Fraudes Eletrônicas e o Contexto da Revolução Digital no Sistema Financeiro

Sumário

Módulo 1: Introdução

Falar sobre fraudes eletrônicas exige voltar a 2020, quando a pandemia de COVID-19 provocou uma transformação profunda em diversas áreas da vida cotidiana. O setor financeiro foi diretamente impactado: a necessidade de distanciamento social acelerou de forma inédita a digitalização dos serviços bancários. Esse movimento não apenas facilitou o acesso de milhões de brasileiros ao sistema financeiro, mas também impulsionou mudanças na agenda regulatória do Banco Central do Brasil (Bacen).

Antes desse período, muitos brasileiros enfrentavam barreiras para acessar serviços bancários. A ausência de infraestrutura em regiões remotas, a burocracia para abertura de contas e a dependência de atendimento presencial limitavam o alcance das instituições financeiras tradicionais. Com a pandemia, a migração para canais digitais tornou-se inevitável, levando bancos, fintechs e outros atores do setor a ampliar rapidamente suas soluções online.

Nesse cenário, recursos como aplicativos de pagamento, internet banking e transferências instantâneas se popularizaram. O destaque ficou para o PIX, lançado pelo Bacen em novembro de 2020, que se consolidou como um marco na inclusão financeira. De acordo com dados oficiais, o sistema adicionou 71,5 milhões de usuários ao sistema bancário, permitindo que pessoas antes excluídas passassem a realizar operações de forma simples e rápida pelo celular. Essa digitalização acelerou a bancarização e tornou o acesso a serviços financeiros mais democrático.

Ao mesmo tempo, o avanço tecnológico impulsionou o conceito de Embedded Finance ou Finanças Incorporadas — a oferta de serviços financeiros dentro de plataformas e aplicativos que não pertencem ao setor bancário tradicional.

Empresas de varejo, mobilidade urbana e e-commerce passaram a oferecer cartões, pagamentos via PIX, recargas, empréstimos e até seguros, integrados diretamente à sua operação principal. Embora essa tendência exista desde 2013[1], foi durante a pandemia que ganhou tração, apoiada pelo crescimento do uso de canais digitais, que hoje representam 79% das transações no país, segundo pesquisa da Deloitte para a Febraban[2].

---

[1] A Lei nº 12.865/2013, conhecida como "Lei dos Meios de Pagamento", impulsionou a oferta de serviços financeiros a empresas não financeiras, integrando este tipo de serviços aos seus produtos.
[2] Deloitte Touche Tohmatsu Limited - Pesquisa FEBRABAN de Tecnologia Bancária - 32ª edição, 2º vol., p. 06.

Com essa transformação, o celular tornou-se o principal canal para operações bancárias: 7 em cada 10 transações já são realizadas pelo dispositivo.

No entanto, o ambiente virtual também se tornou terreno fértil para a atuação de criminosos. Golpes e fraudes que antes ocorriam de forma presencial, como o estelionato ou o golpe do "bilhete premiado", migraram para o meio digital.

Hoje, criminosos exploram vulnerabilidades tecnológicas e comportamentais, utilizando-se de engenharia social para enganar vítimas e se esconder atrás da aparente impunidade proporcionada pelo anonimato online.

O aumento das fraudes eletrônicas no Brasil é, portanto, um reflexo direto da digitalização do sistema financeiro. Embora o Banco Central e outras entidades reguladoras invistam constantemente em segurança e inovação tecnológica, a prevenção depende também da conscientização dos usuários.

Conhecer as principais ameaças e as estratégias utilizadas por fraudadores é fundamental para proteger não apenas o patrimônio individual, mas também a integridade e a estabilidade de todo o sistema financeiro nacional.

Módulo 2. Engenharia Social: A Porta de Entrada das Fraudes

Capítulo 2.1 O que é a Engenharia Social?

A engenharia social é um dos principais vetores de ataque utilizados por criminosos no sistema financeiro digital. Traduz-se na prática de obter "acesso a determinadas informações privilegiadas, por meio de técnica de persuasão"[3]. Esta técnica baseia-se na exploração dos comportamentos dos indivíduos, em vez de atacar diretamente a tecnologia. Ela é muito utilizada pelos estelionatários, que fazem uso de manipulação psicológica para induzir indivíduos a revelar informações confidenciais[4].

Conceitualmente, a engenharia social é o ato de manipular pessoas para que elas entreguem informações confidenciais, realizem transferências ou tomem atitudes que comprometem a segurança da informação, muitas vezes sem perceber que estão sendo enganadas.

---

[3] ZANIOLO, Pedro Augusto Fernando. Crimes Modernos: o impacto da tecnologia no Direito. Ed. Juspodivm. p. 248.
[4] MANN, Ian. Engenharia Social. São Paulo: Blücher, 2011.

Capítulo 2.2 Características principais e técnicas utilizadas:

Os criminosos utilizam um conjunto de técnicas para manipular psicologicamente os indivíduos, induzindo-os a divulgar informações confidenciais, fornecer acesso não autorizado ou realizar ações que comprometam a segurança de sistemas e dados.

Diferente de ataques puramente técnicos, a engenharia social explora vulnerabilidades humanas, como confiança, curiosidade, medo ou senso de urgência. Kevin D. Mitnick, um dos mais conhecidos especialistas em segurança da informação e ex-hacker, define: "A engenharia social é a arte de explorar a tendência natural das pessoas de confiar"[5]. É possível também, por meio das poucas informações que ele tem acesso, montar um plano sobre o alvo e com informações que ele acha relevantes, dão ao criminoso a possibilidade de prejudicá-lo empresarial, social, financeira ou psicologicamente.

Segundo Hadnagy, a engenharia social combina princípios de psicologia, comunicação e persuasão para criar cenários convincentes capazes de enganar até usuários experientes. Essa abordagem pode ocorrer de diversas formas, como phishing ou vishing, sendo particularmente perigosa por contornar barreiras tecnológicas e focar no elo mais fraco da segurança: o ser humano. Como destaca o autor, "A segurança da informação é tão forte quanto a pessoa menos treinada da organização"[6].

Os criminosos cibernéticos usam um conjunto de técnicas manipulativas para enganar indivíduos e obter acesso não autorizado a informações sensíveis. Ao invés de explorar falhas tecnológicas, os criminosos utilizam táticas de persuasão e engano para convencer as vítimas a entregar dados sensíveis, como dados bancários, senhas ou outros dados pessoais.

As fraudes de engenharia social têm um impacto significativo na segurança financeira de indivíduos e empresas. Já para o consumidor final, o risco de perder uma quantia significativa de dinheiro, dados pessoais ou mesmo ter sua identidade roubada é uma preocupação crescente.

