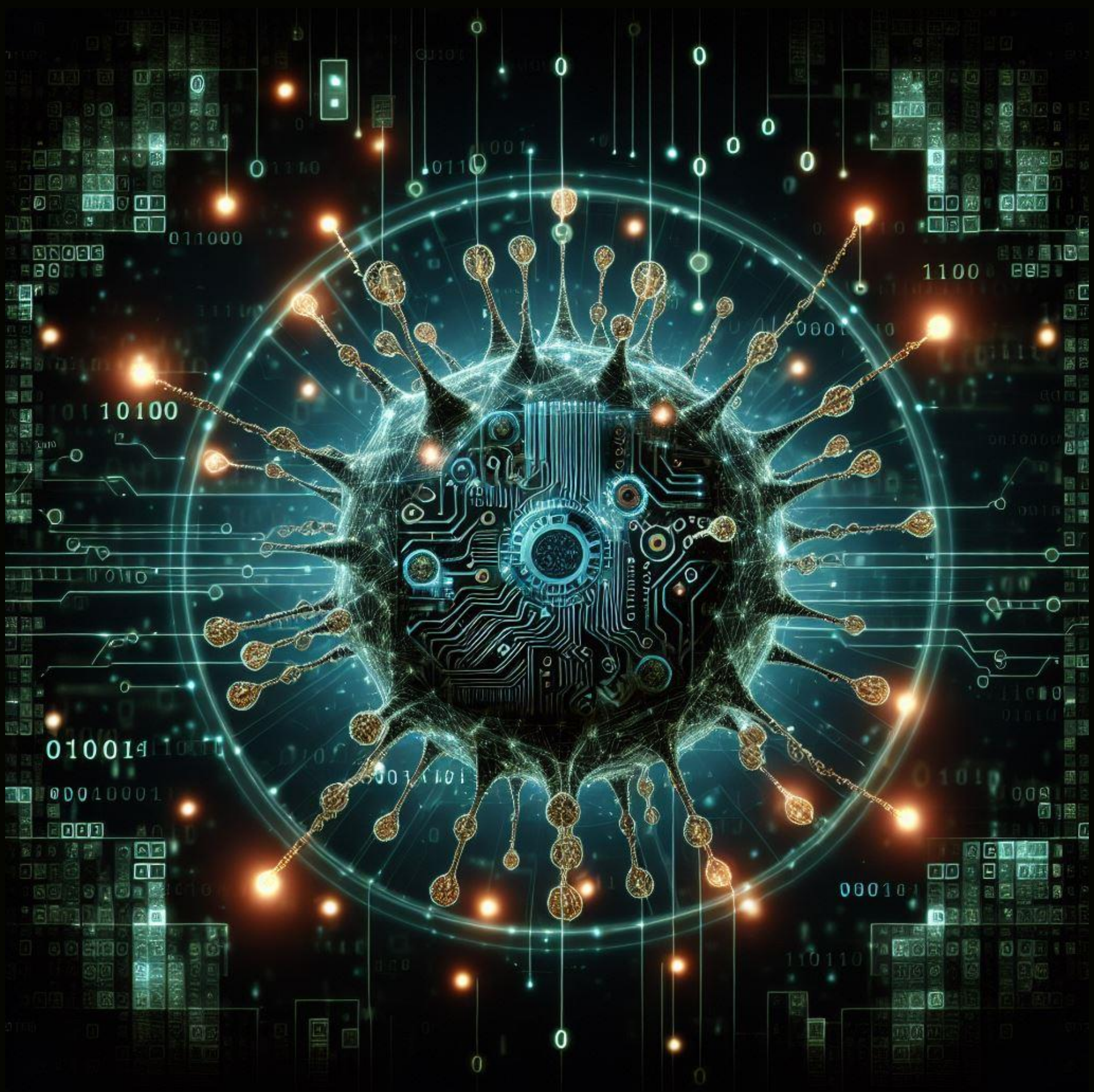
# BLINDAGEM DIGITAL:
## Segurança bancária online



