crimes cibernéticos não apenas afetam a segurança digital, mas também refletem conflitos sociais, políticos e pessoais no mundo virtual. Os criminosos cibernéticos variam desde hackers novatos em busca de notoriedade online até grupos altamente organizados com motivações diversas. Portanto, este artigo busca fornecer uma visão abrangente desse fenômeno multifacetado e urgente que afeta não apenas o Brasil, mas o cenário global.

1. CONCEITO E CARACTERÍSTICAS DOS CRIMES CIBERNÉTICOS

Ferreira (2005, p. 261) fornece uma definição abrangente e fundamental do que compreendemos como Crimes Cibernéticos ou Crimes Virtuais. Essa definição é de suma importância para compreendermos a complexidade desse fenômeno em constante evolução.

Conforme a definição de Ferreira, os crimes cibernéticos podem ser entendidos como atos direcionados de forma maliciosa contra sistemas de informática, sendo que eles podem ser subdivididos em duas categorias principais:

- Atos Contra o Computador: Essa categoria engloba ações que têm como alvo diretamente os sistemas computacionais. Inclui uma série de atividades prejudiciais, como a disseminação de vírus de computador, worms, trojans e ataques de negação de serviço (DDoS). Esses ataques visam comprometer a integridade, a disponibilidade e a confidencialidade dos sistemas.
- Atos Contra os Dados ou Programas de Computador: Aqui, os criminosos têm como objetivo os dados armazenados nos sistemas ou os próprios programas de computador. Isso pode envolver o roubo de informações pessoais, espionagem corporativa, destruição de dados ou até mesmo a manipulação de informações sensíveis.

Além disso, é crucial ressaltar que essas atividades ocorrem por intermédio de sistemas de informática. Dentro desse contexto, segundo o Ministério Público Federal (MPF), as infrações cometidas abrangem uma variedade de áreas sensíveis da sociedade, incluindo:

A) Infrações contra o Patrimônio: Envolvem atividades que visam causar danos financeiros a indivíduos, empresas ou instituições por meio de fraudes eletrônicas, esquemas de phishing e outros métodos.

B) Infrações contra a Liberdade Individual: Englobam ações que violam a privacidade e a segurança pessoal, como o ciberbullying, o stalking online e a disseminação não autorizada de informações pessoais.

C) Infrações contra a Propriedade Imaterial: Essas infrações se relacionam ao uso não autorizado de propriedade intelectual, como pirataria de software, plágio digital e violação de direitos autorais.

No entanto, é importante observar que os crimes cibernéticos não se limitam apenas à busca pelo lucro financeiro. Em certos casos, os criminosos cibernéticos têm motivações que vão além do aspecto monetário. Motivos pessoais, políticos e ideológicos também podem ser impulsionadores desses ataques.

De acordo com informações do Kaspersky Lab (2023), essas motivações podem levar a ataques que buscam danificar computadores ou redes por razões que ultrapassam o interesse financeiro, tornando os crimes cibernéticos um fenômeno ainda mais complexo e multifacetado.

Em resumo, o crime cibernético não é apenas uma ameaça à segurança digital, mas também uma manifestação de conflitos sociais, políticos e pessoais no mundo virtual. Esses crimes podem ser perpetrados por uma ampla gama de atores, desde cibe criminosos altamente organizados e tecnicamente competentes até hackers novatos em busca de notoriedade online.

1.1 DEFINIÇÃO DE CRIMES CIBERNÉTICOS E SUAS PRINCIPAIS CARACTERÍSTICAS

Conforme estabelecido pelo Priberam Dicionário, um Hacker é definido como "uma pessoa com profundos conhecimentos de informática e programação, que se dedica à identificação de falhas em sistemas ou à invasão ilegal de sistemas e redes computacionais." (Dicionário Priberam da Língua Portuguesa 2008-2023).

Nesse cenário, é relevante notar que os praticantes desse tipo de crime podem ser classificados em duas categorias distintas. Por um lado, existem os hackers que fazem uso de técnicas altamente avançadas, explorando vulnerabilidades tecnológicas complexas para atingir seus objetivos. Por outro lado, há os hackers que se valem de técnicas simples, porém enganosas, como golpes de engenharia social, os quais ainda demonstram ser altamente eficazes. Como afirmado por Vitória Ribeiro em 2022, esses atacantes demonstram uma notável capacidade de adaptação, aproveitando tanto a tecnologia mais avançada quanto métodos tradicionais para alcançar seus fins.

