REVISTA MUNDO EM MOVIMENTO
Uninassau-Caruaru
1(1): 56-74, 2024
ISSN: 2966-2176

FURTO DE IDENTIDADE

IDENTITY THEFT

Jamile Eleutiane
Email: jamileeleutiane@gmail.com

Anne Thaís Brito de Oliveira
Email: annethaisoliv@gmail.com

RESUMO: O furto de identidade ocorre quando alguém utiliza informações pessoais de outra pessoa sem autorização para obter vantagens ilícitas ou cometer fraudes.Os dados como nome, CPF, RG, informações bancárias e até perfis em redes sociais, são usados pelos criminosos com a intenção de se passar pela vítima e realizar atividades financeiras ou pessoais em seu nome. Esse tipo de crime pode resultar em prejuízos financeiros, problemas de crédito e até questões legais para a vítima, que muitas vezes desconhece as transações feitas em seu nome. Dentre os crimes mais comuns derivados do furto de identidade estão fraudes com cartões de crédito, obtenção de empréstimos, linhas de crédito, fraudes fiscais e o phishing.Vale ressaltar que para realizar esses tipos de crimes utilizam uma ferramenta especial a inteligência artificial.A legislação brasileira trata o furto de identidade com rigor, podendo incluir crimes como estelionato, falsidade ideológica e até invasão de dispositivo informático, dependendo dos métodos utilizados pelo criminoso.

PALAVRAS-CHAVE: furto de identidade, fraudes, inteligência artificial e phishing.

ABSTRACT: Identity theft occurs when someone uses another person's personal information without authorization to obtain illicit advantages or commit fraud. Data such as name, CPF (Brazilian taxpayer ID), RG (Brazilian identity card), banking information, and even social media profiles are used by criminals with the intent of impersonating the victim and carrying out financial or personal activities in their name.This type of crime can lead to financial losses, credit issues, and even legal problems for the victim, who is often unaware of the transactions made in their name. Among the most common crimes resulting from identity theft are credit card fraud, obtaining loans, credit lines, tax fraud, and phishing. It is worth noting that artificial intelligence is often used as a tool to carry out these types of crimes. Brazilian law treats identity theft rigorously, potentially involving crimes such as fraud, identity falsification, and even unauthorized access to computing devices, depending on the methods used by the criminal.

KEYWORDS: identity theft, fraud, artificial intelligence and phishing.

1. Introdução

O furto de identidade é um problema crescente na sociedade contemporânea, impulsionado pelo avanço das tecnologias e pela massiva circulação de dados na internet. Esse tipo de crime consiste na apropriação indevida de informações pessoais — como o nome, CPF, dados bancários e

senhas — com o objetivo de obter vantagens ilícitas, desde a realização de compras até a contratação dos mais variados serviços. A gravidade desse fenômeno não está apenas no prejuízo econômico, mas também no impacto psicológico para as vítimas, que enfrentam um longo e burocrático processo para provar sua inocência.

O crime de furto de identidade é considerado um furto simples, pelo fato do criminoso subtrair para ele ou para outro os dados pessoais da vítima,sem a necessidade do criminoso usar violência ou ameaça contra a vítima,dessa forma o furto de identidade ocorre e a vítima nem percebe. Porém de acordo com o art 155 § 4º-B do Código Penal, quando o furto de identidade ocorre por meios digitais se torna um furto qualificado onde a pena se torna mais grave.

> O furto de acordo com o "código penal - Decreto-Lei nº 2.848, de 7 de dezembro de 1940.
> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
>
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
>
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
>
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
>
> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
>
> I - com destruição ou rompimento de obstáculo à subtração da coisa;
>
> II - com abuso de confiança, ou mediante fraude, escalada ou destreza;
>
> III - com emprego de chave falsa;

> IV - mediante concurso de duas ou mais pessoas
>
> § 4º-A A pena é de reclusão de 4 (quatro) a 10 (dez) anos e multa, se houver emprego de explosivo ou de artefato análogo que cause perigo comum. (Incluído pela Lei nº 13.654, de 2018)
>
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
>
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)
>
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; (Incluído pela Lei nº 14.155, de 2021)
>
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (Incluído pela Lei nº 14.155, de 2021)”

Uma das principais causas desse tipo de crime é a vulnerabilidade dos sistemas de proteção de dados, além da falta de conscientização da população sobre a importância da segurança digital. Sites fraudulentos, e-mails de phishing e vazamentos de dados em empresas são exemplos comuns de como criminosos obtêm essas informações. A facilidade com que dados pessoais circulam na internet cria um ambiente propício para essas práticas, expondo tanto indivíduos quanto empresas a riscos significativos.