Nathanael Andrade

# SUMÁRIO

- Introdução

1. SEGURANÇA ONLINE
2. PRINCIPAIS AMEAÇAS
3. PROTEÇÃO PARA USUÁRIOS
4. TECNOLOGIAS EM USO
5. INOVAÇÃO COM IA
6. + LEITURAS

- Conclusão

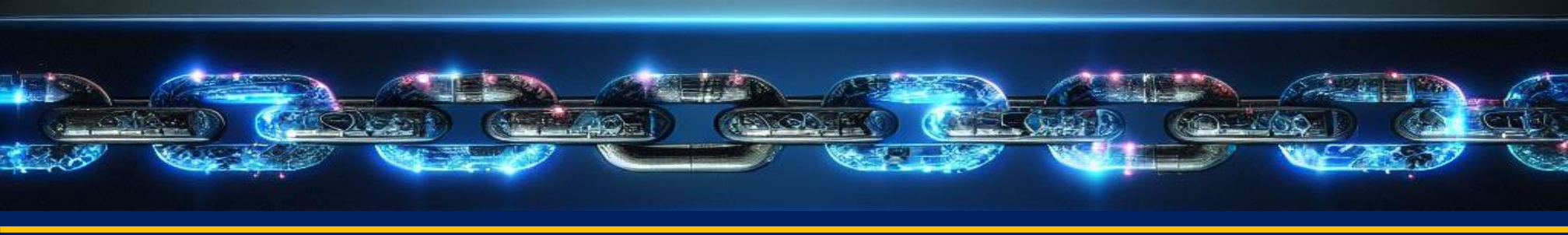
# INTRODUÇÃO

A evolução dos serviços bancários tem sido notável nas últimas décadas. Desde as tradicionais agências físicas até os modernos aplicativos de banco digital, a tecnologia transformou a maneira como gerenciamos nossas finanças. Hoje, é possível realizar transações, pagar contas e até investir com apenas alguns cliques, tudo isso sem sair de casa.

Com essa conveniência, no entanto, surgem novos desafios. A segurança bancária tornou-se uma preocupação central, à medida que cibercriminosos desenvolvem métodos cada vez mais sofisticados para acessar informações financeiras. Phishing, malware e fraudes online são apenas algumas das ameaças que os usuários enfrentam diariamente.

Manter as finanças seguras é essencial para proteger não apenas o dinheiro, mas também a identidade e a privacidade e até mesmo a integridade física dos usuários dos usuários. Adotar medidas de segurança, como o uso de senhas fortes, a autenticação de dois fatores  e os sistemas de geofencing são fundamentais para garantir que as transações financeiras sejam realizadas de forma segura e confiável.

# 1. SEGURANÇA ONLINE



# 2. SEGURANÇA BANCÁRIA ONLINE

As fraudes e ataques cibernéticos têm consequências graves tanto para as instituições financeiras quanto para os clientes.

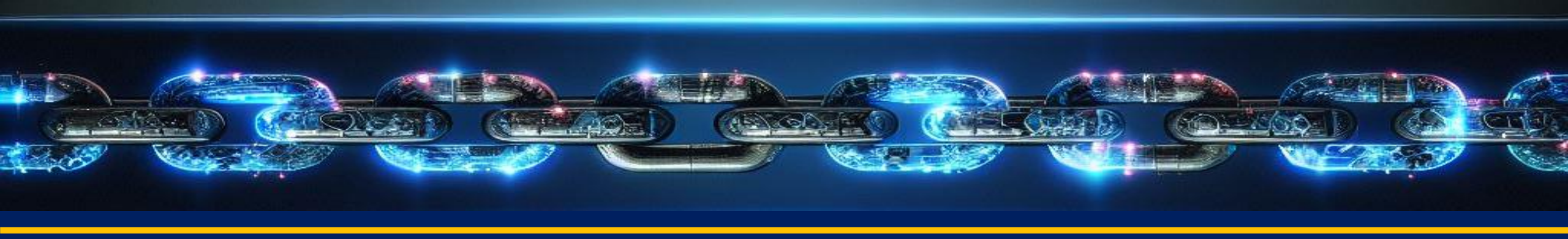
Para as instituições, esses incidentes podem resultar em perdas financeiras, danos à reputação e custos elevados com medidas de remediação e segurança.