Uma característica marcante dos crimes cibernéticos é a natureza dos dados frequentemente roubados. Eles incluem informações pessoais altamente sensíveis, como dados financeiros, números de identificação pessoal e dados de login. É importante ressaltar que tem surgido uma nova modalidade criminosa, conhecida como extorsão digital, na qual os hackers exigem o pagamento de resgates para liberar informações pessoais de indivíduos ou dados confidenciais das empresas. Esse tipo de crime representa uma ameaça adicional, exigindo a atenção e a prevenção rigorosas por parte das organizações e indivíduos.

Em suma, o mundo dos crimes cibernéticos é dinâmico e desafiador. Tanto os hackers quanto as vítimas estão constantemente evoluindo suas estratégias, tornando essencial a adoção de medidas de segurança robustas, atualização constante e conscientização sobre as táticas empregadas por esses criminosos. Além disso, a colaboração entre entidades governamentais, empresas e sociedade em geral é fundamental para lidar eficazmente com a crescente ameaça dos crimes cibernéticos.

2. EXPLORAÇÃO DOS TIPOS MAIS COMUNS DE CRIMES CIBERNÉTICOS E PROCEDIMENTOS MAIS CONHECIDOS

O Brasil é o quinto país mais atacado por cibercriminosos. O ataque cibernético desabilita computadores, rouba dados e viola sistemas. Criminosos virtuais utilizam diversos meios para promover esses ataques, tais como: malware, phising e ransomware.(Forbes 2023)

Eles ocorrem quando o usuário acessa algum anexo malicioso enviado peloscriminosos, através de e-mails falsos, links e SMS, sempre se passando por outra pessoa ou empresa, de forma atrativa, afim de convencer o usuário da idoneidade do link. Quando acessados, esses links ativam os malwares, infectando o sistema deixando o criminoso com total acesso. (Forbes 2023)

Engana-se quem pensa que os ciberataques trazem apenas prejuízos com roubo de informações e dados, de acordo com o relatório Atividade Criminosa Online no Brasil da Axur de 2021, a perda com crimes virtuais no mundo chegou a US$ 6 trilhões. (Forbes 2023).

Separando-os em três categorias: a primeira é definida por ataques que utilizam diretamente um computador, tanto do lado do cibercriminoso quanto da vítima, enquanto a segunda modalidade é definida por obtenção ilícita de uma rede específica através de outros computadores ou dispositivos. (XLOGIC STI 2023)

Já a terceira envolve o impedimento de uma máquina. Ela pode ser infectada por um malware e ter seus dados sequestrados, o que abre uma oportunidade para o criminoso extorquir a vítima e exigir pagamento de resgate. Dentro dessas categorias, os casos mais comuns são:

- ***Malware:*** após ser infectado, o computador fica sob custódia do criminoso e pode ser utilizado para as mais variadas finalidades, como roubo de dados, realização de outros ataques, entre outras transgressões. A dica de ouro é de não clicar em links desconhecidos e suspeitos ou abrir arquivos executáveis desconhecidos, pois, em sua maioria, são esses os métodos utilizados pelos criminosos para obter acesso aos dispositivos das vítimas.

- **Phishing:** esse método é um dos mais comuns praticados no Brasil. Significando pescaria, em livre tradução, o phishing se baseia em "iscas digitais". A vítima pode, por exemplo, ver algum anúncio de dinheiro fácil e clicar no link para saber mais, sem se dar conta de que está dando acesso ao seu dispositivo. O meio utilizado pode ser spam em um e-mail ou mensagem via WhatsApp.

- **DDoS (ataque de negação de serviço):** interrompendo um sistema inteiro de uma rede, os cibercriminosos utilizam

> técnicas avançadas de informática para sobrecarregar servidores e deixá-los fora do ar. Isso é feito com base nos limites de capacidade de um serviço online. Em outras palavras, é gerado um tráfego acima do normal para bombardear e inativar uma estrutura digital. Após essa queda, os marginais podem extorquir, solicitar pagamentos ou até mesmo destruir e vazar dados das vítimas. XLOGIC STI 2023

Segundo Olivo (2010), o Phishing é uma técnica de Engenharia Social que busca persuadir as vítimas com objetivos de capturar informações pessoais e depois utilizá-las de forma com que causem prejuízos, normalmente financeiros. Para Mitnick e Simon (2003), a engenharia social é uma arte teatral, de forma que convence as pessoas que façam coisas que normalmente não fariam para um estranho.

