CENTRO PAULA SOUZA ETEC PADRE CARLOS LEÔNCIO DA SILVA TÉCNICO EM SERVIÇOS JURÍDICOS

CRIMES CIBERNÉTICOS: Golpe do Pix

CYBERCRIME: PIX SCAM

Emelly Helena do Nascimento[1]
Evelin Borges Mendes Gomide[2]
Guilherme de Paula Espindola[3]
Maria Eduarda Nunes Bartholo[4]
Pedro Lucas Guimarães Mendes[5]
Francis Augusto Guimarães[6]

Resumo: Crime cibernético é um tipo de crime que envolve o uso de computadores, redes e tecnologia da informação para cometer uma variedade de atividades ilegais. Esses crimes podem incluir roubo de identidade, fraude eletrônica, hacking, disseminação de vírus e malware, ciberterrorismo, cyberbullying, entre outros. Os criminosos cibernéticos usam técnicas sofisticadas para acessar informações privadas, danificar sistemas e redes, ou extorquir dinheiro de empresas e indivíduos. Esses crimes podem ter consequências graves e afetar a segurança financeira, a privacidade e a reputação das vítimas. Os avanços tecnológicos constantes tornam essencial uma abordagem proativa na proteção contra o crime cibernético. Empresas e indivíduos devem implementar medidas de segurança robustas, como firewalls, antivírus e educação cibernética, para mitigar os riscos. **Palavras-chave:** Internet 1. Golpe 2 . Pix 3.

Abstract: *Cybercrime is a type of crime that involves the use of computers, networks and information technology to commit a variety of illegal activities. These crimes can include identity theft, electronic fraud, hacking, spreading viruses and malware, cyberterrorism, cyberbullying, among others. Cyber criminals use sophisticated techniques to access private information, damage systems and networks, or extort money from companies and individuals. These crimes can have serious consequences and affect victims' financial security, privacy and reputation. Constant technological advances make a proactive approach to protecting against cybercrime essential. Companies and individuals must implement robust security measures, such as firewalls, antivirus and cyber education, to mitigate risks.* ***Keywords:*** *Internet 1. Coup 2. Pix 3.*

[1] Técnico em Serviços Jurídicos - Etec Padre Carlos Leôncio da Silva. emellyhelena2005@gmail.com

[2] Técnico em Serviços Jurídicos - Etec Padre Carlos Leôncio da Silva. evelin.bgomide@gmail.com

[3] Técnico em Serviços Jurídicos - Etec Padre Carlos Leôncio da Silva. guilhermedepaulaespindola5@gmail.com

[4] Técnico em Serviços Jurídicos - Etec Padre Carlos Leôncio da Silva. eduardamaria85700@gmail.com

[5] Técnico em Serviços Jurídicos - Etec Padre Carlos Leôncio da Silva. pedrolucas7889@gmail.com

[6] Professor da Etec Padre Carlos Leôncio da Silva. francisguimaraes@yahoo.com.br

1.INTRODUÇÃO

O Crime Cibernético está previsto pela Lei 14.155/2021. A internet acabou trazendo muitas facilidades tanto para pesquisas, conhecimentos e até mesmo negócios online, mas também trouxe uma grande preocupação para alguns usuários, pois com seus variados tipos, podem afetar qualquer pessoa ou empresa. Por vários problemas devemos ter bastante cuidado ao abrir links ou arquivos desconhecidos que recebemos que nem sempre pode ser confiável.

No mundo contemporâneo, a integração acelerada da tecnologia transformou radicalmente nossa forma de viver. Desde a automação de tarefas cotidianas até a comunicação instantânea global, a tecnologia proporciona uma gama diversificada de facilidades, simplificando processos e conectando comunidades. No entanto, essa revolução digital também introduziu desafios significativos.

Entre esses desafios, os crimes cibernéticos emergem como uma ameaça inegável. Com o aumento das transações online e do armazenamento de dados na nuvem, a segurança e a privacidade de indivíduos e organizações tornaram-se alvos constantes. Hackers habilidosos exploram vulnerabilidades, comprometendo informações confidenciais e prejudicando a confiança na ciberesfera.