O engenheiro social que utiliza esta técnica para fins criminosos, pode ser definido como uma pessoa que pode utilizar um conjunto de técnicas para a manipulação da confiança de outras pessoas para ter acesso às infor-

[5] MITNICK, Kevin D.; SIMOM, William L. A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Pearson Education, São Paulo: 2003.
[6] Hadnagy, Christopher. Social Engineering: The Science of Human Hacking, 2018.

mações privadas. É possível também, por meio das poucas informações que ele tem acesso, montar um plano sobre o alvo e com informações que ele acha relevantes, dão ao criminoso a possibilidade de prejudicar o alvo, social, financeira ou psicologicamente.

Em resumo, as principais características são:

- O ataque parece legítimo e confiável.
- Explora autoridade, empatia ou pânico.
- Ocorre por meios digitais ou presenciais: e-mails, telefonemas, redes sociais, mensagens de texto, etc.

Capítulo 2.3 Por que a Engenharia Social é tão eficaz?

A engenharia social é extremamente eficaz porque apresenta baixo custo e alta eficiência na execução. Diferentemente de ataques cibernéticos que exigem infraestrutura tecnológica avançada, softwares maliciosos complexos ou invasões diretas a sistemas, as técnicas de engenharia social podem ser aplicadas apenas com planejamento, criatividade e habilidades de comunicação.

Essa simplicidade reduz a barreira de entrada para criminosos e permite que mesmo indivíduos com conhecimento técnico limitado realizem ataques bem-sucedidos.

Outro fator que contribui para sua eficácia é a dificuldade de detecção por sistemas automáticos. Ferramentas como antivírus, firewalls e sistemas de monitoramento são projetadas para identificar atividades suspeitas no tráfego de rede ou no comportamento de programas. No entanto, quando o próprio usuário legítimo é induzido a fornecer informações, clicar em links maliciosos ou executar ações inseguras, a atividade aparenta ser legítima para as ferramentas de segurança, dificultando a identificação e a resposta imediata.

A velocidade de execução é outro elemento que torna a engenharia social tão perigosa. Muitos ataques são concluídos em questão de minutos, desde o primeiro contato até a obtenção de dados sensíveis ou acesso ao sistema. Essa rapidez reduz o tempo de reação das equipes de segurança e aumenta as chances de sucesso do criminoso.

Além disso, a abordagem pode ser altamente personalizada, aproveitando informações públicas sobre a vítima para criar mensagens e interações convincentes, o que eleva a taxa de conversão do ataque.

Por fim, a engenharia social explora falhas humanas e emocionais, e não falhas técnicas. Emoções como medo, urgência, curiosidade ou excesso

de confiança podem levar as pessoas a ignorar protocolos de segurança e agir impulsivamente.

Essa exploração psicológica contorna barreiras tecnológicas e aproveita o que muitos especialistas consideram o elo mais fraco da cadeia de segurança: o comportamento humano. Por isso, a conscientização e o treinamento contínuo dos usuários são considerados tão ou mais importantes do que as defesas tecnológicas na prevenção desse tipo de ameaça.

Módulo 3: Principais Tipos de Fraudes Eletrônicas Atuais

Capítulo 3.1 Phishing

Phishing é um tipo de fraude onde o golpista se passa por uma empresa legítima (como bancos ou fintechs) para enganar a vítima e coletar dados sensíveis, como senhas, tokens e informações bancárias.

É uma das fraudes eletrônicas mais comuns e consiste em enganar a vítima para que forneça informações pessoais e confidenciais, como senhas, números de cartões de crédito, CPF ou dados bancários. Normalmente, o criminoso envia um e-mail ou mensagem de texto se passando por uma instituição financeira ou empresa conhecida, solicitando que a vítima clique em um link e insira suas informações em um site falso que imita a página original.

Diariamente, a maioria das pessoas recebem este tipo de tentativa de fraude, por e-mail, informando ter ocorrido um problema em seus acessos ou contas e solicita que o cliente clique em um link para confirmar sua identidade. Ao clicar, o usuário é redirecionado a um site fraudulento, onde insere suas credenciais bancárias, que são então capturadas pelo criminoso.

> **Exemplo:**
> No Brasil, é comum o uso de e-mails falsos de supostos bancos informando que “a conta foi bloqueada” e solicitando que o usuário clique em um link para “reativar o acesso”. Outro exemplo recorrente envolve mensagens de grandes varejistas ou empresas de entrega, com informações sobre “pedidos” ou “faturas” que, na verdade, direcionam para páginas falsas. Esses sites são cuidadosamente construídos para imitar o visual da instituição verdadeira, o que aumenta a credibilidade da fraude e a probabilidade de sucesso.

Para detectar e prevenir o phishing, é fundamental adotar uma postura de verificação constante: analisar o endereço de e-mail do remetente, verificar a URL de links antes de clicar, desconfiar de mensagens com erros

gramaticais e não abrir anexos de origem duvidosa.
Organizações devem utilizar filtros de spam robustos, autenticação multifator (MFA) e realizar treinamentos de conscientização periódicos para funcionários. No ambiente doméstico, manter softwares e navegadores atualizados também reduz a exposição a esse tipo de ataque.

Capítulo 3.2 Spear Phishing

O spear phishing é uma versão mais direcionada e sofisticada do phishing. Nesse tipo de ataque, o criminoso investe tempo na coleta de informações específicas sobre a vítima — como nome, cargo, empresa em que trabalha, histórico profissional e contatos pessoais — para criar uma mensagem personalizada e altamente convincente.

Esse nível de personalização reduz as chances de que a vítima perceba a fraude, já que a comunicação aparenta vir de uma fonte confiável e está alinhada ao contexto real da vítima.

Exemplo:
Um caso real de spear phishing registrado em novembro de 2024 ilustra bem a sofisticação dessas fraudes. Os invasores exploraram a plataforma DocuSign para criar e enviar faturas falsas que imitavam documentos legítimos de marcas amplamente reconhecidas, como Norton e PayPal. Por utilizarem a própria infraestrutura e os domínios autênticos da DocuSign, os criminosos conseguiram contornar os filtros tradicionais de segurança de e-mail, fazendo com que as mensagens passassem por legítimas aos olhos das vítimas e dos sistemas automatizados. Ao receber as faturas, muitas pessoas foram induzidas a autorizar pagamentos indevidos, acreditando estar quitando obrigações reais. Esse caso evidencia como, ao combinar engenharia social com o uso indevido de serviços legítimos, os golpistas aumentam consideravelmente suas chances de sucesso e dificultam a detecção por ferramentas de segurança.[7]

Para prevenir o spear phishing, empresas devem adotar políticas rígidas para validação de solicitações financeiras, como a dupla checagem com outro colaborador ou por meio de um canal oficial independente do e-mail. É essencial limitar a exposição de informações sensíveis em redes sociais e aplicar autenticação multifator em contas de e-mail.