Phishing é uma prática criminosa em que golpistas tentam obter dados sensíveis, como senhas, informações bancárias e números de cartão de crédito, enganando as vítimas por meio de mensagens fraudulentas. Essas mensagens geralmente imitam comunicações de instituições confiáveis, como bancos, empresas de tecnologia ou serviços de e-

commerce, para induzir a vítima a clicar em links maliciosos ou fornecer dados pessoais.

Essas fraudes ocorrem principalmente por e-mails, SMS, redes sociais ou sites falsos, que replicam visualmente sites legítimos. Uma vez que o usuário fornece seus dados, os criminosos podem usá-los para cometer fraudes financeiras, roubo de identidade ou outros tipos de crimes cibernéticos.

Com o avanço da tecnologia os crimes digitais se tornaram mais frequentes, entrando em vigor na legislação brasileira em 2012,como crime cibernético. O crime cibernético ocorre quando o autor comete qualquer tipo de ato ilícito usando os meios digitais para violar a privacidade e os dados através dos meios virtuais ou eletrônicos. Alguns desses crimes são Clonagem de whatsapp,Boletos falsos,Fraudes bancárias. Nesse contexto os ataques de *phishing* têm se tornado uma das formas mais eficazes de exploração cibernética.

As táticas que são observadas no crime de ciberataque phishing, em que um fraudador finge ser um executivo da empresa que precisa urgentemente de uma transferência eletrônica para uma conta nova ou desconhecida.Os ladrões de identidade geralmente obtêm informação pessoal como senhas, números de identidade, números de cartão de crédito ou CPF, e fazem mau uso destes dados para agir de forma fraudulenta em nome da vítima.

Podemos observar assim uma das leis sobre cibercrimes de n°(12.737/2012),mais conhecida como Lei Carolina Dieckmann tem como principal finalidade criminalização da invasão de celulares, de computadores ou qualquer sistema informático para obter, adulterar ou destruir dados a

fim de obter vantagem ilícita, que podem ser o objetivo de invasão dos dispositivos informáticos para instalar a vulnerabilidade nas vítimas.

> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput** .
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

> **Ação penal**
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A "Lei Carolina Dieckmann" é o nome popular dado à Lei nº 12.737/2012, criada após a atriz Carolina Dieckmann ter fotos pessoais vazadas sem consentimento em 2011. Esse incidente trouxe à tona a necessidade de uma legislação específica para crimes cibernéticos no Brasil. A lei foi sancionada em 2012 e entrou em vigor em 2013, estabelecendo punições para crimes digitais, incluindo a invasão de dispositivos eletrônicos e a obtenção de dados pessoais sem autorização.

Os Principais pontos da Lei Carolina Dieckmann:

1.1. Invasão de Dispositivos:

- A lei criminaliza a invasão de dispositivos informáticos (computadores, smartphones, tablets) alheios para obter, adulterar ou destruir dados sem autorização.
- A pena é de 3 meses a 1 ano de prisão, além de multa.

1.2. Agravantes:

- A pena pode ser aumentada se houver divulgação, comercialização ou transmissão dos dados obtidos ilegalmente.

- Caso a invasão resulte na obtenção de comunicações privadas, segredos comerciais ou industriais, ou de informações sigilosas, a pena pode aumentar.

1.3. Falsificação e Fraude Eletrônica:

- A lei também abrange situações de falsificação e fraudes eletrônicas, podendo ser aplicada em casos de roubo de identidade e outros tipos de fraudes digitais.

