Engenharia Social

O ELO HUMANO NA SEGURANÇA BANCÁRIA

André C A Loureiro

Engenharia Social - O Elo Humano na Segurança Bancária

Autor: André Cavalcanti Assumpção Loureiro
Matricula: c107192

1. Introdução

Engenharia social consiste em técnicas de manipulação psicológica utilizadas para induzir indivíduos a divulgarem informações confidenciais, como credenciais de acesso ou dados financeiros. Essa prática representa uma vulnerabilidade significativa para o setor bancário, pois pode acarretar prejuízos financeiros substanciais e danos à credibilidade da instituição.

Este estudo tem como objetivo analisar o funcionamento dos ataques de engenharia social, identificando as principais vulnerabilidades exploradas e as estratégias de mitigação mais eficazes para o setor bancário. Abordaremos as táticas empregadas por agentes mal-intencionados, apresentando exemplos práticos de medidas preventivas adotadas com sucesso por instituições financeiras.

Diante do aumento da sofisticação dessas práticas, torna-se imprescindível que os bancos invistam em treinamentos contínuos para seus colaboradores e implementem políticas de segurança cibernética rigorosas para minimizar riscos.

2. Conceitos Fundamentais

A engenharia social é uma técnica de manipulação psicológica que visa persuadir indivíduos a divulgar informações confidenciais e/ou realizar ações que comprometam a segurança de uma organização. Essa abordagem explora vulnerabilidades humanas, que são muitas vezes pouco observadas em análises tradicionais de segurança da informação.

Há diversos tipos de ataques de engenharia social e historicamente, a engenharia social tem sido utilizada em diversas formas, desde golpes simples, que miram pessoas comuns, até ataques cibernéticos sofisticados, voltados a corporações grandes instituições. A evolução dessas táticas destaca a importância de uma abordagem holística para a segurança, considerando tanto os aspectos técnicos quanto comportamentais.

Compreender esses conceitos é essencial para mitigar os riscos no setor bancário, onde a manipulação psicológica pode ter consequências financeiras e reputacionais significativas.

3. Vulnerabilidades no Setor Bancário

O setor bancário é um alvo atrativo para ataques de engenharia social devido ao alto valor das informações e recursos financeiros envolvidos. As vulnerabilidades exploradas incluem falhas nos processos internos, falta de treinamento adequado e confiança excessiva em protocolos de segurança puramente técnicos.

Os erros humanos mais comuns incluem:

- compartilhamento inadvertido de informações sensíveis
- reutilização de senhas fracas e
- ausência de verificação de identidade em procedimentos críticos.

Exemplos de ataques bem-sucedidos incluem o uso de e-mails falsos tendo como remetente autoridades internas e chamadas telefônicas manipulativas. Stanley Milgram, autor de trabalhos sobre indução de obediência e construção de autoridade demonstrou como é possível levar indivíduos a cometer erros graves, mesmo quando contrariam seus próprios valores morais. Ataques de engenharia social costumam se utilizar da confusão gerada por urgências e "máscaras de autoridade" para persuadir pessoas a tomarem decisões equivocadas sem questionar a legitimidade da fonte.

Reconhecer essas vulnerabilidades e como elas podem surgir é o primeiro passo para a implementação de uma estratégia de defesa eficaz, focando na preparação contínua e na criação de uma cultura organizacional baseada em sistemas sólidos de segurança.

4. Técnicas e Táticas de Ataque

Algumas técnicas de engenharia social são usadas para explorar vulnerabilidades no setor bancário. Algumas das mais comuns incluem:

Exemplos Brasileiros de Golpes de Engenharia Social

Phishing e Spear Phishing

Em 2022, a Natura, uma das maiores empresas de cosméticos do Brasil, foi alvo de um ataque de spear phishing. Criminosos comprometeram contas de e-mail internas e enviaram mensagens falsas para parceiros e fornecedores, tentando obter informações financeiras e dados sensíveis.

O incidente destacou a importância da conscientização sobre mensagens fraudulentas, tanto internamente quanto com parceiros externos.
Fonte: hlti.com.br

Pretexting

Em 2015, uma jovem de 23 anos em Macapá (AP) se passou por um advogado no aplicativo de relacionamentos Tinder para obter vantagens financeiras das vítimas, como empréstimos, ao longo do desenvolvimento da falsa relação.

Ela foi presa no mesmo ano e assumiu o crime.
Fonte: compugraf.com.br

Baiting

Embora não haja um caso específico amplamente divulgado no Brasil, é comum que criminosos utilizem iscas digitais, como anúncios de downloads gratuitos de softwares populares ou promoções irresistíveis, que, ao serem acessados, instalam malwares nos dispositivos das vítimas.