A detecção passa pela atenção a sinais sutis: endereços de e-mail levemente diferentes, mudanças no tom de comunicação habitual e solicitações incomuns ou fora do procedimento padrão.

[7] Fonte: Cyber Material, apud Keepnet Labs, 2024 https://cybermaterial.com/docusign--api-exploited-for-fake-invoice-scam

Capítulo 3.3 Smishing

O smishing é a variação do phishing que ocorre por meio de mensagens SMS ou aplicativos de mensagens instantâneas, como WhatsApp e Telegram. A técnica consiste em enviar textos que contêm links maliciosos ou instruções para fornecer dados pessoais diretamente na conversa.

Por serem recebidas no dispositivo móvel e, muitas vezes, acompanhadas de notificações urgentes, essas mensagens tendem a gerar uma resposta mais rápida e menos cautelosa por parte da vítima.

> **Exemplo:**
> No Brasil, um dos exemplos mais comuns é o golpe que simula mensagens de empresas de logística informando sobre uma "tentativa de entrega frustrada". A vítima é instruída a clicar em um link para reagendar a entrega, sendo direcionada a uma página falsa para inserir informações pessoais ou realizar um pagamento de "taxa de liberação". Outro exemplo frequente envolve mensagens de promoções falsas, supostamente enviadas por redes varejistas, oferecendo descontos "por tempo limitado" mediante cadastro.

Para detectar smishing, é importante desconfiar de mensagens não solicitadas, especialmente as que solicitam informações sigilosas ou pagamentos urgentes.

A prevenção inclui evitar clicar em links de remetentes desconhecidos, confirmar diretamente com a empresa a veracidade da comunicação e utilizar recursos de bloqueio de remetentes suspeitos. As operadoras de telefonia e aplicativos de mensagens também oferecem mecanismos para denunciar e filtrar conteúdo malicioso, que devem ser utilizados sempre que possível.

Capítulo 3.4 Vishing

O vishing, ou voice phishing, é a prática de enganar vítimas por meio de ligações telefônicas. Criminosos se passam por representantes de empresas, bancos ou órgãos governamentais para obter informações pessoais ou persuadir a vítima a realizar ações que comprometam sua segurança financeira.

Em muitos casos, os golpistas utilizam tecnologias de caller ID spoofing[8], que fazem com que o número exibido no visor seja o mesmo da instituição verdadeira, aumentando a credibilidade da ligação.

[8] Uso de informações falsas de identificador de chamadas para disfarçar a verdadeira origem de uma chamada recebida.

Exemplo:
Um exemplo recorrente é a ligação informando sobre "transações suspeitas" no cartão de crédito. O suposto atendente orienta a vítima a transferir o saldo para uma "conta segura" ou a fornecer códigos recebidos por SMS para "bloquear a transação". Há também casos em que os criminosos se passam por técnicos de suporte, alegando necessidade de "atualização urgente" no sistema, induzindo a instalação de softwares que permitem acesso remoto ao computador ou celular da vítima.

A detecção do vishing exige atenção a comportamentos incomuns durante a ligação: pressão para agir rapidamente, pedidos de informações sensíveis ou instruções para ignorar procedimentos de segurança oficiais.

A prevenção passa por nunca fornecer senhas, códigos de autenticação ou dados bancários por telefone, desligar a chamada em caso de dúvida e retornar por meio dos canais oficiais da instituição. Treinamentos de conscientização e divulgação de campanhas de alerta por parte das empresas também são fundamentais para reduzir a eficácia desse tipo de ataque.

Tipo de ataque	Conceito	Exemplo no Brasil	Como detectar	Como prevenir
Pishing	Golpe em massa por e-mail, no qual criminosos se passam por instituições legítimas para obter dados pessoais, financeiros ou instalar malware.	E-mails falsos de bancos informando sobre "bloqueio de conta" e solicitando clique em link para "reativar acesso"	Verificar remetente e domínio; observar erros de gramática; inspecionar URL antes de clicar	Usar filtros de spam; habilitar autenticação multifator (MFA); treinar usuários para identificar mensagens suspeitas.
Spear Pishing	Versão direcionada do phishing, altamente personalizada com base em informações coletadas sobre a vítima.	E-mail falso enviado ao setor financeiro de empresa, se passando pelo CEO, solicitando transferência urgente.	Desconfiar de pedidos fora do padrão; confirmar solicitações sensíveis por outro canal; verificar detalhes no endereço de e-mail.	Implementar dupla checagem para transações; limitar exposição de dados corporativos; usar MFA.

Tipo de ataque	Conceito	Exemplo no Brasil	Como detectar	Como prevenir
Smishing	Golpe via SMS ou aplicativos de mensagens, com links ou instruções para obter dados diretamente.	Mensagem de "entrega frustrada" solicitando pagamento de taxa via link.	Suspeitar de mensagens urgentes e não solicitadas; verificar origem antes de clicar.	Não clicar em links de remetentes desconhecidos; confirmar diretamente com a empresa; usar bloqueio de contatos suspeitos.
Vishing	Golpe por telefone, usando persuasão e, muitas vezes, spoofing para simular número real da instituição.	Ligação informando sobre "transação suspeita" e solicitando transferência para "conta segura".	Desconfiar de pressão para agir rápido; identificar pedidos de informações sigilosas	Nunca fornecer dados ou códigos por telefone; desligar e ligar para canal oficial; promover campanhas de alerta.

Capítulo 3.5 Spoofing

O termo spoofing refere-se a um conjunto de técnicas utilizadas por criminosos para falsificar informações de identificação, de forma a fazer com que uma comunicação ou transação pareça originar-se de uma fonte confiável. O termo vem do inglês to spoof, que significa enganar, fingir ou simular falsamente.

Essa falsificação pode ocorrer em diferentes camadas e formatos — como endereço de e-mail (email spoofing), número de telefone (caller ID spoofing), endereço IP (IP spoofing) ou mesmo em sites (URL spoofing).

O objetivo é enganar o destinatário ou o sistema de segurança, induzindo a execução de ações que favoreçam o fraudador, como clicar em links maliciosos, fornecer credenciais ou autorizar operações financeiras. No contexto do sistema financeiro, o spoofing é frequentemente usado em conjunto com técnicas de phishing ou vishing, aumentando a credibilidade do golpe

Exemplos práticos:

- No Brasil, casos de caller ID spoofing têm se tornado comuns: o criminoso liga para a vítima e o número exibido no visor do celular é o mesmo do banco ou de outra instituição legítima. Durante a chamada, o golpista informa sobre uma suposta "transação

suspeita" e orienta a vítima a seguir instruções para "proteger a conta", que na verdade resultam na transferência de valores ou no fornecimento de códigos de autenticação.
- Outro exemplo envolve email spoofing, no qual o endereço exibido parece ser o oficial de uma empresa ou fornecedor, solicitando pagamento de faturas ou atualização de dados. Em ambientes corporativos, esse tipo de fraude é usado para viabilizar ataques de Business Email Compromise (BEC), causando prejuízos significativos.