1.4. Responsabilidade por Divulgação:

- A divulgação de informações pessoais obtidas ilegalmente é punida, visando proteger a privacidade das vítimas.

A Lei Carolina Dieckmann foi um marco no combate aos crimes cibernéticos no Brasil, criando um precedente para a proteção de dados e privacidade dos usuários de internet e dispositivos digitais. Posteriormente, a Lei Geral de Proteção de Dados (LGPD) complementou essa legislação, ampliando a proteção dos dados pessoais no ambiente digital.

Outra forma de furtar a identidade das vítimas ocorre através de uma ferramenta chamada deepfake, traduzindo para o portugues quer dizer imagem falsa, essa tecnica pega a imagem de qualquer pessoa,na maioria das vezes são rostos de famosos, sendo foto ou através de vídeos e utiliza a inteligência artificial para modificar o que o famoso quer dizer,conseguindo dessa maneira a sincronização dos movimentos sonoros e dos lábios deles,criando áudios falsos que a própria pessoa não sabe da existência desses áudios de maneira tão real que se você estiver distraído vc vai acabar caindo em um golpe .

Os criminosos estão utilizando bastante essa técnica, através de promoções onde a vítima fica tão tentada em ganhar o produto de graça,a

única exigência seria só pagar o frete e responder umas perguntas, nessas perguntas a vítima acaba dando todos os seus dados pessoais, sem imaginar que está sendo furtada ao adquirir esses dados pessoais da vítima os criminosos utilizam em vários locais, deixando a vítima endividada.

2.Vazamento de Dados em Empresas: Impactos e Medidas de Prevenção

O vazamento de dados em empresas tem se tornado um problema crescente e preocupante no cenário atual. Com a digitalização dos processos e a quantidade cada vez maior de informações sensíveis armazenadas eletronicamente, as organizações estão mais vulneráveis a ataques cibernéticos e falhas de segurança. Quando esses dados são expostos, as consequências podem ser graves, afetando tanto a integridade da empresa quanto a privacidade de seus clientes e colaboradores.

Uma das principais consequências do vazamento de dados é o prejuízo à imagem da empresa. Quando informações pessoais ou financeiras de clientes são comprometidas, a confiança no negócio é abalada. A percepção pública de que a organização não é capaz de proteger informações sensíveis pode levar à perda de clientes e, em casos mais graves, até à falência da empresa.

Além disso, as empresas que não conseguem evitar vazamentos podem enfrentar sanções legais. No Brasil, a Lei Geral de Proteção de Dados (LGPD) regulamenta o uso, armazenamento e compartilhamento de dados pessoais, e penaliza as empresas que não seguem essas diretrizes. As

multas por descumprimento da LGPD podem chegar a 2% do faturamento da empresa, com limite de R$ 50 milhões por infração, além de exigências para reparação de danos aos titulares dos dados.

Os prejuízos financeiros também são significativos. Além das multas, a organização pode precisar investir em auditorias, investigações internas, suporte técnico e campanhas para recuperar sua imagem. Em certos casos, é necessário fornecer serviços de proteção contra fraudes aos clientes afetados, o que aumenta ainda mais os custos operacionais.

Outro impacto relevante é o aumento do risco de fraudes e crimes digitais. Informações vazadas podem incluir dados bancários, documentos pessoais, números de cartões de crédito e até mesmo credenciais de acesso a sistemas. Esses dados podem ser usados por criminosos para realizar fraudes, roubos de identidade ou ataques direcionados, colocando em risco tanto indivíduos quanto a empresa.

Para mitigar esses riscos, as empresas precisam adotar práticas de segurança robustas. Uma das principais medidas é a implementação de sistemas de criptografia para proteger os dados em trânsito e em repouso. Além disso, a educação e treinamento de funcionários sobre segurança da informação são essenciais, uma vez que muitos vazamentos ocorrem por erros humanos ou phishing.

Outra medida importante é o uso de firewalls e sistemas de monitoramento para detectar e bloquear atividades suspeitas. A realização periódica de auditorias e testes de invasão (pentests) também é recomendada para identificar vulnerabilidades nos sistemas antes que sejam exploradas por atacantes.