Para os clientes, especialmente os mais vulneráveis (como idosos, pessoas com pouco conhecimento tecnológico e mesmo os usuários que vivem em áreas afastadas), as consequências incluem a perda de dinheiro, roubo de identidade e o estresse associado à recuperação de suas finanças e informações pessoais, além da possibilidade de serem submetidos à violência física na mão de bandidos que podem mantê-los sob coação enquanto processam a .

Por fim, a confiança no sistema bancário pode ser abalada, afetando a relação entre bancos e seus clientes.

Assim, a segurança em transações financeiras online é crucial para proteger os usuários e instituições contra uma variedade de ameaças.

# 2. PRINCIPAIS AMEAÇAS



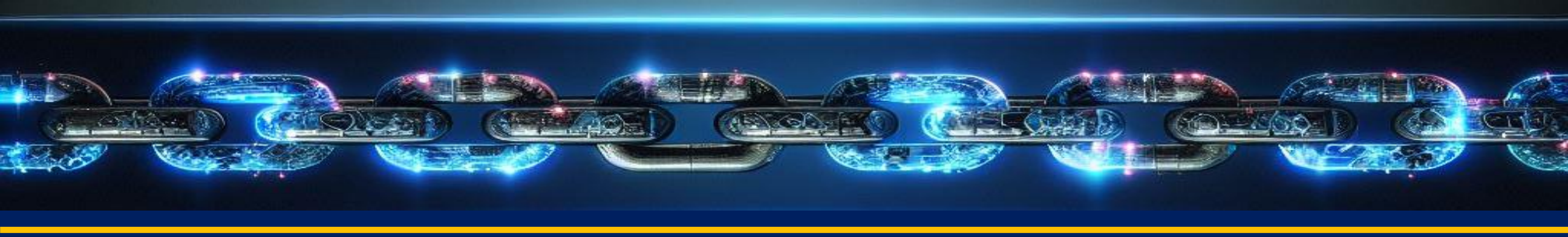
# 2. PRINCIPAIS AMEAÇAS NO MUNDO FÍSICO

Nas salas de autoatendimento  (SAA) das instituições financeiras, o cliente bancário está exposto a um tipo de ameaça mista, uma vez que a fraude em terminal eletrônico ocorrerá a partir de uma interação entre pessoas ou entre pessoas e dispositivos corrompidos.

Assim,  é importante estar sempre atento e sempre bem informado para evitar as ações dos bandidos no mundo físico.

Exemplos de golpes comuns nos terminais de autoatendimento

- **Chupa-Cabra:** Dispositivos instalados nos terminais para copiar dados do cartão
- **Falso Funcionário:** Golpistas se passam por funcionários do banco para oferecer ajuda.
- **Troca de Cartão:** Golpistas distraem a vítima e trocam seu cartão por outro.
- **Sequestros relâmpagos:** clientes são mantidos como reféns enquanto suas contas bancárias são sacadas.