Neste contexto, a resposta legal torna-se crucial. As leis que visam combater os crimes cibernéticos estão em constante evolução para lidar com as complexidades dessas ameaças digitais. discutiremos não apenas as disposições legais existentes, mas também as tendências e inovações na legislação, destacando como os sistemas jurídicos se adaptam para enfrentar um cenário em constante mutação.

Além disso, explorar exemplos de crimes cibernéticos, mostrando as consequências enfrentadas por perpetradores e vítimas. Isso proporcionará uma compreensão mais profunda das implicações práticas das leis em vigor e da necessidade contínua de atualizações legislativas para acompanhar o avanço rápido da tecnologia.

Em resumo, esta apresentação não apenas abordará as leis destinadas a enfrentar e punir crimes cibernéticos, mas também mergulhará nas complexidades do ambiente digital, destacando a interseção dinâmica entre tecnologia, segurança jurídica e a necessidade contínua de adaptação para preservar a integridade cibernética.

2.DESENVOLVIMENTO

O crime cibernético é cometido por criminosos que tem intensão de ganhar dinheiro ou invadir a privacidade de alguém, quase sempre são realizados por indivíduos ou organizações, usando técnicas avançadas.

Normalmente os dispositivos são infectados através do malware que tem a função de prejudicar ou explorar quaisquer dispositivos, rede ou serviço. Extraindo dados utilizados das vítimas para ter ganhos.

Os crimes mais cometidos estão relacionados aos, furto de dados, apologia ao crime, divulgação de fotos íntimas e o plágio. Deste tem aumentado a invasão da segurança, tendo em torno um aumento de 31% no ano de 2020 a 2021. Da consultoria Accenture, cada empresa registrou 270 ataques em 2021.Uma violação custa a uma empresa em média de US$200.000 fazendo que muitas empresas fecham dentro de 6 meses, de acordo com a seguradora Hiscox.

Além dos ataques de empresas, eles também afetam os indivíduos, pois muitos armazenam dados e informações pessoais.

Como surgiu o crime cibernético:

O termo cibercrime foi criado no final da década de 1990, que com o crescimento da internet e sua divulgação em diversas esferas da sociedade, o cibercrime também se expandiu. Foram registrados casos de fraudes online, Phishing e disseminação de Malware.

Hoje em dia o cibercrime continuou a evoluir com o crescimento das transações online, comércio eletrônico e serviços financeiros digitais. E novas formas de crime cibernético surgiram, incluindo vazamento de dados, exploração de vulnerabilidades em sistemas e ataques direcionados a governos e empresas.

2.1 CASOS

Alguns casos são as publicidades enganosas, aquelas que apresentam informações falsas ou enganosas sobre um produto ou serviço, com o objetivo de induzir os consumidores a tomar decisões com base em informações incorretas. Essa prática é ilegal em muitos países e pode causar danos aos consumidores e à confiança da empresa.

Existem vários tipos de publicidade enganosa, alguns exemplos incluem:

Falsas alegações, quando a publicidade faz afirmações não comprovadas sobre as características ou benefícios do produto, levando os consumidores a acreditar em algo que não é verdadeiro;

Omissão de informações, quando a publicidade omite informações relevantes sobre o produto ou serviço, levando os consumidores a tomar decisões com base em uma visão parcial ou incompleta da oferta;

Preços falsos ou enganosos, quando a publicidade apresenta preços que não correspondem ao valor real do produto ou serviço, seja por meio de promoções fictícias ou ocultação de taxas adicionais;

Fotos e imagens enganosas: Quando a publicidade usa imagens ou fotos manipuladas para fazer o produto parecer diferente do que realmente é.