Ademais, as empresas devem adotar uma política de acesso restrito, garantindo que apenas funcionários autorizados tenham acesso a

informações sensíveis. A implementação de autenticação multifator (MFA) é outra prática eficaz, pois dificulta o acesso não autorizado, mesmo que as credenciais sejam comprometidas.

Por fim, é crucial que a organização tenha um plano de resposta a incidentes. Isso inclui procedimentos para identificar rapidamente o vazamento, comunicar o problema às partes envolvidas e adotar medidas para minimizar os danos. A transparência durante a crise é fundamental para preservar a confiança dos clientes e parceiros.

Em suma, o vazamento de dados em empresas é um problema complexo que exige atenção contínua e investimentos em segurança da informação. As organizações precisam se antecipar às ameaças e garantir a proteção dos dados sob sua responsabilidade. Além de cumprir a legislação, adotar boas práticas de segurança é essencial para manter a confiança do mercado e garantir a sustentabilidade do negócio.

O vazamento de dados em empresas pode ocorrer de diversas formas, geralmente envolvendo falhas de segurança, ataques cibernéticos ou erros humanos. A seguir, estão os principais métodos utilizados pelos Ataques de hacker, também conhecido como Ciberataques, ocorre quando esses criminosos utilizam técnicas sofisticadas para invadir sistemas e roubar dados. Entre os métodos mais comuns estão:

2.1. Fraude com Cartão de Crédito

Um dos crimes mais comuns de furto de identidade ocorre por meio da clonagem de cartões de crédito. Nesse golpe, os criminosos obtêm os dados do cartão da vítima e os utilizam para realizar compras ou transações sem autorização. A coleta de informações pode ocorrer por meio de dispositivos chamados skimmers, instalados em terminais de pagamento,

ou através de sites falsos. Esse tipo de crime causa sérios danos financeiros e pode prejudicar o histórico de crédito da vítima, exigindo medidas rigorosas para restaurar sua situação financeira.

2.2. Fraude com Documentos Pessoais

O roubo de documentos pessoais, como RG, CPF e CNH, é outro método comum de furto de identidade. Com esses dados, criminosos conseguem abrir contas bancárias, solicitar empréstimos, contratar serviços e até mesmo praticar outros crimes em nome da vítima. Esse tipo de crime é especialmente preocupante porque pode levar anos para ser descoberto, além de demandar um processo longo e complicado para que a vítima prove sua inocência e recupere sua identidade.

2.3. Roubo de Identidade no Ambiente de Trabalho

Em alguns casos, os criminosos conseguem acesso a dados pessoais por meio de informações compartilhadas em ambientes de trabalho. Podem se passar por colegas ou superiores e pedir detalhes pessoais para "atualização de cadastro" ou "verificação de segurança". A vítima, confiando no ambiente, fornece os dados, que são usados para praticar fraudes. Esse tipo de roubo de identidade é uma ameaça tanto para a vítima quanto para a empresa, que pode ser responsabilizada pela segurança insuficiente dos dados de seus funcionários.

2.4. Fraude em Redes Sociais

Com o crescimento das redes sociais, os golpistas também utilizam essas plataformas para roubar informações pessoais. Por meio de perfis

falsos, eles podem enviar mensagens para coletar informações confidenciais, como CPF, endereço, ou até dados bancários, sob o pretexto de promoções ou sorteios. Outra tática é acessar as redes da vítima para obter dados compartilhados publicamente e montar um perfil detalhado. Com essas informações, eles aplicam golpes financeiros ou invadem outras contas da vítima.

2.5. Fraude por Phishing

O phishing é uma prática onde os criminosos enviam e-mails ou mensagens de texto se passando por instituições confiáveis, como bancos, empresas ou órgãos governamentais. Esses comunicados frequentemente contêm links para páginas falsas que solicitam informações pessoais ou financeiras. A vítima, acreditando na legitimidade do pedido, insere seus dados, que são roubados e usados para fraudes. Esse tipo de golpe é cada vez mais sofisticado e pode afetar pessoas de todas as idades e níveis de conhecimento tecnológico.