# 2. PRINCIPAIS AMEAÇAS  ONLINE

As ameaças no mundo digital são muitas e estão  cada vez mais sofisticadas. Alguns dos golpes mais comuns são explanados abaixo:

- Phishing: E-mails ou mensagens falsas que parecem ser de instituições legítimas, solicitando informações pessoais ou financeiras.
- Vishing: Golpes por telefone onde os fraudadores se passam por funcionários de bancos para obter dados sensíveis.
- Malware: Programas maliciosos que infectam dispositivos para roubar informações bancárias.
- Roubo de Identidade: Uso não autorizado de informações pessoais para realizar transações fraudulentas.
- Smishing: Mensagens de texto fraudulentas que tentam induzir você a clicar em links maliciosos.
- Golpes de Suporte Técnico: Falsos técnicos de suporte que alegam problemas no seu dispositivo e pedem acesso remoto ou pagamento.
- Fraudes em Compras Online: Sites falsos que imitam lojas legítimas para roubar informações de pagamento.

MANTER-SE INFORMADO E ATENTO É ESSENCIAL PARA GARANTIR A SUA SEGURANÇA FÍSICA E A DE SUAS TRANSAÇÕES BANCÁRIAS. CUIDE-SE E PROTEJA SUAS FINANÇAS!

# 3. PROTEÇÃO PARA OS USUÁRIOS

# 4. PROTEÇÃO PARA USUARIOS

O desenvolvimento de uma cultura de cuidados é essencial para reduzir a ocorrência de golpes em ambientes de autoatendimento e em aplicativos de internet banking. Para os usuários, isso significa adotar práticas seguras, como a utilização de senhas fortes e únicas, a ativação da autenticação em duas etapas e a constante vigilância sobre suas transações financeiras. A conscientização sobre os métodos comuns de fraude, como phishing e engenharia social, também é crucial para que os usuários possam identificar e evitar possíveis ameaças.

Por outro lado, as instituições financeiras têm a responsabilidade de implementar medidas de segurança robustas e de fácil utilização. Isso inclui a adoção de tecnologias avançadas de criptografia, a realização de auditorias regulares de segurança e a oferta de suporte ao cliente eficiente para lidar com possíveis incidentes de fraude. Além disso, é fundamental que essas instituições invistam em campanhas educativas para informar e orientar seus clientes sobre as melhores práticas de segurança.

A colaboração entre usuários e instituições financeiras é a chave para criar um ambiente digital mais seguro. Quando ambos os lados estão bem informados e comprometidos com a segurança, a probabilidade de sucesso dos golpes diminui significativamente. Essa parceria não só protege os ativos financeiros, mas também fortalece a confiança no sistema bancário digital, permitindo que mais pessoas usufruam dos benefícios da tecnologia com tranquilidade.

# SEGURANÇA BANCÁRIA – NO AUTOATENDIMENTO

- Prefira utilizar terminais de autoatendimento em locais movimentados e bem iluminados.
- Evite realizar transações em horários de pouco movimento.
- Atenção ao redor
- Fique atento a pessoas suspeitas ao redor.
- Se sentir-se inseguro, cancele a operação e procure outro terminal.
- Cubra o teclado ao digitar sua senha.
- Não aceite ajuda de estranhos, mesmo que pareçam funcionários do banco.
- Recolha todos os comprovantes e recibos após a transação. Descarte-os de forma segura, evitando que contenham informações pessoais.
- Verifique se há algo estranho no leitor de cartões antes de usá-lo.
- Nunca aceite ajuda de estranhos e procure um funcionário identificado.
- Sempre guarde seu cartão imediatamente após a transação.