Para evitar, os consumidores podem tomar algumas precauções:

Pesquisar e comparar, faça pesquisas sobre o produto ou serviço antes de tomar uma decisão. Compare as informações desenvolvidas em diferentes fontes para garantir sua precisão;

Garantindo fontes, procure informações em fontes, como sites oficiais, estimativas de consumidores e órgãos reguladores;

Ler os detalhes, preste atenção aos detalhes da oferta, incluindo letras pequenas e termos e condições. As informações importantes muitas vezes estão em locais menos visíveis;

Conheça seus direitos, esteja ciente dos seus direitos como consumidor e das leis de proteção do consumidor em vigor no seu país;

Denuncie práticas suspeitas, caso a publicidade seja enganosa, denuncie-a às autoridades competentes ou órgãos de proteção ao consumidor.

Crimes virtuais crescem no Brasil, com muitas pessoas vivendo diversas emoções ao perceber que acreditou em algo que não existe e perdendo seus bens. Alguma delas deixando suas histórias como um alerta para todos indivíduos. Sendo assim:

‘’O número de golpes cometidos pela internet sofreu um aumento de 175% durante a pandemia e nossa equipe conversou com vítimas de fraude financeira e Stalking, além de acompanhar uma operação policial contra a pornografia infantil. Um dos personagens ouvidos pelo programa foi o auxiliar de educação Claudinei de Jesus

Oliveira. Aos 50 anos, o morador de Sorocaba entrou para a estatística das vítimas de um dos golpes mais comuns na internet, o do boleto falso, e a repórter Sara Pavani foi à cidade acompanhar o caso da família e também ouviu um especialista, que dá dicas de como não passar pela mesma situação.''

''Outra vítima ouvida por nossa equipe - o repórter Guilherme Belarmino e o repórter cinematográfico Alex Gomes - foi a modelo Rayanne Adorno, de Teresina (PI). Ameaçada pelo ex-companheiro, o francês Malik Roy, ela conseguiu dar fim a três anos de angústia ao vê-lo ser preso este mês. Ele foi denunciado pelo Ministério Público do Piauí por injúria racial, violência doméstica e Stalking, que passou a ser considerado crime a partir de abril de 2021, e é o ato de perseguir alguém reiteradamente.''

Já as repórteres Danielle Zampollo e Nathalia Tavolieri acompanharam a ação de policiais em São Paulo na nona fase da Operação Luz na Infância, que combate crimes de abuso e de exploração sexual de crianças e adolescentes na internet. A dupla foi à casa de um dos suspeitos e registrou a prisão de um homem de 37 anos, acusado de armazenar e compartilhar fotos e vídeos com conteúdo relacionado à pornografia infantil.

2.2 LEIS

Os crimes na internet correspondem a todos aqueles crimes que acontecem em ambientes virtuais, e podem ser classificados de duas maneiras:

PRIMEIRA DIVISÃO

Crimes puros: tem o objetivo de atingir o sistema de um computador, seja a parte física ou de dados, geralmente praticado por hackers;

Crimes mistos: o alvo não é o computador, mas os bens da vítima, ou seja, a internet é utilizada como meio para realizar o crime, como, por exemplo, transferências ilícitas de bens e/ou valores;

Crimes comuns: aqueles que utilizam a internet para realizar o crime, sendo assim reconhecidos pela lei, como o caso da pornografia infantil que já é abordado no Estatuto da Criança e do Adolescente.

SEGUNDA DIVISÃO

Crimes próprios: aqueles praticados exclusivamente por meio de computadores;

Crimes impróprios: que atingem o bem comum sendo o meio virtual apenas uma das formas de execução do crime, podendo ser praticado por outros meios.

E como que a Lei atua para punir os que utilizam de má fé os meios tecnológicos?

Em 30 de novembro de 2012, com a edição da Lei N° 12.737, o Código Penal Brasileiro foi alterado, sendo acrescentado os artigos 154-A, 154-B, 266 e 298 para punição dos crimes cometidos na internet.

E essa Lei ficou conhecida por "Lei Carolina Dieckmann", o caso de uma atriz global, sancionada pela presidente da Época, Dilma Rousseff, após algumas fotos íntimas da atriz terem vazado por conta de uma invasão em seu computador pessoal.

LGPD (Lei Geral de Proteção de Dados) Lei N° 13.709/2018, com objetivo de proteger os direitos fundamentais da liberdade e privacidade.