2.6. Roubo de Identidade para Falsificação de Benefícios

Nesse tipo de fraude, o criminoso utiliza os dados de outra pessoa para solicitar benefícios governamentais, como auxílio-desemprego, aposentadoria ou benefícios sociais. Muitas vezes, as vítimas só descobrem o roubo quando tentam solicitar um benefício legítimo e são informadas de que já há um registro em seu nome. Esse crime não só prejudica financeiramente as vítimas, mas também compromete recursos públicos destinados a quem realmente precisa.

Para proteger sua empresa contra furto de identidade, é essencial evitar práticas que possam expor dados sensíveis de colaboradores, clientes e da própria organização. Aqui estão alguns dos principais erros a serem evitados:

1. Não negligenciar a segurança de dados:

- Deixar de investir em segurança digital torna os sistemas vulneráveis. É fundamental proteger dados com firewalls, criptografia, antivírus atualizados e redes seguras.

2. Evitar o compartilhamento excessivo de dados:

- Compartilhar dados sensíveis com muitos colaboradores ou terceiros aumenta o risco de vazamento. Limite o acesso apenas a quem realmente precisa dessas informações.

3. Não deixar de treinar os colaboradores:

- Sem treinamento, os colaboradores podem ser alvos fáceis para golpes como phishing e engenharia social. Eduque a equipe para identificar e evitar ameaças, como e-mails e links suspeitos.

4. Não usar autenticação básica:

- Utilizar apenas senhas para acesso é insuficiente. Implemente autenticação multifatorial (MFA) e requisitos de senhas fortes para todos os sistemas.

5. Evitar senhas fáceis ou repetidas:

- Senhas simples ou utilizadas em múltiplas contas são mais vulneráveis a ataques. Estabeleça uma política de senhas seguras e incentive mudanças periódicas.

6. Não monitorar atividades internas:

- Ignorar o monitoramento de acessos e atividades deixa sua empresa exposta a acessos não autorizados. Monitore acessos a dados sensíveis para identificar comportamentos anômalos.

6. Não descuidar de dispositivos móveis e externos:

- Dispositivos de colaboradores, como laptops e celulares, podem ser um ponto de vulnerabilidade se não forem protegidos. Exija o uso de senhas, criptografia e políticas de acesso em dispositivos externos.

7. Não manter backups e planos de resposta a incidentes:

- A ausência de backups e de um plano de resposta a incidentes compromete a capacidade de recuperação em caso de ataques. Mantenha backups atualizados e um plano para responder rapidamente a violações de segurança.

Ao evitar esses erros e adotar uma política rigorosa de segurança de dados, você reduz significativamente o risco de sua empresa sofrer com furto de identidade.

3.Considerações Finais

Esses crimes de furto de identidade demonstram como a proteção dos dados pessoais é crucial na sociedade digital atual. Uma das leis mais recentes que o SENADO FEDERAL aprovou foi o projeto de LEI N° 1272, DE 2023 que acrescentado no Código penal decreta:

> O CONGRESSO NACIONAL decreta: Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passa a viger acrescido do seguinte art. 308-A : Adulteração maliciosa de vídeos ou áudios Art. 308-A. Adulterar arquivos de vídeo ou de áudio, mediante clonagem da voz, substituição de rosto, sincronização labial ou outra ferramenta de inteligência artificial, com a intenção de divulgar notícias falsas ou prejudicar pessoa física ou jurídica. Pena – reclusão, de dois a quatro anos, e multa.
> § 1º Na mesma pena incide quem faz uso do vídeo ou do áudio, sabendo ser adulterado, para divulgação de notícia falsa ou para prejudicar pessoa física ou jurídica, se a conduta não constituir crime mais grave.
> § 2º Se o vídeo ou o áudio é divulgado na internet, redes sociais ou outro meio análogo: Pena – reclusão, de quatro a oito anos, e multa.

Os impactos do furto de identidade são variados. Financeiramente, a vítima pode ter seu nome negativado e sofrer restrições de crédito devido a dívidas que não contraiu. Psicologicamente, a sensação de invasão e a dificuldade em resolver os problemas geram angústia e desconfiança. Além disso, o crime prejudica a economia, ao aumentar os custos de segurança e seguros para instituições financeiras e outros setores.