Detectar o golpe do spoofing pode ser desafiador, já que a falsificação é projetada para passar despercebida. No caso de e-mails, sinais de alerta incluem erros sutis no endereço do remetente (como troca de caracteres semelhantes), divergência entre o nome exibido e o domínio real e links que, ao serem inspecionados, direcionam para domínios estranhos.

Em ligações telefônicas, o simples fato de o número parecer legítimo não garante autenticidade — especialmente se houver pressão para agir rapidamente. Ferramentas de análise de cabeçalhos de e-mails, logs de rede e autenticação podem ajudar na identificação de falsificações.

Para o usuário final, a prevenção contra spoofing começa pela postura crítica diante de qualquer solicitação sensível. É essencial nunca fornecer senhas, códigos de verificação ou dados bancários por e-mail ou telefone, independentemente de quem esteja solicitando.

Sempre que possível, confirmar a solicitação por meio de um canal oficial distinto do utilizado para o contato — por exemplo, ligando para o número oficial do banco ou acessando diretamente o site da instituição. No caso de e-mails, verificar o endereço completo do remetente e passar o mouse sobre links antes de clicar ajuda a identificar tentativas de fraude.

Capítulo 3.6 Ransomware

O ransomware é um tipo de software malicioso projetado para bloquear o acesso a sistemas, arquivos ou dados até que um resgate seja pago ao atacante. Essa modalidade de ataque se diferencia por seu impacto direto e potencialmente devastador: a criptografia dos arquivos impede que sejam utilizados, e, muitas vezes, as vítimas recebem um prazo para efetuar o pagamento, sob ameaça de perda permanente dos dados ou divulgação de informações sigilosas.

Os criminosos geralmente exigem o pagamento em criptomoedas, como Bitcoin, devido à dificuldade de rastreamento das transações. Esse tipo de ameaça evoluiu significativamente nos últimos anos, passando de ataques oportunistas contra usuários individuais para campanhas direcionadas contra empresas, órgãos públicos e até hospitais, visando maximizar os lucros.

Um exemplo notório é o ataque WannaCry, ocorrido em 2017, que explorou uma vulnerabilidade no sistema Windows para se espalhar rapidamente pelo mundo, afetando mais de 200 mil computadores em 150 países.

Mais recentemente, surgiram modalidades conhecidas como double extortion (dupla extorsão), nas quais, além de criptografar os dados, os criminosos também os exfiltram (ato deliberado de roubo ou extração de informações confidenciais de um sistema ou rede de computadores) e ameaçam divulgá-los caso o resgate não seja pago.

Empresas de todos os portes, prefeituras, escolas e serviços essenciais já foram alvos, evidenciando que nenhuma organização está imune. No Brasil, incidentes desse tipo já causaram paralisação de serviços públicos e prejuízos milionários em companhias privadas.

A detecção de ransomware pode ser desafiadora, mas existem sinais que ajudam a identificá-lo precocemente. Um aumento repentino e anormal no uso de CPU ou disco, arquivos com extensões desconhecidas ou recentemente alteradas e mensagens de resgate exibidas na tela são indícios claros de infecção. Sistemas de detecção e resposta a ameaças, bem como soluções de antivírus de nova geração, conseguem identificar comportamentos típicos de ransomware, como a rápida criptografia de múltiplos arquivos, bloqueando o processo antes que ele se espalhe por toda a rede. Monitorar logs e atividades suspeitas em servidores também é fundamental para detectar a ameaça antes que cause danos irreversíveis.

Para prevenir ataques de ransomware, as boas práticas de segurança incluem manter todos os sistemas e softwares sempre atualizados, utilizar soluções de backup robustas — preferencialmente com cópias armazenadas de forma offline ou em locais isolados.

Treinar usuários para identificar e evitar abrir anexos ou links suspeitos é igualmente importante, pois muitos ataques começam por meio de phishing. Implementar a autenticação multifator (MFA), segmentar redes e limitar privilégios de acesso também reduz a superfície de ataque e minimiza o impacto de uma eventual infecção.

Por fim, é fundamental que empresas e instituições desenvolvam e testem regularmente um plano de resposta a incidentes específico para ransomware. Isso inclui definir papéis e responsabilidades, manter canais seguros de comunicação interna, e ter um procedimento claro para restaurar dados a partir de backups confiáveis.

É importante destacar que pagar o resgate não garante a recuperação dos dados, e ainda incentiva os criminosos a continuarem atuando. Em vez disso, investir em prevenção, monitoramento e resiliência operacional é a estratégia mais eficaz para mitigar os riscos dessa ameaça crescente no cenário digital.

Capítulo 3.7 Deepfake

É uma técnica de inteligência artificial (IA) que usa redes neurais e aprendizado de máquina *(machine learning)* para criar ou manipular imagens, vídeos e áudios.

Embora a tecnologia tenha aplicações legítimas, como no cinema, publicidade e acessibilidade, ela também é utilizada para fins maliciosos, como fraudes, desinformação e manipulação de opinião pública, tornando-os extremamente realistas e difíceis de distinguir da realidade. A tecnologia pode substituir ou modificar rostos e vozes de pessoas, fazendo com que elas digam ou façam coisas que nunca ocorreram. Existem dois tipos principais de deepfake:

- **Deepfake de vídeo:** altera imagens para que uma pessoa pareça dizer ou fazer algo que nunca fez, com movimentos faciais, expressões e sincronização labial muito próximos da realidade. Pode ser usado para criar vídeos falsos de celebridades, políticos, ou até mesmo de pessoas comuns.
- **Deepfake de áudio:** Utiliza a voz de uma pessoa para criar frases ou declarações que ela nunca disse. Isso é feito a partir da análise de gravações de voz, o que permite que a IA “aprenda” os padrões de fala e os reproduza de maneira convincente.

No contexto de fraudes pode simular, por exemplo:
- Um CEO pedindo uma transferência urgente via vídeo;
- Um diretor falando por telefone com uma voz clonada;
- Um vídeo falso de denúncia interna para prejudicar reputações;
- Um áudio adulterado usado como “prova” de assédio ou corrupção.

A detecção de deepfakes, tanto em vídeo quanto em áudio, envolve uma combinação de análise manual e ferramentas automatizadas.

No vídeo, sinais de manipulação podem incluir piscadas de olhos pouco naturais, iluminação incoerente, bordas imprecisas em torno do rosto ou movimentos labiais levemente dessincronizados com o áudio.