Esses malwares podem roubar informações pessoais ou financeiras, comprometendo a segurança dos usuários.
Fonte: keepersecurity.com

Tailgating

Casos de tailgating no Brasil não são frequentemente divulgados publicamente.
No entanto, essa prática ocorre quando uma pessoa não autorizada segue de perto um funcionário autorizado para entrar em áreas restritas de uma empresa, aproveitando-se da confiança ou distração para obter acesso físico a instalações seguras.

É uma técnica de engenharia social que explora a cortesia ou desatenção dos funcionários para obter acesso não autorizado.
Fonte: checkpoint.com

Esses exemplos demonstram como diferentes técnicas de engenharia social têm sido aplicadas no Brasil, reforçando a necessidade de vigilância e educação contínua em segurança da informação.

Essas táticas são frequentemente combinadas para aumentar as chances de sucesso. Um entendimento detalhado de cada abordagem permite que as instituições financeiras identifiquem melhor as vulnerabilidades em seus fluxos de processos e criem defesas mais robustas, educando continuamente seus colaboradores para identificar tentativas de manipulação.

5. Consequências de Falhas em Segurança

As falhas de segurança no setor bancário podem acarretar sérios prejuízos financeiros e de reputação. Quando uma instituição é vítima de um ataque bem-sucedido de engenharia social, pode sofrer desde a perda direta de recursos financeiros até a exposição de dados confidenciais de clientes.

Além do impacto financeiro, a perda de confiança do público pode ser devastadora, resultando em fuga de clientes e desvalorização no mercado. As consequências legais também são graves, com multas pesadas e processos judiciais devido ao não cumprimento de normas regulatórias.

É essencial que os bancos compreendam esses riscos e adotem medidas preventivas robustas para evitar tais falhas.

Consequências de Cair em Golpes de Engenharia Social no Brasil

Phishing e Spear Phishing

- **Prejuízo Financeiro:** No caso da Natura, o ataque poderia ter causado grandes perdas financeiras caso os criminosos tivessem êxito em obter transferências ou pagamentos fraudulentos.
- **Vazamento de Dados:** Informações sensíveis de clientes e parceiros podem ser expostas, resultando em quebra de sigilo e possível penalização sob a LGPD (Lei Geral de Proteção de Dados).
- **Danos à Reputação:** A imagem da empresa foi afetada, comprometendo a confiança de clientes e parceiros comerciais.
- Fonte: hlti.com.br

Pretexting

- **Perda Financeira:** No caso da fraude pelo Tinder em Macapá, as vítimas cederam empréstimos e valores financeiros diretamente à golpista.
- **Impacto Emocional:** As vítimas também sofreram abalos emocionais por terem confiado em alguém que explorou o vínculo afetivo para fins criminosos.
- **Danos à Imagem Pessoal:** Para a autora do golpe, o caso resultou em sua prisão e exposição pública.
- Fonte: compugraf.com.br

Baiting

- **Infecção por Malware:** Pendrives e links maliciosos podem instalar softwares espiões, comprometendo dados sensíveis e acessos bancários.
- **Roubo de Identidade:** Dados como CPF, endereços e informações bancárias podem ser coletados e usados para fraudes e abertura de contas falsas.
- **Comprometimento de Sistemas Corporativos:** Caso o malware atinja redes empresariais, pode haver paralisação de operações e extorsão (ransomware).
- Fonte: keepersecurity.com

Tailgating

- **Acesso Não Autorizado:** Um invasor pode acessar áreas restritas, comprometendo a segurança física de pessoas e equipamentos.
- **Espionagem Industrial:** Informações sigilosas podem ser acessadas ou copiadas, resultando em prejuízos competitivos para a empresa.
- **Risco à Integridade Física:** Em empresas de alta segurança, como bancos e centros de dados, a presença não autorizada pode representar riscos diretos à segurança dos funcionários.
- Fonte: checkpoint.com

Esses casos evidenciam as diversas consequências que golpes de engenharia social podem causar, desde prejuízos financeiros até danos emocionais e comprometimento de dados. A educação e a prevenção são essenciais para reduzir os impactos dessas práticas criminosas.

6. Métodos de Prevenção e Mitigação

Para mitigar os riscos de engenharia social, os bancos devem implementar abordagens de segurança abrangentes, que envolvam tanto aspectos técnicos quanto humanos. Não vamos abordar mais detalhes, mas seguem algumas das boas práticas que podem refletir na melhoria da segurança interna de corporações.