# SEGURANÇA BANCÁRIA – NO MUNDO “ONLINE

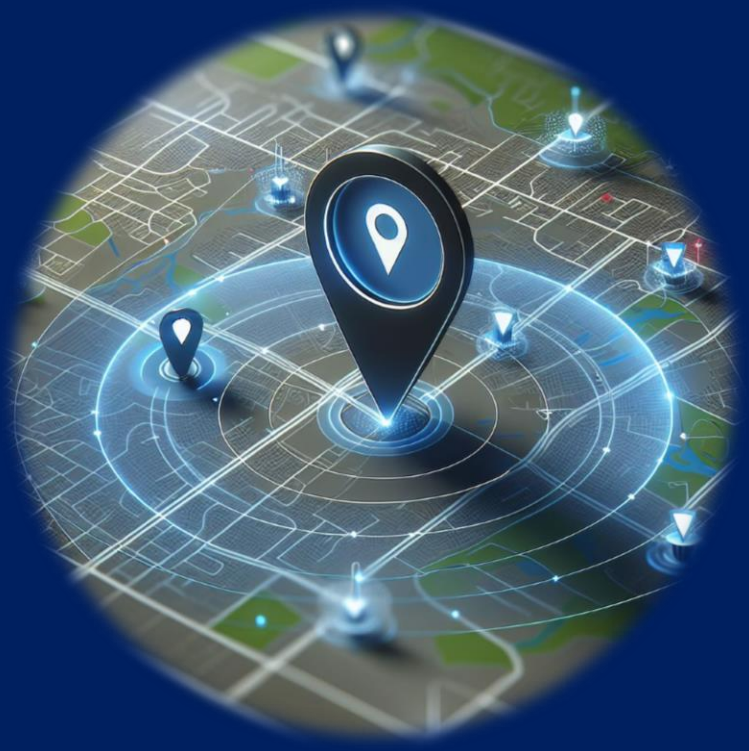
- Senhas e Autenticação: Utilize senhas fortes e únicas para cada serviço bancário.
- Ative a autenticação em duas etapas sempre que possível.
- Mantenha seu dispositivo (computador, smartphone, tablet) atualizado com as últimas versões de software e antivírus.
- Evite acessar contas bancárias em dispositivos públicos ou redes Wi-Fi abertas.
- Desconfie de e-mails e mensagens que solicitam informações pessoais ou financeiras.
- Verifique sempre o remetente e evite clicar em links suspeitos.
- Baixe aplicativos bancários apenas das lojas oficiais (Google Play, App Store).
- Verifique as permissões solicitadas pelo aplicativo e desconfie de solicitações excessivas.
- Verifique regularmente o extrato de sua conta para identificar transações suspeitas.
- Ative notificações de transações para acompanhar movimentações em tempo real.

# SEGURANÇA BANCÁRIA – NO MUNDO “ONLINE

- Senhas e Autenticação: Utilize senhas fortes e únicas para cada serviço bancário.
- Ative a autenticação em duas etapas sempre que possível.
- Mantenha seu dispositivo (computador, smartphone, tablet) atualizado com as últimas versões de software e antivírus.
- Evite acessar contas bancárias em dispositivos públicos ou redes Wi-Fi abertas.
- Desconfie de e-mails e mensagens que solicitam informações pessoais ou financeiras.
- Verifique sempre o remetente e evite clicar em links suspeitos.
- Baixe aplicativos bancários apenas das lojas oficiais (Google Play, App Store).
- Verifique as permissões solicitadas pelo aplicativo e desconfie de solicitações excessivas.
- Verifique regularmente o extrato de sua conta para identificar transações suspeitas.
- Ative notificações de transações para acompanhar movimentações em tempo real.