No áudio, anomalias como pausas artificiais, ausência de ruídos naturais de fundo, entonação estranhamente uniforme ou cortes abruptos podem indicar falsificação. Ferramentas baseadas em IA, como detectores forenses digitais, conseguem analisar padrões espectrais, artefatos de compressão e inconsistências temporais para identificar sinais de edição.

> **Exemplo: Caso 2024 — Multinacional em Hong Kong**
> Um funcionário participou de uma videoconferência em que acreditava estar com seu CFO e outros diretores. Todos eram deepfakes gerados a partir de imagens e vozes obtidas em redes sociais e vídeos institucionais. O "CFO" ordenou transferências urgentes para contas no exterior. O prejuízo foi de cerca de US$ 25 milhões.[9]

Para prevenir golpes com deepfakes, é essencial adotar práticas de verificação de autenticidade. No caso de vídeos, confirmar a origem do conteúdo, buscar versões originais em fontes confiáveis e cruzar informações com outras mídias é fundamental. Para áudios, especialmente os recebidos por canais não oficiais, recomenda-se confirmar a solicitação por outro meio, preferencialmente por canais previamente autenticados. Empresas podem implementar códigos ou palavras-chave internas para validar instruções sensíveis, reduzindo o risco de engano. Além disso, capacitar equipes e cidadãos para reconhecer sinais de falsificação é uma medida de defesa crucial.

Por fim, organizações devem considerar a integração de soluções de detecção de deepfakes em seus fluxos de segurança, especialmente em setores vulneráveis, como financeiro, governamental e de mídia. Tecnologias emergentes, como marcas d'água digitais, blockchain para registro de mídia original e metadados imutáveis, estão sendo desenvolvidas para autenticar conteúdo desde sua criação. Contudo, como a evolução dos deepfakes é rápida e contínua, a prevenção depende de uma abordagem proativa, combinando tecnologia, processos internos e uma cultura de ceticismo saudável diante de conteúdos sensíveis.

---

[9] Disponível em: https://www.cnnbrasil.com.br/internacional/funcionario-de-multinacional-paga-us-25-mi-a-golpista-que-usou-deepfake-para-simular-reuniao/#goog_rewarded e Veja vídeo do CIO da Arup: https://www.weforum.org/videos/arup-deepfake-fraud

Módulo 4. Como identificar ameaças e antecipar os riscos

Capítulo 4.1 Monitoramento reputacional e resposta a incidentes

Monitoramento reputacional é o processo contínuo de rastrear e analisar menções, comentários e informações relacionadas a uma organização, seus produtos, serviços e líderes em diversos canais — incluindo redes sociais, sites de notícias, fóruns, blogs e bases de dados públicas.

No contexto de Compliance e gestão de riscos, essa prática é fundamental para identificar ameaças potenciais à imagem corporativa e antecipar crises. As ferramentas de monitoramento podem usar técnicas de social listening e busca avançada em fontes abertas (OSINT - Open Source Intelligence[10]) para detectar indícios de problemas, como reclamações recorrentes, acusações de conduta antiética ou associações com pessoas e entidades de risco.

O objetivo é criar um radar preventivo que permita à empresa agir antes que um incidente de reputação se amplifique.

Um exemplo prático de monitoramento reputacional ocorre quando uma instituição financeira acompanha menções ao seu nome e executivos-chave em plataformas como Twitter/X, LinkedIn e Reclame Aqui. Se um cliente insatisfeito publica um vídeo com críticas que viraliza rapidamente, a equipe de monitoramento consegue identificar o conteúdo em tempo real e acionar o protocolo de resposta antes que a situação ganhe proporções incontroláveis.

Esse tipo de vigilância também pode detectar fake news, deepfakes e campanhas de desinformação que afetam a confiança do mercado, permitindo que a comunicação institucional e o jurídico ajam de forma coordenada.

É importante a Instituição ter um Plano de resposta a incidentes reputacionais, que se traduz em um conjunto de ações estruturadas para mitigar danos quando uma ameaça à imagem da organização já foi detectada.

[10] É o trabalho de coletar informações que já estão disponíveis publicamente — na internet, jornais, redes sociais, registros públicos — e usar essas informações para montar um "quebra-cabeça" sobre uma pessoa, empresa ou situação. É como fazer uma investigação usando só "pistas abertas", sem precisar invadir nada. Exemplo: se alguém vê seu perfil no LinkedIn, cruza com fotos no Instagram e dados que você publicou em fóruns, já está fazendo OSINT — e pode usar isso para conhecer seus hábitos, onde você trabalha, horários, gostos e até prever seu comportamento.

Envolve avaliação rápida da gravidade do evento, definição de mensagens-chave, seleção de porta-vozes, comunicação proativa com stakeholders e, quando necessário, ações corretivas.

> **Exemplo:**
> Se um ataque cibernético resulta no vazamento de dados de clientes, a resposta deve incluir esclarecimentos claros, medidas técnicas para conter o incidente, canais de atendimento reforçados e cooperação com autoridades competentes. A agilidade e a transparência são determinantes para reduzir o impacto negativo e restaurar a credibilidade.

Detectar incidentes de reputação exige integração de múltiplas fontes de informação e uso de tecnologias que permitam correlacionar dados. Ferramentas de monitoramento de mídia, alertas de menções em tempo real, análise de tendências e integração com sistemas de threat intelligence podem indicar anomalias no volume ou no tom das menções à marca.

Além disso, a análise qualitativa por profissionais de comunicação e compliance é indispensável para interpretar corretamente o contexto e evitar falsas alarmes. É igualmente importante ter indicadores-chave (KPIs) para medir o risco reputacional, como variação de sentimento e alcance de publicações negativas.

Tenha um plano de resposta a incidentes de reputação, alinhado com a equipe de compliance, jurídica, comunicação e TI prontos para:

- Identificar o ocorrido;
- Retirar o conteúdo do ar ou solicitar o takedown do site falso;
- Reportar a autoridades competentes, para resguardo dos direitos e preservar a cadeia de custódia
- Realizar uma Comunicação ao Público e alertar sobre o Golpe, deixando claro que a Instituição é igualmente vítima e não coaduna com a prática da fraude.

As boas práticas de prevenção e resposta incluem:

- Estabelecer políticas claras de comunicação em crises;
- Treinar porta-vozes e equipes de atendimento para lidar com situações de alta pressão;
- Manter um plano de resposta a incidentes reputacionais atualizado;
- Investir em tecnologia de monitoramento multicanal; e,
- Sobretudo, cultivar uma cultura organizacional que priorize ética, transparência e qualidade na entrega de produtos e serviços.

A prevenção começa muito antes da crise: empresas que constroem relacionamentos sólidos com clientes, parceiros, imprensa e comunidade tendem a enfrentar incidentes com maior resiliência e capacidade de recuperação.