- **Treinamento e Conscientização:** Realizar workshops e treinamentos regulares para funcionários, abordando táticas de engenharia social e como identificar tentativas de manipulação.
- **Políticas de Segurança Rigorosas:** Implementar protocolos claros para a manipulação de dados sensíveis e verificar a identidade em todas as comunicações críticas.
- **Testes de Vulnerabilidade:** Realizar simulações de ataques e auditorias regulares para identificar e corrigir pontos fracos.
- **Controles Técnicos:** Utilizar autenticação multifator (MFA), criptografia de ponta a ponta e monitoramento contínuo de atividades suspeitas.

A combinação dessas práticas contribui para um ambiente mais seguro e resiliente contra ataques de engenharia social.

7. Boas Práticas e Estudos de Caso

Para uma segurança bancária eficaz, é essencial adotar boas práticas baseadas em evidências concretas e estudos de caso bem-sucedidos. A análise de estratégias aplicadas por instituições financeiras de renome demonstra que a implementação de programas contínuos de treinamento e testes de vulnerabilidade pode reduzir drasticamente a exposição a ataques cibernéticos e fraudes.

Exemplos notáveis de aplicação bem-sucedida:

- **BK Bank:** Fundado em 2015, o BK Bank enfrentava uma média de 80 mil tentativas de intrusão fraudulenta a cada 5 minutos. Para mitigar essas ameaças, adotou soluções avançadas de segurança, incluindo o FortiWeb e o FortiGate Next-Generation Firewall, bloqueando eficazmente atividades maliciosas e garantindo conformidade com padrões rigorosos de segurança. (Fonte: Fortinet)
- **Banco BTG Pactual:** Com o objetivo de ampliar a conformidade e segurança, o banco criou um catálogo de dados em um ambiente de data lake, permitindo mapeamento eficiente para identificar e prevenir ataques, como o envenenamento de dados, reforçando a integridade das informações. (Fonte: Security Leaders)
- **Caixa Econômica Federal:** Por meio da solução SecureJourney da Topaz, a Caixa identificou cenários de risco que impactavam seus aplicativos bancários, protegendo a instituição e seus usuários contra perdas financeiras. (Fonte: SiliconWeek)

O estudo aprofundado desses casos e de outros exemplos de sucesso permite não apenas compreender as táticas mais eficazes, mas também adaptar políticas de segurança com base em resultados comprovados. Essas práticas fortalecem a resiliência institucional e promovem uma cultura organizacional de segurança cibernética mais robusta e proativa.

8. Conclusão e Recomendações

A segurança no setor bancário é um desafio contínuo, especialmente diante da evolução das táticas de engenharia social, que exploram a manipulação psicológica para obter informações sensíveis ou acesso não autorizado a sistemas. Essa ameaça crescente exige uma abordagem integrada e proativa, combinando treinamentos frequentes, políticas claras e controles técnicos eficazes.

Recomendações práticas incluem:

- Implementação de treinamentos regulares para todo o quadro de funcionários, enfatizando a identificação e resposta a tentativas de manipulação.
- Revisão periódica das políticas de segurança para garantir sua atualização frente às novas ameaças e práticas recomendadas.
- Uso de tecnologias de autenticação avançada, como autenticação multifator, para dificultar acessos não autorizados.
- Promoção de uma cultura organizacional focada na segurança, incentivando os colaboradores a reportarem comportamentos suspeitos de forma proativa.

Essas medidas, quando aplicadas de forma consistente e abrangente, ajudam a proteger as instituições bancárias de ataques cibernéticos e a preservar a confiança dos clientes, assegurando a integridade dos dados e a continuidade das operações.

9. Referências Bibliográficas

- Mitnick, K., & Simon, W. (2011). "The Art of Deception: Controlling the Human Element of Security." Wiley.
- Hadnagy, C. (2010). "Social Engineering: The Art of Human Hacking." Wiley.
- Granger, S. (2001). "Social Engineering Fundamentals: Part I & II." Symantec Press.
- Mitnick, K., & Vamosi, R. (2017). "The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data." Little, Brown and Company.
- Abagnale, F. (2001). "The Art of the Steal: How to Protect Yourself and Your Business from Fraud, America's #1 Crime." Broadway Books.
- Milgram, S. (1974). "Obedience to Authority: An Experimental View." Harper & Row.
- How A Tech Billionaire's Company Misplaced $46.7 Million And Didn't Know It
- HLTI: Spear Phishing
- Compugraf: Tipos de Engenharia Social
- Keeper Security: Social Engineering Attacks
- Checkpoint: Social Engineering vs Phishing
- Fortinet: BK Bank
- Security Leaders: Banco BTG Pactual
- SiliconWeek: Caixa Econômica Federal