Marco Civil da Internet, Lei N° 12.965/2014, que garante a proteção dos dados pessoais, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil.

2.3 MODELOS

Existem muitos tipos de crimes cibernéticos, incluindo:

Roubo de identidade: quando um criminoso usa informações pessoais, como nome, número do Seguro Social ou informações financeiras, sem a autorização da vítima para obter crédito, realizar transações bancárias ou outras atividades financeiras;

Fraude eletrônica: quando um criminoso usa um meio eletrônico, como um email fraudulento ou um site falso, para obter informações pessoais ou financeiras de uma vítima;

Hacking: quando um criminoso usa técnicas para acessar informações privadas ou danificar sistemas de computador;

Malware: quando um criminoso usa um software malicioso para infectar um sistema de computador ou dispositivo móvel com o objetivo de roubar informações ou danificar o sistema;

Phishing: quando um criminoso usa um e-mail fraudulento ou site falso para obter informações pessoais ou financeiras de uma vítima;

Ransomware: quando um criminoso usa um software malicioso para bloquear o acesso a um sistema ou dados, exigindo um resgate para restaurar o acesso;

Ciberbullying: quando um criminoso usa a tecnologia da informação para assediar ou ameaçar alguém;

Ciberterrorismo: quando um criminoso usa a tecnologia da informação para causar danos graves ou ameaçar a segurança global;

Extorsão: quando um criminoso usa a tecnologia da informação para extorquir dinheiro de uma vítima;

Esses são apenas alguns exemplos de crimes cibernéticos, e a lista continua crescendo à medida que os criminosos cibernéticos desenvolvem novas técnicas e tecnologias para cometer crimes.

3 GOLPE DO PIX

O golpe do PIX é uma forma de fraude que aproveita do sistema de pagamento instantâneo (PIX), que foi introduzido no Brasil em 2020. Essa modalidade de golpe pode envolver diferentes estratégias, mas geralmente tem o objetivo de enganar as pessoas para que realizem transferências de dinheiro para os golpistas.

Como funciona o golpe do Pix:

Os golpistas formam um comprovante de transferência via Pix de um determinado banco e o enviam por e-mail ou qualquer outro aplicativo. Ao receber o falso *print*, logo a pessoa estranha a mensagem e pergunta do que se trata. Nesse momento, o criminoso responde que errou ao fazer a transferência e pede à vítima para reembolsar o valor para a conta dele – daí o nome "Pix reverso", Ou seja, além de não ter depositado dinheiro algum na conta da vítima, o ladrão ainda tenta fazer com que ela lhe pague uma quantia. Também são enviadas mensagens ou e-mail com um link para cadastro da chave Pix levando a uma página falsa criada pelos golpistas. O golpe pode funcionar de várias maneiras, mas geralmente envolve a manipulação

ou exploração do sistema de pagamento no Brasil para enganar as pessoas. Alguns dos outros métodos comuns são:

Troca de chaves, que nada mais é do que o golpista convencer o usuário a adicionar sua chave PIX (CPF, número de telefone ou e-mail) em uma conta bancária controlada por golpistas. Dessa forma, quando o usuário fizer um pagamento, o dinheiro vai para a conta do golpista em vez do destinatário desejado;

QR code falso, o golpista envia um QR code com um valor errado, fazendo com que o usuário transfira uma quantia maior do que pretendia;

Engenharia social, onde o golpista usa informações pessoais disponíveis publicamente sobre o usuário para ganhar sua confiança e convencê-lo a fazer pagamentos.

Reembolsos inexistentes, os golpistas podem se passar por empresas ou instituições financeiras e prometerem reembolsos que, na realidade, não existem. A vítima é induzida a fornecer informações pessoais e bancárias para receber o suposto reembolso.

É importante ressaltar que o PIX em si não é inseguro. O problema reside no comportamento humano e na falta de atenção às boas práticas de segurança ao realizar transações financeiras.