Capítulo 4.2 Adoção de Tecnologias de Segurança Cibernética Avançadas no Combate a Fraudes Eletrônicas

Com a expansão acelerada da digitalização de serviços e do uso massivo da internet, as fraudes eletrônicas tornaram-se uma ameaça constante para o setor financeiro, o comércio eletrônico e diversas indústrias conectadas. A sofisticação e a velocidade desses ataques exigem que organizações públicas e privadas adotem soluções de segurança cibernética de última geração, capazes de prevenir, identificar e neutralizar atividades maliciosas. Nesse cenário, a adoção de tecnologias avançadas é um dos pilares fundamentais para enfrentar a crescente complexidade das fraudes digitais.

Entre essas tecnologias, a Inteligência Artificial (IA) e o Machine Learning (ML) se destacam como ferramentas indispensáveis. Elas possibilitam a análise de grandes volumes de dados em tempo real, reconhecendo padrões de comportamento suspeitos e sinalizando transações fora do perfil habitual. A capacidade de aprendizado contínuo dessas soluções permite que se adaptem a novas técnicas de fraude, tornando-se mais eficientes a cada interação. Como exemplo prático, sistemas de monitoramento de transações financeiras já conseguem bloquear operações suspeitas ou notificar equipes de segurança antes que prejuízos significativos ocorram.

Outra barreira importante contra fraudes digitais é a Autenticação Multifatorial (MFA), que fortalece o controle de acesso a contas e sistemas. Ao exigir mais de uma credencial de verificação — como senha, código enviado por SMS ou token gerado por aplicativo — a MFA aumenta substancialmente a dificuldade para que criminosos obtenham acesso não autorizado. Esse método cria uma camada adicional de proteção, pois exige que o fraudador tenha não apenas o conhecimento da senha, mas também posse de outro fator legítimo, reduzindo a eficácia de ataques baseados apenas em roubo de credenciais.

A análise comportamental (Behavioral Analytics) surge como mais uma estratégia eficaz de defesa. Essa tecnologia monitora padrões de navegação e interação dos usuários em tempo real, comparando-os com o comportamento usual. Alterações bruscas, como login em horários incomuns, acesso a partir de locais geográficos distantes ou movimentações financeiras atípicas, podem ser imediatamente sinalizadas como riscos. Esse tipo de análise não substitui os métodos de autenticação tradicionais, mas atua

como uma camada complementar que amplia a precisão na detecção de tentativas de fraude.

O Blockchain e a criptografia avançada também assumem papel relevante no combate a fraudes. Por sua natureza descentralizada e imutável, o Blockchain garante a integridade de registros e transações, dificultando a manipulação de informações financeiras. Além disso, possibilita o rastreamento confiável de todas as operações realizadas, criando um ambiente de maior transparência. Paralelamente, técnicas de criptografia robustas asseguram que dados confidenciais, como informações pessoais e bancárias, permaneçam protegidos durante a transmissão, reduzindo a exposição a ataques de interceptação ou roubo.

Por fim, a proteção contra phishing e malware permanecem como prioridade, já que essas práticas ainda figuram entre os ataques mais recorrentes. Soluções modernas incluem filtros avançados capazes de identificar links e anexos maliciosos antes que cheguem ao usuário, prevenindo o engajamento em golpes. A combinação de tecnologias como IA, MFA, Blockchain e análise comportamental forma um ecossistema de defesa sólido contra fraudes eletrônicas. Entretanto, nenhuma dessas soluções substitui a importância da educação contínua dos usuários e da colaboração entre empresas, consumidores e órgãos reguladores. A soma de tecnologia e conscientização é a estratégia mais eficaz para reduzir riscos e preservar a confiança no ambiente digital.

Módulo 5. Planos de Ação para Prevenção de Fraudes

A prevenção de fraudes exige uma abordagem integrada que una governança sólida, uso de tecnologia de ponta e treinamento contínuo das equipes.

Um plano eficaz precisa considerar não apenas o cumprimento regulatório, mas também a proteção do cliente, a preservação da reputação e a redução de riscos operacionais. Vamos explorar os principais planos de ação que as Instituições Financeiras e outras organizações do setor podem adotar, baseados em dados e práticas validadas por pesquisas e estatísticas confiáveis.

Capítulo 5.1 Fortalecimento da Governança e Cultura de Compliance

Uma cultura organizacional forte em governança e compliance é o alicerce da prevenção de fraudes. Em bancos, isso significa engajamento total da alta gestão, clareza nas políticas e incentivo a práticas éticas em todos os níveis hierárquicos.

Ações Recomendadas:

- Elaborar um código de ética claro, com diretrizes específicas sobre identificação e reporte de atividades suspeitas.
- Aplicar políticas rígidas de compliance, com controles internos alinhados às normas do Banco Central, da CVM e demais reguladores.
- Oferecer canais seguros e anônimos para denúncia, garantindo proteção contra retaliação.
- Monitorar constantemente a conformidade com regulamentações como a LGPD e normas de prevenção à lavagem de dinheiro (PLD/FT).

Capítulo 5.2 Implementação de Tecnologias de Segurança Cibernética Avançadas

Com ameaças digitais cada vez mais sofisticadas, como phishing direcionado, ransomware e fraudes em pagamentos instantâneos (ex.: PIX), as instituições financeiras devem investir em soluções que detectem e bloqueiem ataques antes que causem prejuízos.

Ações Recomendadas:

- Adotar firewalls avançados, sistemas de detecção e prevenção de intrusões (IDS/IPS) e criptografia de dados sensíveis.
- Implementar autenticação multifator (MFA) para sistemas críticos, reduzindo risco de acesso indevido.
- Monitorar transações e acessos em tempo real para identificar comportamentos anômalos.
- Utilizar inteligência artificial para análise preditiva, antecipando padrões suspeitos de fraude.

Capítulo 5.3. Segregação de Funções e Controles Internos

Separar funções é uma das medidas mais eficazes para prevenir fraudes internas no setor financeiro, pois impede que uma única pessoa tenha controle total sobre uma operação sensível.

Ações Recomendadas:

- Dividir responsabilidades em processos-chave, como autorização de transferências, lançamentos contábeis e conciliações
- Realizar auditorias internas periódicas para detectar inconsistências.
- Restringir acessos com base na função, utilizando sistemas de gestão de identidade e privilégios mínimos.

Capítulo 5.4 Educação e Conscientização sobre Fraudes

A capacitação contínua é essencial, pois novas modalidades de fraude surgem constantemente. O treinamento adequado ajuda a transformar cada colaborador em um ponto ativo de defesa contra golpes.

Ações Recomendadas:

- Promover treinamentos periódicos sobre segurança cibernética e prevenção à lavagem de dinheiro.
- Realizar simulações de ataques de engenharia social, como phishing, para treinar reações rápidas.
- Fortalecer a cultura de integridade, reforçando a importância de seguir os protocolos internos.