O combate ao furto de identidade exige uma atuação conjunta entre o poder público, as empresas e os cidadãos. O Estado precisa garantir leis e regulamentos mais rigorosos, enquanto as empresas devem investir em tecnologias de proteção e políticas de privacidade eficazes. Por outro lado, cabe ao cidadão adotar boas práticas de segurança, criando senhas fortes e diferentes nunca repetir ,verificar o endereço que você está comprando ou colocando seus dados se é verídico, não compartilhar seus dados pessoais de forma desnecessária, ter muito cuidado com os e-mails que recebem, pois a partir do momento em que você dar seus dados os criminosos conseguem de forma mais rápida enganar a vítima ela se torna mais vulnerável.Para se proteger, é recomendável não clicar em links

suspeitos, verificar a autenticidade de comunicações e usar mecanismos de segurança como autenticação em duas etapas e softwares de segurança.

Para combater o furto de identidade e os crimes associados, uma abordagem abrangente deve envolver a implementação de medidas preventivas, tecnológicas e legais, além de conscientização pública. Aqui estão algumas soluções:

3.1. Educação e Conscientização:

- Realizar campanhas para informar a população sobre os riscos do furto de identidade e sobre como se proteger, especialmente no uso de redes sociais e transações online.
- Treinar empresas para reconhecer atividades suspeitas e adotar boas práticas na proteção de dados.

3.2. Autenticação Avançada:

- Implementar autenticação multifatorial (MFA) e reconhecimento biométrico, como impressões digitais ou reconhecimento facial, dificultando o acesso de criminosos a contas e sistemas.

3.3. Monitoramento de Dados e Alertas de Fraude:

- Utilizar sistemas de monitoramento que alertam o usuário e as instituições sobre atividades suspeitas em contas bancárias ou cartões de crédito.
- Serviços de monitoramento de crédito também são úteis para que as pessoas acompanhem alterações em seu histórico financeiro.

3.4. Criptografia de Dados e Segurança de Redes:

- As empresas devem adotar criptografia para proteger dados sensíveis e garantir que apenas pessoas autorizadas tenham acesso.

- Implementação de redes seguras com firewalls, VPNs e outras barreiras que dificultem invasões cibernéticas.

3.5. Inteligência Artificial para Prevenção:

- Ferramentas de inteligência artificial e machine learning ajudam a detectar comportamentos anômalos, o que pode ser um sinal de tentativa de fraude.
- IA também pode ser usada para aprimorar sistemas de autenticação e melhorar a resposta a possíveis ataques.

3.6. Legislação e Reforço Legal:

- Revisar e fortalecer as leis de proteção de dados e identidade, como a LGPD no Brasil.
- Aumentar as penalidades para crimes de furto de identidade e assegurar que as vítimas tenham apoio legal e financeiro para resolver os danos causados.

3.7. Parcerias entre Setor Público e Privado:

- Promover parcerias entre governo e empresas de tecnologia para compartilhar informações sobre ataques e desenvolver melhores práticas de segurança.
- Criar canais de denúncia e resposta rápida que permitam bloquear e investigar crimes de identidade em tempo real.

Essas soluções abrangentes, quando adotadas em conjunto, oferecem uma abordagem sólida para reduzir a incidência de furto de identidade e proteger tanto indivíduos quanto instituições.

REFERÊNCIAS

Furto e Roubo. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/furto-e-roubo>. Acesso em: 26 out. 2024.

L12737. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 30 out. 2024.

DE DEZEMBRO DE, DE 7.; DE VÍDEOS OU ÁUDIOS., PCOC DO A. 308-A. –. AM PROJETO DE LEI N° 1272, DE 2023. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9292780&disposition=inline>. Acesso em: 31 out. 2024.

LUGARINHO, H. Roubo de Dados Pessoais Pela Internet: a Empresa Pode ser Responsabilizada? Disponível em: <https://clickcompliance.com/roubo-de-dados-pessoais-pela-internet-a-empresa-pode-ser-responsabilizada/>. Acesso em: 1 nov. 2024.