3.1 “ Urubu do Pix ”:

O golpe do Urubu do Pix é um entre os muitos esquemas fraudulentos que circulam na Internet para roubar pessoas interessadas em obter dinheiro fácil e rápido. Por meio de redes sociais, cibercriminosos compartilham uma proposta tentadora, em que as vítimas precisariam apenas lhes enviar quantias em dinheiro para receber, supostamente, até 10 vezes o valor depositado. Após a transferência, contudo, o dinheiro investido fica retido em contas falsas ou roubadas por golpistas.

O esquema funciona assim: os golpistas usam redes sociais como Twitter, Instagram e TikTok para divulgar uma oferta tentadora. Segundo os anúncios, você só precisa enviar uma quantia em dinheiro via Pix para uma chave desconhecida e receber até 10 vezes o valor de volta. Por exemplo, se você enviar R$ 100,00 eles dizem que vão te devolver R$ 1.000,00.

Para atrair as vítimas, eles usam imagens de um urubu ao lado de uma tabela com os valores dos supostos investimentos e seus retornos. Os golpistas também mostram vídeos e capturas de tela de pessoas que supostamente participaram do esquema e ficaram ricas.

Depois que realiza a transferência, o dinheiro nunca mais retorna. Os golpistas ficam com ele e bloqueiam o seu contato.

Essas pessoas usam contas falsas ou roubadas para receber o dinheiro e dificultar o rastreamento. A pessoa fica no prejuízo e ainda arrisca ter seus dados pessoais e bancários expostos.

Como prevenir e denunciar:

Para evitar cair nesse tipo de golpe, algumas medidas são importantes como verificar sempre as informações, antes de fazer qualquer transação, verifique cuidadosamente os dados da pessoa ou empresa que está recebendo o pagamento;

Desconfiar de ofertas muito vantajosas, desconfie de promoções ou sorteios que pareçam ser boas demais para serem verdadeiras. Sempre pesquise e confirme a veracidade da oferta antes de tomar qualquer decisão. Esse tipo de golpe é chamado de engenharia social, pois se aproveita da manipulação psicológica das pessoas para tirar vantagem. Os criminosos criam um senso de urgência e uma proposta irrecusável para fazer com que os internautas acreditem na mentira e não pensem muito antes de agir, comprando a ideia tentadora e enviando dinheiro;

Não compartilhar informações pessoais, nunca forneça dados pessoais, senhas ou informações bancárias por telefone, e-mail ou mensagens, especialmente se a solicitação vier de fontes desconhecidas. Proteja seus dados. E se caso receber alguma mensagem ou anúncio sobre o Urubu do Pix, denuncie e alerte seus amigos e familiares para que não ocorra de mais pessoas caírem no golpe;

Manter o aplicativo seguro, proteja seu smartphone com senhas ou biometria e certifique-se de que seu aplicativo PIX esteja sempre atualizado;

Buscar informações oficiais, em caso de dúvida, entre em contato diretamente com a empresa ou instituição financeira envolvida na transação para verificar a autenticidade da solicitação.

No mundo digital, os golpes são uma realidade cada vez mais presente. Sendo esse uns dos exemplos mais recentes. No entanto, esse esquema é apenas uma das muitas armadilhas criadas por criminosos na Internet, visando enganar pessoas que

buscam uma maneira fácil e rápida de obter dinheiro. Tendo o modo de aplicação bastantes semelhantes.

Uma dica importante é buscar informações em fontes confiáveis, como os portais do Banco Central e da Comissão de Valores Mobiliários (CVM), a fim de verificar se o ativo em questão é legítimo ou se trata de uma tentativa de golpe. Além disso, é essencial estar sempre atualizado sobre os novos golpes que surgem e compartilhar essas informações, criando uma rede de proteção coletiva.

No mundo virtual, a prevenção é a melhor defesa. Ao adotar medidas de segurança e manter-se informado com as tendências dos cibercriminosos é uma das formas de evitar esses tipos de golpes na internet.

3.2 Recorde no Brasil:

Um estudo recente da *Nord Security* revela que aproximadamente 71% dos brasileiros já se tornaram vítimas de pelo menos um golpe online. O levantamento, que contou com a participação de 1194 cidadãos maiores de 18 anos, foi realizado entre os dias 20 e 22 de março de 2023. Segundo o relatório, as fraudes mais comuns estão ligadas a finanças e informações bancárias.