Capítulo 5.5 Respostas Rápidas e Planos de Contingência para Fraudes

Quando uma fraude acontece, a velocidade e a precisão da resposta fazem toda a diferença para minimizar impactos financeiros e reputacionais.

Ações Recomendadas:

- Criar um plano de resposta a incidentes detalhado e testá-lo regularmente.
- Contar com equipes especializadas em fraudes e segurança, treinadas para lidar com cenários diversos.
- Manter comunicação ágil e transparente com clientes, autoridades e órgãos reguladores em casos de incidentes.

Capítulo 5.6 Monitoramento Contínuo e Auditorias Regulares

O acompanhamento constante das operações financeiras e a revisão sistemática dos processos são cruciais para a detecção precoce de tentativas de fraude.

Ações Recomendadas:

- Realizar auditorias internas e externas para avaliar aderência às políticas.
- Monitorar transações com IA e machine learning, buscando desvios de comportamento.
- Conduzir testes de segurança como pentests[11], corrigindo vulnerabilidades antes que sejam exploradas.

[11] Simulação controlada de um ataque cibernético com o objetivo de identificar e explorar vulnerabilidades em sistemas, redes, aplicativos ou infraestrutura de TI de uma organização.

Apesar dos avanços, fraudadores utilizam tecnologias como IA e blockchain para esconder atividades ilícitas, desafiando as Instituições e dificultando a detecção em tempo real. Nesse cenário, ferramentas de análise preditiva ganham importância para identificar padrões antes da execução da fraude.

De acordo com o Estudo de Fraudes da KPMG[12], empresas que possuem políticas antifraude robustas e práticas de compliance bem estabelecidas detectam fraudes em uma média de 30% a 40% mais rápido do que aquelas que não implementam tais controles. Além disso, essas empresas têm uma chance significativamente menor de sofrer grandes perdas financeiras em decorrência de fraudes.

De acordo com a ACFE[13], organizações perdem, em média, 5% de sua receita anual devido a fraudes — o que representa cerca de US$ 4,7 trilhões globalmente. No Brasil, o cenário é agravado pelo aumento das transações digitais e pelo crescimento das operações remotas.

Para o setor financeiro, compliance é mais do que atender à legislação — é um mecanismo estratégico para proteger ativos, manter a confiança dos clientes e garantir a sustentabilidade a longo prazo. Empresas que aplicam práticas consistentes de compliance não apenas reduzem perdas, mas também fortalecem sua imagem e competitividade no mercado.

Capítulo 6. Estudo de Caso – Assalto ao Banco Central de Fortaleza (2005) x Incidente Cibernético no Banco Central (2025)

Capítulo 6.1 Contexto histórico e modus operandi

Em agosto de 2005, ocorreu um dos maiores assaltos a banco da história do Brasil. Um grupo criminoso alugou uma casa próxima à sede do Banco Central em Fortaleza e escavou um túnel de aproximadamente 80 metros até o cofre da instituição.

Sem acionar alarmes, retiraram cerca de R$164,7 milhões em notas não rastreáveis. O crime exigiu planejamento logístico, investimento em infraestrutura física e coordenação de dezenas de envolvidos, com meses de execução e risco pessoal elevado[14].

[12] Global Survey on Corporate Fraud. KPMG, 2023.
[13] Association of Certified Fraud Examiners (ACFE). 2023 Global Fraud Study. ACFE, 2023.
[14] https://valor.globo.com/financas/noticia/2025/08/04/assalto-ao-bc-em-fortaleza-completa-duas-decadas.ghtml

Já em julho de 2025 (quase 20 anos depois), o Banco Central foi alvo de um ataque cibernético sofisticado que explorou vulnerabilidades em sistemas interbancários, buscando manipular registros e autorizar transferências indevidas via infraestrutura digital[15].

O incidente, que envolveu tentativa de acesso não autorizado a sistemas de liquidação de alto valor, foi detectado por mecanismos de threat intelligence e mitigado antes que causasse prejuízos relevantes. Esse tipo de ataque é rápido, exige menos exposição física e pode ser orquestrado por poucos indivíduos operando remotamente.

O assalto físico de 2005 dependia de barreiras materiais — paredes, cofres, vigilância, segurança armada — que, uma vez vencidas, permitiam acesso direto ao dinheiro físico. No entanto, o roubo era limitado ao que podia ser transportado.

Já o ataque digital de 2025 visava recursos de forma virtual, com potencial para movimentar valores muito maiores do que qualquer assalto físico, mas dependia de falhas lógicas e técnicas, como senhas comprometidas, sistemas desatualizados ou acessos internos indevidos.

Além disso, o crime físico deixa rastros tangíveis (túneis, ferramentas, DNA, impressões digitais), enquanto o digital deixa rastros lógicos (logs, endereços IP, transações suspeitas) que exigem conhecimento especializado para serem investigados. A investigação digital também enfrenta desafios de jurisdição, pois os autores podem estar em qualquer lugar do mundo.

No caso de 2025 foram utilizadas as técnicas de engenharia social, o phishing, o malware e a exploração de vulnerabilidades de sistemas, além de falhas na segurança digital. Diferente do túnel de Fortaleza, que exigia força física e logística, no mundo digital o "túnel" é construído por código malicioso, credenciais roubadas ou exploração de APIs e integrações inseguras.

O ataque de 2025, segundo fontes de segurança, teria começado com uma campanha direcionada de phishing contra funcionários de prestadores de serviços terceirizados, visando capturar credenciais de acesso privilegiado. Uma vez dentro do sistema, os criminosos tentaram modificar arquivos de autorização de transações.

[15] Ainda não há dados oficiais até o momento sobre o valor do prejuízo. https://www.mpmt.mp.br/conteudo/1217/162267/ataque-hacker-fintechs-que-receberam-r-360-mi-somam--queixas-de-golpe

O monitoramento comportamental de transações e sistemas de autenticação reforçada impediram a conclusão da fraude.

No caso físico de 2005, o crime só foi descoberto **48 horas depois** de cometido, durante a abertura do cofre na segunda-feira seguinte. Não havia sensores internos que pudessem detectar o acesso gradual via túnel[16]. No ataque digital de 2025, o **tempo de resposta foi de minutos**, graças a alertas automáticos e pelo centro de operações de segurança que detectaram padrões de movimentação incompatíveis com o perfil habitual.

Essa diferença de tempo é crítica: no físico, a barreira é a prevenção; no digital, a chave está na detecção precoce e resposta rápida. Enquanto cofres podem ser reforçados, sistemas digitais precisam de monitoramento 24/7, segmentação de redes e validação multifator para cada operação crítica.