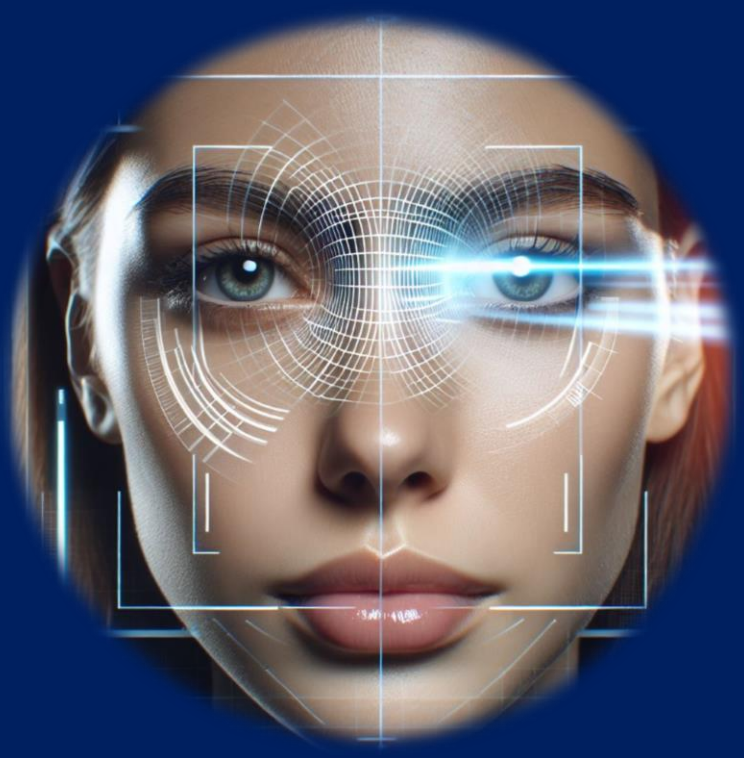
# 4. TECNOLOGIAS EM USO

**Autenticação Multifatorial (MFA):** Adiciona camadas extras de verificação para garantir que apenas o usuário autorizado possa acessar suas contas.




**GEOFENCING:** Tecnologia que permite definir áreas seguras para transações. Se uma transação for iniciada fora dessas áreas, o usuário é notificado e a transação é bloqueada até confirmação.

**BLOCKCHAIN:** Adicionar camadas extras de verificação para garantir que apenas o usuário autorizado possa acessar suas contas.



**BIOMETRIA:** Adicionar camadas extras de verificação para garantir que apenas o usuário autorizado possa acessar suas contas.

**INTELIGENCIA ARTIFICIAL:** Adicionar camadas extras de verificação para garantir que apenas o usuário autorizado possa acessar suas contas.

**CRIPTOGRAFIA:** Adicionar camadas extras de verificação para garantir que apenas o usuário autorizado possa acessar suas contas.


# 5. INOVAÇÃO COM IA

# 5. SOLUÇÕES INOVADORAS COM IA

A inteligência artificial (IA) desempenha um papel crucial na segurança online para usuários bancários, proporcionando uma camada adicional de proteção contra fraudes e ataques cibernéticos.

Com a capacidade de analisar grandes volumes de dados em tempo real, a IA pode identificar padrões suspeitos e comportamentos anômalos, permitindo a detecção precoce de atividades fraudulentas.

Além disso, sistemas de IA podem aprender e se adaptar continuamente às novas ameaças, tornando-se mais eficazes na prevenção de ataques. Isso não só aumenta a segurança das transações bancárias, mas também fortalece a confiança dos usuários nos serviços bancários digitais.

Há diversas possibilidades para aumentar a segurança bancária com o uso da IA. Vamos apresentar a seguir algumas soluções que, a princípio, podem parecer mirabolantes mas que em breve poderão ser realidade na vida de cada um de nós

## 1. Detecção Proativa de Fraudes

A IA pode analisar grandes volumes de dados em tempo real para identificar padrões suspeitos. Algoritmos de aprendizado de máquina podem ser treinados para reconhecer comportamentos anômalos, como transações financeiras incomuns ou tentativas de login de locais inesperados. Isso permite a detecção proativa de fraudes antes que elas causem danos significativos.

## 2. Assistentes Virtuais Inteligentes

Assistentes virtuais equipados com IA podem educar os usuários sobre práticas seguras na internet e alertá-los sobre possíveis golpes. Esses assistentes podem fornecer dicas personalizadas com base no comportamento do usuário e até mesmo simular cenários de phishing para treinar os usuários a reconhecerem ameaças.