Esses ataques demonstram elevada eficácia, pois atingem inúmeras vítimas com relativa facilidade. Os predadores manipulam os usuários, induzindo-os a usar a funcionalidade de compartilhamento para disseminação, ou facilitam a apropriação indevida de informações ou infecção de dispositivos, entre outros danos possíveis.

3. AÇÕES PARA COMBATER CRIMES CIBERNÉTICOS

Combater o crime cibernético no Brasil é importante para garantir a segurança online. De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), aqui estão algumas ações que podem ser tomadas para combater o crime cibernético:

- Educação Cibernética: Promover a conscientização e educação cibernética entre os cidadãos para que saibam como se proteger online.

- Cooperação Internacional: Trabalhar em conjunto com outros países para investigar e combater crimes cibernéticos que tenham origem no exterior.

- Leis e Regulamentações: Fortalecer as leis e regulamentações relacionadas à cibersegurança e ao crime cibernético.

- Polícia Cibernética: Reforçar as unidades de polícia cibernética para investigar e reprimir atividades criminosas online.

- Parcerias Público-Privadas: Estabelecer parcerias entre o governo e empresas privadas de tecnologia para compartilhar informações e recursos na luta contra o crime cibernético.

- Investimento em Tecnologia: Investir em tecnologia de segurança cibernética de ponta para proteger infraestruturas críticas e dados sensíveis.

- Conscientização Empresarial: Promover a cibersegurança em empresas e organizações, incentivando a adoção de práticas seguras.

- Denúncias: Encorajar as pessoas a denunciar atividades suspeitas online para as autoridades.

Lembre-se de que a luta contra o crime cibernético é contínua e exige esforços coordenados de todos os setores da sociedade.

A educação é fundamental para combater o crime cibernético. As pessoas precisam saber como se proteger online para evitar cair em golpes e ataques. A cooperação internacional é necessária para investigar e combater crimes cibernéticos que tenham origem no exterior. A regulamentação é importante para estabelecer regras e punições para crimes cibernéticos.

Além das ações listadas no texto, o CERT.br também recomenda a adoção de medidas de segurança individual e corporativa para proteger-se do crime cibernético. Essas medidas incluem:

- Uso de senhas fortes e únicas;

- Atualização regular de softwares;
- Instalação de antivírus e firewall;
- Cuidado com links e anexos suspeitos;
- Backup regular de dados

3.1 A NECESSIDADE DOS PROFISSIONAIS ESPECIALIZADOS PARA O COMBATE AO CRIME CIBERNÉTICO NO BRASIL

A necessidade de profissionais especializados no combate ao crime cibernético no Brasil é uma questão crítica e premente, dada a crescente vulnerabilidade do país a ataques cibernéticos. Em 2022, o Brasil registrou um alarmante número de mais de 200 milhões de ataques cibernéticos, um aumento significativo de 30% em relação ao ano anterior, conforme relatórios do Instituto Internacional de Pesquisa em Políticas Públicas (ISPI) na Cibe segurança Global 2023.

Esses ataques cibernéticos não são apenas uma ameaça teórica, mas causam prejuízos tangíveis, incluindo o roubo de dados sensíveis, fraudes financeiras e danos à infraestrutura crítica do país. Para enfrentar essa realidade, é imperativo adotar um conjunto de ações abrangente, abordando diferentes aspectos da cibe segurança.

A conscientização da população sobre os riscos e as práticas seguras na internet é um primeiro passo crucial. No entanto, para enfrentar o crime cibernético em sua totalidade, são necessárias ações que envolvam a cooperação internacional, a regulamentação e, igualmente importante, a formação de profissionais altamente especializados.

Um dos maiores obstáculos que o Brasil enfrenta no combate ao crime cibernético é a carência de profissionais com conhecimento técnico e expertise na área. Isso é evidenciado no legislativo, onde a elaboração de leis eficazes que abordem o crime cibernético é prejudicada pela falta de especialistas em tecnologia da informação e segurança cibernética. O judiciário também enfrenta desafios, uma vez que há uma escassez de juízes e promotores com experiência em casos relacionados ao cibe crime.