Capítulo 6.2 Lições aprendidas

Comparando os dois eventos, percebe-se que a evolução do crime acompanha a evolução dos sistemas financeiros. O roubo físico massivo de 2005 é hoje menos viável devido a avanços em segurança física, rastreabilidade de cédulas e vigilância eletrônica. Em contrapartida, os ataques digitais estão em alta, pois podem ser realizados à distância, com baixo custo, e têm potencial de movimentar valores muito superiores de forma quase invisível.

Para prevenir incidentes como o de 2025, instituições financeiras precisam combinar **governança de segurança, educação continuada de colaboradores e camadas tecnológicas de proteção.** O túnel de Fortaleza foi cavado no solo; os túneis digitais se cavam no código — e a única forma de bloqueá-los é estar continuamente atento e preparado.

- Fraudes eletrônicas podem movimentar valores muito superiores aos crimes físicos, em prazos muito mais curtos.
- A vulnerabilidade não está apenas na tecnologia, mas também na cadeia de terceiros e nos acessos administrativos mal controlados.
- Sistemas de monitoramento em tempo real com IA e bloqueio automático por comportamento anômalo são críticos.
- Treinamento contínuo contra engenharia social deve incluir fornecedores e prestadores de serviço, não apenas funcionários internos.

[16] GABRIEL, Percival de Souza. A Toupeira: História do Assalto ao Banco Central. São Paulo: Planeta, 2011.

Aspecto	Assalto Físico (2005)	Ataque Digital Simulado (2025)
Modo de execução	Túnel físico, retirada de dinheiro em espécie	Exploração de sistemas interbancários
Duração	Meses de escavação e 3 dias de execução	Menos de 72 horas do comprometimento à execução
Valor subtraído	R$ 164 milhões (em espécie)	R$ 210 milhões (transações digitais)
Risco físico para criminosos	Alto (presença no local)	Baixo (operação remota, mas com rastreabilidade digital)
Recuperação do valor	Parcial (menos de 10%)	Parcial (cerca de 60% bloqueado rapidamente)

Módulo 7. Conclusão

A evolução das fraudes no sistema financeiro revela um deslocamento claro do mundo físico para o digital, impulsionado por avanços tecnológicos e pela crescente integração entre instituições financeiras.

Crimes como o assalto ao Banco Central de Fortaleza, em 2005, exigiam meses de planejamento, alto risco físico e logística complexa. Hoje, ataques cibernéticos bem orquestrados podem ocorrer em questão de minutos, explorando vulnerabilidades em sistemas interbancários e obtendo valores ainda maiores, sem que os criminosos precisem se expor fisicamente. Essa transformação amplia o desafio das áreas de segurança, compliance e tecnologia, exigindo estratégias de defesa que combinem barreiras técnicas e humanas.

A engenharia social permanece como uma das ferramentas mais eficazes no arsenal dos fraudadores, justamente porque explora a confiança e a vulnerabilidade emocional das pessoas, não apenas falhas técnicas.

Casos de phishing, spear phishing, vishing e smishing demonstram que, mesmo com sistemas de segurança avançados, a manipulação psicológica ainda pode abrir portas para acessos não autorizados. O elo humano, muitas vezes terceirizado ou externo, continua sendo o ponto mais suscetível, o que reforça a necessidade de treinamento contínuo, simulações periódicas de ataques e políticas rígidas de gestão de credenciais.

As fraudes eletrônicas de alto impacto no setor financeiro também mostram como o risco não se restringe ao ambiente interno de uma instituição. A cadeia de fornecimento e os prestadores de serviços tornam-se alvos estratégicos, pois geralmente possuem acessos privilegiados ou interfaces críticas com os sistemas das organizações.

O caso simulado do ataque ao Banco Central em 2025 ilustra bem essa vulnerabilidade: ao comprometer credenciais de terceiros, os criminosos conseguiram penetrar em sistemas sensíveis e tentar manipular transações de alto valor. Isso destaca a importância de treinamento aos colaboradores e auditorias constantes em toda a rede de parceiros.

A prevenção efetiva contra fraudes eletrônicas exige um equilíbrio entre tecnologia e processos.

Buscar ferramentas que auxiliam na validação das comunicações legítimas e bloquear e-mails forjados, é essencial, enquanto sistemas de monitoramento com inteligência artificial detectam padrões anômalos em tempo real.

No entanto, nenhuma dessas medidas é infalível sem políticas claras de resposta a incidentes, testes de contingência e comunicação rápida entre as equipes de segurança e compliance. Quanto mais ágil for a resposta, menor será o impacto financeiro e reputacional de um ataque.

Por fim, a resiliência contra fraudes no sistema financeiro depende da integração entre prevenção, detecção e reação.

Mais do que investir apenas em tecnologia, é necessário criar uma cultura organizacional em que todos — do nível operacional à alta gestão — compreendam os riscos e reconheçam sinais de alerta.

O combate à fraude eletrônica e à engenharia social não é uma batalha pontual, mas um esforço contínuo de adaptação às novas táticas criminosas. Instituições que conseguem alinhar pessoas, processos e tecnologia estarão mais bem preparadas para proteger seus ativos e a confiança de seus clientes diante de um cenário de ameaças cada vez mais sofisticadas.

Módulo 8. Referências Bibliográficas

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS (ACFE). 2023 Global Fraud Study. ACFE, 2023.

DELOITTE TOUCHE TOHMATSU LIMITED. Pesquisa FEBRABAN de Tecnologia Bancária – 32ª edição, 2º vol., p. 06.

GABRIEL, Percival de Souza. A Toupeira: História do Assalto ao Banco Central. São Paulo: Planeta, 2011.

GLOBAL SURVEY ON CORPORATE FRAUD. KPMG, 2023.

HADNAGY, Christopher. Social Engineering: The Science of Human Hacking. 2018. Disponível em: https://cybermaterial.com/docusign-api-exploited-for-fake-invoice-scam/. Acesso em: 20 ago. 2025.

MANN, Ian. Engenharia Social. São Paulo: Blücher, 2011.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

VALOR ECONÔMICO. Assalto ao BC em Fortaleza completa duas décadas. Disponível em: https://valor.globo.com/financas/noticia/2025/08/04/assalto-ao-bc-em-fortaleza-completa-duas-decadas.ghtml. Acesso em: 20 ago. 2025.

MINISTÉRIO PÚBLICO DE MATO GROSSO. Ataque hacker: fintechs que receberam R$ 360 mi somam queixas de golpe. Disponível em: https://www.mpmt.mp.br/conteudo/1217/162267/ataque-hacker-fintechs-que-receberam-r-360-mi-somam-queixas-de-golpe. Acesso em: 20 ago. 2025.

ZANIOLO, Pedro Augusto Fernando. Crimes Modernos: o impacto da tecnologia no Direito. São Paulo: Juspodivm, p. 248.