## 3. Autenticação Biométrica Avançada

A IA pode aprimorar os sistemas de autenticação biométrica, como reconhecimento facial e de voz, para garantir que apenas usuários autorizados tenham acesso a informações sensíveis. Algoritmos avançados podem detectar tentativas de falsificação, como o uso de fotos ou gravações de voz, aumentando a segurança.

## 4. Análise de Sentimento e Linguagem Natural

A análise de sentimento e processamento de linguagem natural (NLP) podem ser usados para monitorar comunicações em tempo real, como e-mails e mensagens de texto, identificando linguagem que sugira tentativas de golpe. Isso pode incluir a detecção de urgência falsa, pedidos de informações pessoais ou links suspeitos.

## 5. Redes Neurais para Previsão de Golpes

Redes neurais profundas podem ser treinadas para prever novos tipos de golpes com base em dados históricos e tendências emergentes. Isso permite que as empresas se preparem e ajustem suas defesas antes que novos métodos de fraude se tornem prevalentes.

## 6. Blockchain e Contratos Inteligentes

A IA pode ser combinada com tecnologias de blockchain para criar contratos inteligentes que executam automaticamente transações seguras e verificáveis. Isso pode reduzir a possibilidade de fraudes em transações financeiras e comerciais, garantindo que todas as partes cumpram suas obrigações.

## 7. Sistemas de Reputação Baseados em IA

Plataformas online podem usar IA para criar sistemas de reputação que avaliem a confiabilidade de vendedores, compradores e outros usuários. Isso pode ajudar a identificar e isolar rapidamente contas fraudulentas, protegendo os usuários de interações maliciosas.

## 8. Monitoramento de Redes Sociais

A IA pode monitorar redes sociais para detectar e remover rapidamente contas falsas e atividades suspeitas. Algoritmos podem identificar padrões de comportamento associados a golpes, como a criação de múltiplas contas em um curto período de tempo ou a disseminação de links maliciosos.

## 9. Educação e Conscientização Automatizadas

Plataformas de IA podem fornecer programas de educação e conscientização automatizados, adaptados às necessidades de diferentes grupos de usuários. Isso pode incluir tutoriais interativos, quizzes e simulações que ensinam os usuários a reconhecer e evitar golpes.

## 10. Colaboração Internacional Facilitada pela IA

A IA pode facilitar a colaboração entre agências de segurança e empresas em diferentes países, compartilhando informações sobre ameaças e estratégias de mitigação em tempo real. Isso pode criar uma rede global de defesa contra golpes, tornando mais difícil para os fraudadores operarem em escala internacional.


# 6. + LEITURAS

**DICAS IMPORTANTES E CARTILHA DE SEGURANÇA DA CAIXA –** https://www.caixa.gov.br/seguranca/Paginas/default.aspx

**Prejuízo com golpes:** https://finsidersbrasil.com.br/estudos-e-relatorios/prejuizo-com-golpes-financeiros-supera-r-2-bi-segundo-pesquisa/

**Hackers:** https://vradvogados.com.br/como-os-hackers-conseguem-acessar-contas-bancarias-por-aplicativos-principais-metodos-e-como-se-proteger/

**Segurança quântica:** https://securityleaders.com.br/seguranca-na-era-quantica-qual-o-futuro-da-protecao-por-criptografia/