Mesmo a maioria dos participantes já tendo sido vítima de algum tipo de ameaça virtual, 69% deles foram capazes de identificar todas as ameaças apresentadas durante a pesquisa. No entanto, 26% dos entrevistados admitiram que seus dispositivos foram infectados por vírus, malware ou Spyware no último ano.

O operador de máquinas Fábio da Silva Pereira entrou em um site de leilão de veículos. Onde ele deu um lance de R$ 59 mil sem nunca ao menos ter visto o carro presencialmente. Recebeu até uma nota fiscal com QR Code. Logo o operador revela o que vivenciou:

"Eu fiz um Pix, uma transferência via Pix, no valor de R$ 59 mil. O site parecia, até então, ser um site legalizado, bem direito, nós ficamos acompanhando. Tive que fazer a inscrição no site, entrar com o meu documento, meus dados, tudo direitinho, e fiz todo o procedimento para poder fazer o lance" Apenas 24 horas depois de fazer o pagamento, ele percebeu que tinha caído num golpe e registrou o caso na polícia.

3.3 Convenção de Budapeste:

‘’O Governo Federal promulgou a Convenção sobre o Crime Cibernético, firmada em Budapeste. O Brasil, ao aceitar o convite do Conselho da Europa, passou a ser um dos países que aderiram a tal instrumento internacional multilateral, fortalecendo, assim, os laços de cooperação com parceiros estratégicos no enfrentamento aos crimes cibernéticos.

O Decreto nº 11.491, que traz a decisão, foi publicado no Diário Oficial da União (DOU), no dia 12 de abril de 2023. Por meio da denominada Convenção de Budapeste, firmada em 23 de 2001, as autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos, assim como de outras infrações penais, que demandem a obtenção de provas eletrônicas/digitais armazenadas em outros países. Prevê-se uma cooperação “mais intensa, rápida e eficaz”’. Diz Ministério da Justiça e Segurança Pública.

A Convenção de Budapeste reúne grande número de países com os quais o Brasil compartilha a maior parte dos casos de cooperação jurídica internacional hoje em tramitação e serve de base de colaboração contra ampla variedade de crimes realizados por via cibernética. Somando-se a 67 membros, o país contará com ferramenta adicional para combater o crime cibernético, que exige meios de cooperação internacional céleres, mediante os quais os órgãos responsáveis possam requerer e compartilhar as provas necessárias.

As autoridades brasileiras terão, assim, acesso mais ágil a provas eletrônicas produzidas sob jurisdição estrangeira, o que repercutirá positivamente em termos de condenação penal dos crimes cibernéticos.

Budapeste prevê como crimes, especificamente, o acesso e intercepção ilegal em redes informáticas, o dano e sabotagem informática, o uso de vírus, e a posse, produção e distribuição de material de pornografia infantil na Internet.

Seus tipos variam entre fraude por e-mail e pela Internet, Fraude de identidades (onde informações pessoais são roubadas e usadas), roubo de dados financeiros ou de pagamento com cartão, roubo e venda de dados corporativos, ciberextrorção (exigir dinheiro para evitar um ataque ameaçado).

Na convenção indica as penas a prática dos crimes, pois nela, visa facilitar a cooperação internacional para o combate ao crime na internet. O documento lista os principais crimes cometidos por meio da rede mundial de computadores.

O Tratado reconhece ainda a necessidade da cooperação entre os Estados e a indústria privada no combate da cibercriminalidade, e ainda a proteção aos desenvolvimentos das tecnologias da informação. A adesão do Brasil na Convenção é um passo importante para o aprimoramento da legislação penal contra os crimes cibernéticos. Pois trata-se de cooperação internacional.