Para lidar com esse problema complexo, é necessário um esforço coordenado de todos os setores da sociedade. O governo, o setor privado e a sociedade civil devem unir forças para enfrentar essa ameaça em constante evolução. Uma das medidas mais urgentes é o investimento na capacitação de profissionais especializados em segurança cibernética. Isso inclui a formação de advogados com conhecimento técnico para contribuir na elaboração de leis eficazes e a capacitação de juízes e promotores para lidar com casos relacionados ao cibe crime de maneira eficiente e justa.

Além disso, a promoção de programas educacionais que incentivem o estudo da cibe segurança desde o nível básico até o superior é fundamental para criar uma base sólida de profissionais altamente qualificados nessa área. A formação de equipes multidisciplinares, envolvendo especialistas técnicos, advogados e profissionais da aplicação da lei, também é uma estratégia eficaz para enfrentar os desafios complexos que o crime cibernético apresenta.

Em resumo, a escassez de profissionais especializados é um dos principais gargalos no combate ao crime cibernético no Brasil. A capacitação e o investimento nessa mão de obra altamente qualificada são cruciais para fortalecer a capacidade do país de enfrentar essa ameaça crescente e proteger seus cidadãos e infraestrutura digital.

3.2 IMPUNIDADE QUANTO AOS CRIMES CIBERNÉTICOS

A impunidade em relação aos crimes cibernéticos é uma questão urgente e preocupante que afeta não apenas o Brasil, mas muitos países ao redor do mundo. Os crimes cibernéticos estão em constante evolução, tornando-se cada vez mais sofisticados e difíceis de rastrear e punir. Isso cria uma situação na qual os criminosos cibernéticos muitas vezes escapam das consequências de suas ações, causando prejuízos significativos à sociedade e à economia.

O exemplo citado pelo autor TOZZETO (2010) sobre as perdas dos bancos brasileiros em 2014, que totalizaram cerca de 1,8 bilhões de reais, ilustra a magnitude dos danos financeiros causados pelos crimes cibernéticos. Esses crimes incluem

roubo de senhas, boletos falsos e outros golpes que visam aproveitar a falta de conhecimento da população sobre segurança digital.

Além disso, nos últimos anos, temos testemunhado o aumento de crimes cibernéticos que exploram as redes sociais, como a disseminação de pornografia infantil, o *bullying* virtual, a violação de direitos autorais e o racismo. Esses crimes afetam diretamente a integridade das vítimas e têm um impacto negativo em toda a sociedade.

Uma das razões para a impunidade relacionada aos crimes cibernéticos é a falta de especialização dos legisladores e da magistratura na área. O mundo digital é altamente complexo e em constante mudança, o que torna essencial que aqueles que fazem e aplicam as leis compreendam profundamente os aspectos técnicos e jurídicos relacionados aos crimes cibernéticos.

O uso de criptoativos por criminosos cibernéticos para lavagem de dinheiro também é uma preocupação crescente e requer uma abordagem legal especializada para combater essa forma de crime.

Para lidar com a impunidade em crimes cibernéticos, é necessário um esforço conjunto que envolva não apenas mudanças na legislação, como o aumento de penas para crimes virtuais, mas também investimentos substanciais em programas de conformidade criminal e cibe segurança por parte de empresas públicas e privadas.

Essas iniciativas podem incentivar a capacitação de profissionais na área de segurança cibernética, promovendo o conhecimento técnico necessário para enfrentar os desafios do cibe crime de forma eficaz.

Embora existam avanços legislativos, como o Marco Civil da Internet, a Lei nº 13.709 de Proteção de Dados e a Lei nº 12.737 mais conhecida como Lei Carolina Dieckmann, ainda há muito a ser feito para criar leis específicas para o ciberespaço.

A complexidade dessas questões exige a colaboração entre especialistas em tecnologia e legisladores para garantir que as leis sejam eficazes na prevenção e punição dos crimes cibernéticos.