**Criptografia:**

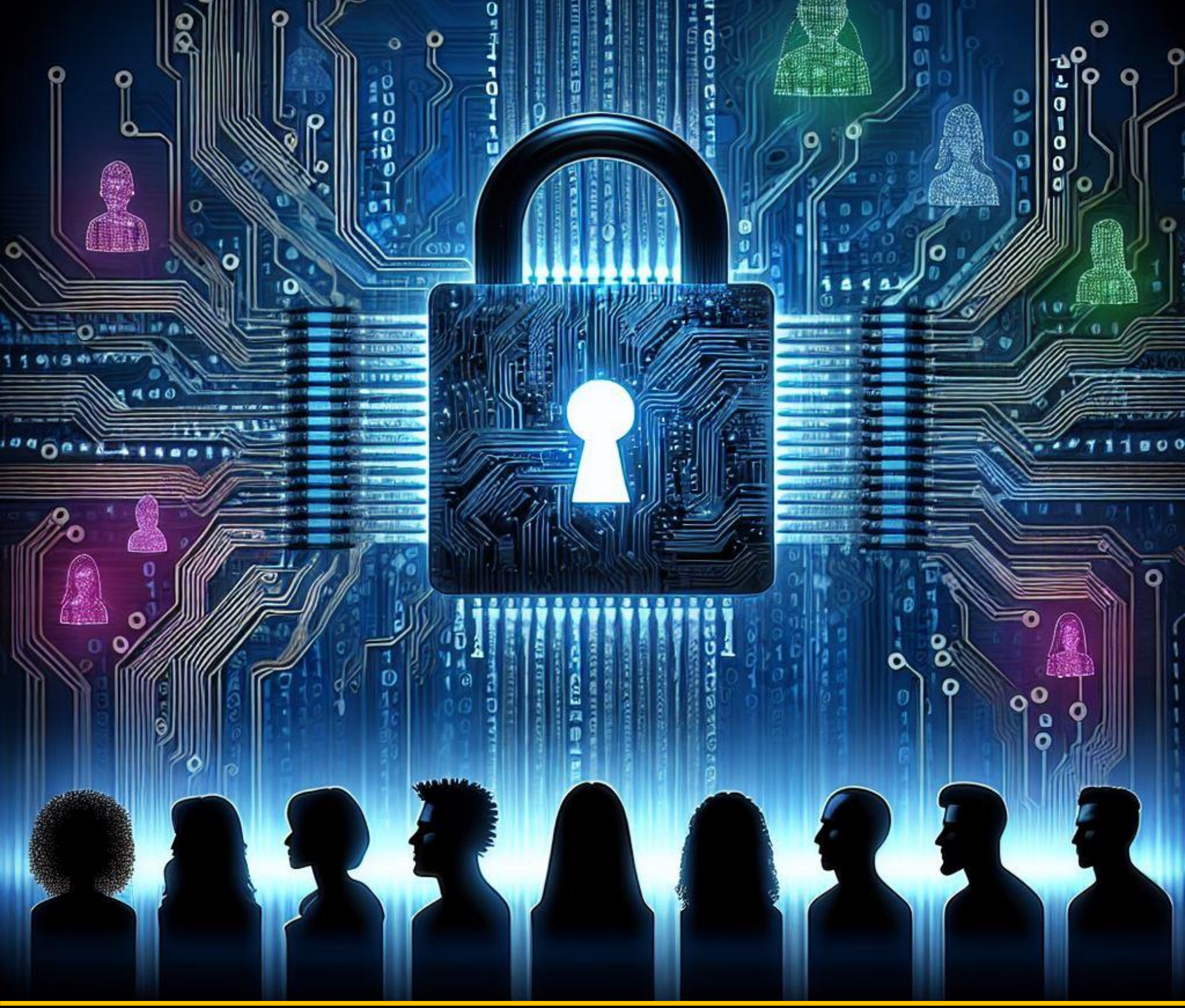
https://www.ibm.com/br-pt/topics/quantum-safe-cryptography

**IA na segurança bancária:**

https://febrabantech.febraban.org.br/temas/inteligencia-artificial/como-os-bancos-estao-usando-a-inteligencia-artificial-e-o-big-data-para-evitar-a-exposicao-a-crimes-financeiros

https://cantarinobrasileiro.com.br/o-papel-da-ia-na-seguranca-dos-bancos/

**(todos os links com acesso em 20/12/2024)**



# “OS HOMENS CRIAM AS FERRAMENTAS. AS FERRAMENTAS RECRIAM O HOMEM”

MARSHALL McLUHAN