3.4 Como evitar os crimes cibernéticos:

Manter o software e o sistema operacional atualizados garante que você se beneficie das correções de segurança mais recentes que protege o seu computador; Usar um antivírus ou uma solução de segurança de Internet abrangente, como o Kaspersky Total Security, é uma forma inteligente de proteger seu sistema contra-ataques;

Use senhas fortes que sejam difíceis de adivinhar e não as registre em lugar algum. Com isso vai aumentar a dificuldade dos hackers;

Nunca abra anexos em e-mails de spam;

Uma maneira muito comum pela qual os computadores acabam infectados por ataques de malware e outras formas de crime cibernético é por meio de anexos em emails de spam. Nunca abra um anexo estranho;

Não clique em links de spam ou em sites desconhecidos;

Outra maneira pela qual as pessoas acabam sendo vítimas de crimes cibernéticos é clicando em links de e-mails de spam ou em sites desconhecidos. Evite fazer isso para manter sua segurança;

Nunca forneça dados pessoais por telefone ou e-mail, a menos que tenha confiança na pessoa;

Entre em contato diretamente com a empresa para confirmar pedidos suspeitos;

Se uma empresa ligar para você e solicitar dados ou informações pessoais, desligue. Ligue de volta usando o número no site oficial para garantir que você está

falando com a empresa e não com um cibercriminoso. O ideal é usar um telefone diferente, pois os cibercriminosos podem manter a ligação conectada;

Fique de olho nas URLs em que está clicando. Evite clicar em links com URLs desconhecidas ou que pareçam spam;

Fique de olho nos seus extratos bancários;

É importante perceber o quanto antes que você foi vítima de um crime cibernético;

Fique de olho nos seus extratos bancários e questione o banco sobre qualquer transação que pareça estranha. O banco poderá investigar se é a respeito de uma ação criminosa.

Além disso, as instituições financeiras também têm a responsabilidade de investir em medidas de segurança e educação para seus clientes, a fim de reduzir o número de golpes e proteger a integridade financeira dos usuários. A conscientização e a vigilância constante são fundamentais para combater o golpe do PIX e outras formas de fraudes financeiras.

As instituições financeiras têm um papel fundamental na proteção dos seus clientes contra crimes cibernéticos e na segurança das transações financeiras. Para isso, elas adotam diversas medidas para garantir a integridade dos sistemas e a privacidade dos dados dos usuários. Algumas dessas medidas incluem:

Criptografia, as instituições financeiras utilizam técnicas de criptografia para proteger as informações sensíveis dos clientes, como senhas, números de contas e dados de cartões de crédito. A criptografia garante que os dados sejam transmitidos de forma segura e sejam armazenados de maneira protegida nos servidores da instituição;

Autenticação em duas etapas (2FA), a 2FA é uma medida de segurança que requer duas formas de identificação antes de permitir o acesso à conta do cliente. Além da senha, é necessário fornecer um segundo fator, como um código enviado por SMS, e-mail ou gerado por um aplicativo de autenticação;

Monitoramento de atividades suspeitas, as instituições financeiras possuem sistemas de monitoramento avançados para detectar atividades incomuns ou suspeitas nas contas dos clientes. Caso alguma atividade fora do padrão seja identificada, a instituição pode bloquear a conta temporariamente ou entrar em contato com o cliente para verificar a autenticidade da transação;

Sistemas antifraude, as instituições financeiras investem em sistemas antifraude que utilizam algoritmos e aprendizado de máquina para identificar padrões de comportamento e transações fraudulentas. Esses sistemas ajudam a prevenir e combater atividades criminosas em tempo real;

Atualizações constantes, as instituições financeiras mantêm seus sistemas e aplicativos sempre atualizados para corrigir possíveis vulnerabilidades e garantir a segurança dos dados dos clientes;

Educação do cliente, além das medidas técnicas, as instituições financeiras também investem em programas de conscientização e educação do cliente sobre segurança cibernética. Isso inclui orientações sobre como evitar golpes, proteger suas informações pessoais e reconhecer tentativas de Phishing;

Canais de denúncia e suporte, as instituições financeiras disponibilizam canais de atendimento ao cliente para relatar atividades suspeitas, fraudes ou problemas de segurança. Dessa forma, os clientes podem obter ajuda rapidamente caso suspeitem de alguma irregularidade em suas contas;

Testes de segurança, periodicamente, as instituições financeiras realizam testes de segurança para avaliar a resistência de seus sistemas a possíveis ataques. Esses testes ajudam a identificar e corrigir vulnerabilidades antes que sejam exploradas por criminosos.