Portanto, a superação da impunidade em crimes cibernéticos requer uma abordagem multidisciplinar, envolvendo educação, legislação atualizada e

investimentos em tecnologia e cibersegurança, a fim de proteger os cidadãos e a infraestrutura digital do país.

CONCLUSÃO

Desta forma conclui-se com este trabalho que o Brasil é um país que está avançando em sua legislação no que trata dos crimes virtuais. Más que ainda assim ainda tem muito que desenvolver se comparado com outros países que já tinham uma legislação que trata deste assunto há algum tempo, como é o caso dos estados unidos, de forma que possa acompanhar com igualdade os crimes virtuais ao passo em que a tecnologia se desenvolve, tornando possível a aplicação das leis penais em qualquer indivíduo que pratique um delito virtual com a mesma eficiência de uma pena aplicada a alguém que comete o crime de homicídio.

Os questionamentos foram devidamente explicados e confirmou o que já se era esperado, que são crimes bastantes rentáveis e com baixa punição e que quando se tem a punição e que quando se tem a punição se é bem leve e não intimada nenhum pouco os criminosos de nosso país.

As hipóteses se mostraram verdadeiras conforme as pesquisas realizadas.

ANALYSIS OF THE IMPACTS OF CYBER CRIMES IN BRAZILIAN SOCIETY: CHALLENGES AND COMBAT PROSPECTS

Cybercrimes, also known as virtual crimes, pose a growing and intricate threat in the digital age. They encompass malicious activities targeted at computer systems and data. Types of crimes include computer attacks and data breaches, affecting areas such as property, individual freedom, and intellectual property. Impunity is a problem due to a lack of legal expertise in the field. Addressing this threat requires international cooperation, updated regulations, and investments in technology and cybersecurity. Specialized professional training is essential. In summary, cybercrimes are multifaceted, reflecting social conflicts and demanding a multidisciplinary approach to mitigate their impacts.

Keywords: Cybercrimes, cybersecurity, regulation, impunity, professional training.

REFERÊNCIAS

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acessado em: 07 de outubro de 2023.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018.** Lei Geral da Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em: 7 de outubro de 2023.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2**. Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: http://www.cert.br. Acessado em: 23 de setembro de 2023.

FERREIRA, Ivette Senise. Direito & Internet: **Aspectos Jurídicos Relevantes.** 2 ed. São Paulo: Quartier Latin, 2005.

"hacker", in **Dicionário Priberam da Língua Portuguesa** [em linha], 2008-2023. Disponível em: https://dicionario.priberam.org/hacker. Acesso em 20 de junho 2023.

KASPERSKY. **O que são crimes cibernéticos.** Disponível em: https://www.kaspersky.com.br/resource-center/threats/cybercrime. Acesso em: 30 de setembro de 2023.

MITNICK, Kevin D..; SIMON, William L. **A arte de enganar.** São Paulo: Pearson Makron Books, 2003.

OLIVO, C.K. **Avaliação de características para detecção de phishing de email.** Dissertação (mestrado), Pontifícia Universidade Católica do Paraná, Curitiba: 2010.

REVISTA FORBES. **5 tipos mais comuns de ciberataques que ocorrem no Braisl.** Disponível em: https://forbes.com.br/forbes-tech/2023/05/5-tipos-mais-comuns-de-ciberataques-que-ocorrem-no-brasil/. Acesso em 20 de junho de 2023.

RIBEIRO, Vitória. Pesquisa avançada em Google. Disponível em: https://www.privacidade.com.br/voce-sabe-o-que-e-um-crime-cibernetico/ Acesso em 03 junho 2023.

TECMUNDO. **Crimes cibernéticos: o que é, quais os riscos mais comuns e como denunciar.** Disponível em: www.tecmundo.com.br/seguranca/260062-crimes-ciberneticos-comuns-denunciar.htm. Acesso em 03 junho 2023.

XLOGIC STI. **Crimes cibernéticos: o que é, quais os mais comuns e como denunciar?.** Disponível em: https://www.xlogic.com.br/crimes-ciberneticos-o-que-e-quais-os-mais-comuns-e-como-denunciar/. Acesso em 30 de setembro de 2023

RODRIGUES COSTA, ANA JULYA. TCC. UNIVERSIDADE POTIGUAR. (2023)Acesso 23 de setembro de 2023. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/34701/1/TCC%20%20Vers%C3%A3o%20Final.pdf