Entre tanto as instituições financeiras estão constantemente aprimorando suas medidas de segurança cibernética para proteger os dados e o patrimônio de seus clientes. Logo, é essencial que os próprios clientes também sejam proativos e tomem medidas para proteger suas informações. A colaboração entre instituições e clientes é fundamental para criar um ambiente mais seguro no mundo digital.

4 CONSIDERAÇÕES FINAIS

Os crimes cibernéticos são uma ameaça global que exige colaboração entre governos, empresas e indivíduos. Investir em educação cibernética, implementar leis atualizadas e promover medidas de segurança robustas são essenciais. é necessário devido à evolução das ameaças enfrentar os crimes cibernéticos pois precisamos ter um esforço constante para criar um ambiente digital mais seguro e resistente.

Em um mundo cada vez mais conectado, os crimes cibernéticos não apenas representam uma ameaça significativa que ultrapassa fronteiras físicas, mas também desafia a segurança digital em todos os setores da sociedade.

A pesquisa realizada não se limitou apenas a mapear as origens dos crimes cibernéticos, mas também aprofundou a análise dos impactos dessas atividades maliciosas na sociedade moderna. A investigação abordou questões como a evolução das táticas dos criminosos digitais, o papel da dark web e as consequências socioeconômicas para empresas e cidadãos.

Ao examinar as dimensões mais amplas, a pesquisa destaca a urgência de estratégias abrangentes para combater os crimes cibernéticos. Além de medidas reativas, como leis e regulamentações, destaca-se a importância crucial de abordagens proativas, como investir em programas de educação cibernética desde as idades mais jovens. A promoção de uma compreensão abrangente dos perigos online e o estabelecimento de melhores práticas de segurança tornam-se elementos essenciais na construção de uma sociedade digital mais resiliente.

O estudo também investigou casos de sucesso em iniciativas educacionais cibernéticas ao redor do mundo, fornecendo insights sobre estratégias eficazes que podem ser adotadas em diferentes contextos culturais e educacionais.

Além disso, a pesquisa aborda a necessidade de colaboração entre setores público e privado, destacando a importância da cooperação internacional para enfrentar uma ameaça que não conhece fronteiras. A criação de parcerias entre empresas, governos e organizações sem fins lucrativos surge como uma abordagem vital para fortalecer a resiliência cibernética global.

Em resumo, esta pesquisa não apenas analisou as várias dimensões dos crimes cibernéticos, mas também propôs estratégias abrangentes, desde a educação precoce até a colaboração global, visando mitigar os impactos e construir uma sociedade digital mais segura e consciente.

5 REFERÊNCIAS

AUTOR FARIA, Antonio Bento de, 1876. **Código penal brasileiro** data 1961, 1959, 1933 https://blog.algartelecom.com.br/tecnologia/crimes-ciberneticos/ https://online.pucrs.br/blog/public/crimes-ciberneticosconceitoprevencao?hs_amp=true

https://blog.g7juridico.com.br/crimes-na-internet/
https://www.infomoney.com.br/minhas-financas/instituicoes-financeiras-criamseguro-que-indeniza-em-casos-de-golpes-com-pix-veja-como-funciona/amp/
https://blog.picpay.com/golpe-do-pix/
https://olist.com/blog/pt/gestao-empresarial/pos-venda/publicidade-enganosa/
https://blog.pagseguro.uol.com.br/o-que-e-engenharia-social/
https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origemdocibercrime-203073/
https://g1.globo.com/profissao-reporter/noticia/2022/07/27/crimes-virtuais-crescemno-brasil-veja-flagrante-e-historias-de-vitimas-com-o-profissao-reporter.ghtml
https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=D11491&text=Promulga%20a%20Conven%C3%A7%C3%A3o%20sobre%20o,23%20de%20novembro%20de%202001
https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime .