

MÓDULO 2

A mente do fraudador:

Entendendo a engenharia social

A mente do fraudador: Desvendando a engenharia social e
a psicologia por trás dos ataques

Resumo Este artigo se aprofunda no tema da **Engenharia Social**, a tática mais utilizada por criminosos cibernéticos, que explora a natureza humana em vez de falhas técnicas. Analisamos como os fraudadores utilizam gatilhos psicológicos como **pressa, medo e curiosidade** para manipular colaboradores e obter acesso a informações sensíveis ou sistemas. O texto detalha cenários práticos de manipulação em diferentes canais de comunicação (telefone, WhatsApp, e-mail) e enfatiza a regra de ouro para a defesa: **Parar, Pensar e Verificar**. O objetivo é capacitar o colaborador a reconhecer e neutralizar essas ameaças, transformando-o em uma barreira de segurança.

1. Introdução: o elo mais fraco é o humano

A Engenharia Social é definida como a arte de manipular pessoas para que forneçam informações confidenciais ou realizem ações que comprometam a segurança [1]. Em vez de gastar tempo e recursos tentando quebrar a criptografia de um sistema, o fraudador mira no **elo mais fraco**: o ser humano.

Para uma cooperativa de crédito, onde a confiança e o relacionamento interpessoal são pilares, a Engenharia

Social representa um risco exponencial. O criminoso se aproveita da boa vontade, da cortesia e, principalmente, do desejo do colaborador de ser prestativo para contornar as mais sofisticadas defesas tecnológicas.

Este artigo irá desvendar as táticas psicológicas empregadas pelos fraudadores e fornecer ferramentas mentais para que o colaborador possa se proteger e proteger a cooperativa.

2. Como os criminosos usam a psicologia

Os Engenheiros Sociais são mestres em psicologia aplicada. Eles criam narrativas convincentes que exploram fraquezas emocionais e cognitivas,

levando a vítima a agir impulsivamente ou contra seus próprios interesses. Os três gatilhos psicológicos mais explorados são:

2.1. O gatilho da pressa (Urgência)

A urgência é a tática mais comum. O fraudador cria uma situação de **crise imediata** para impedir que a vítima tenha tempo de pensar ou verificar a informação, eles tentam criar uma situação inesperada que em uma condição normal/real, seria de urgência e precisaria da intervenção imediata.

A pressa anula o pensamento crítico da vítima, já que, muitas das vezes, apesar de uma situação genérica ela se encaixa perfeitamente na rotina da pessoa. O objetivo é fazer com que o colaborador reaja por instinto e medo da consequência, ou até mesmo um senso de responsabilidade acima da média.

Vamos analisar alguns exemplos, o primeiro é clássico, "Sua conta será bloqueada em 5 minutos se você não clicar neste link.", muita atenção aqui, pois essa frase muitas das vezes vem com um remetente importante que na verdade é um disfarce, "Seu chefe precisa urgentemente que você transfira este valor para fechar um negócio agora.", geralmente direcionado ao pessoal ou ao e-mail do setor financeiro, "O sistema está fora do ar e preciso da sua senha de acesso para restabelecê-lo imediatamente.", muito comum ser atribuído como um contato do setor de TI, eles nunca dizem de qual sistema,



qual o usuário ou qual a necessidade real, sempre constroem a situação em cima de frases e condições genéricas pois não tem informação interna para construir a narrativa.

2.2. O gatilho do medo (Autoridade e Ameaça)

O conceito de Simulação de Autoridade baseia-se no princípio psicológico da obediência, onde indivíduos tendem a seguir instruções de figuras percebidas como superiores ou legítimas, mesmo que essas instruções sejam questionáveis. O fraudador se apropria de uma identidade de poder como um gerente, auditor, técnico de TI, ou até mesmo um oficial da lei para estabelecer uma falsa legitimidade.

A tática explora a deferência natural que as pessoas têm por posições de poder dentro de uma hierarquia corporativa ou social. Ao se apresentar como alguém que tem o direito de solicitar informações confidenciais ou frase "manutenção de emergência no servidor" adiciona o elemento de urgência. A vítima, ao ouvir sobre uma "emergência" que pode afetar toda a operação, sente-se compelida a cooperar imediatamente, violando o protocolo fundamental de nunca compartilhar senhas.

A Ameaça de Perda ou Punição explora o medo inato de consequências

exigir uma ação imediata, o atacante anula a resistência da vítima. A vítima, temendo as consequências de desobedecer a uma ordem legítima, age rapidamente para cumprir a solicitação, sem realizar a devida verificação.

"Sou do setor de TI e preciso que você me diga sua senha para fazer uma manutenção de emergência no servidor."

Neste cenário, o fraudador se disfarça de um técnico de TI. A escolha dessa figura é estratégica, pois o setor de TI é inherentemente associado à gestão de sistemas críticos e à necessidade de acesso privilegiado. A inclusão da

negativas, sejam elas financeiras, legais ou profissionais.

Esta abordagem manipula a aversão à perda, um viés cognitivo que demonstra que a dor de perder algo é psicologicamente duas vezes mais poderosa do que o prazer de ganhar algo equivalente. O fraudador constrói uma narrativa de crise, como uma violação de segurança, uma dívida

pendente, ou uma infração legal, e se posiciona como a única solução para o problema. A vítima é levada a acreditar que a única maneira de evitar a punição ou a perda é seguir as instruções do atacante, geralmente clicando em um link malicioso ou fornecendo dados pessoais.

"Você violou a política de segurança. Para evitar um processo, clique aqui e preencha o formulário."

A alegação de que a vítima "violou a política de segurança" gera instantaneamente medo de punição. O fraudador, então, oferece uma

"saída" rápida e fácil: "clique aqui e preencha o formulário". Essa ação, apresentada como o caminho para a redenção ou para evitar o desastre, é na verdade o mecanismo de ataque (phishing). O medo sobrepuja a cautela, fazendo com que a vítima ignore o bom senso e os protocolos de segurança.

Em suma, a eficácia dessas táticas reside na capacidade do fraudador de desviar a atenção da vítima do o quê está sendo solicitado para o porquê está sendo solicitado.

2.3. O gatilho da curiosidade (Isca - *Baiting*)

A curiosidade humana é uma poderosa alavanca psicológica que os fraudadores exploram com grande eficácia. Esta tática, frequentemente associada ao baiting (isca), não se baseia na coerção, mas sim na atração, utilizando ofertas tentadoras ou a promessa de acesso a informações inesperadas e privilegiadas para aguçar o interesse da vítima. O objetivo é desviar o foco da vítima de sua cautela habitual, transformando o desejo de saber ou de obter vantagem em um impulso para a ação imediata. O colaborador, movido pela expectativa de recompensa ignora os sinais de alerta

e se expõe ao risco, clicando em links ou abrindo anexos maliciosos.

"Veja as fotos polêmicas da reunião de diretoria."

A promessa de conteúdo "polêmico" cria um senso de exclusividade e urgência, levando a vítima a clicar no link ou anexo para satisfazer o interesse imediato em assuntos internos da empresa.

"Você ganhou um prêmio! Clique aqui para resgatar."

Esta tática apela à ganância e à esperança de uma recompensa inesperada, fazendo com que a vítima ignore a improbabilidade da oferta e siga as instruções para "resgatar" o

prêmio, que geralmente envolve a inserção de dados pessoais ou o download de malware.

"Relatório de bônus salariais para 2025. Abra o anexo."

O assunto, diretamente ligado ao salário e à progressão de carreira, é altamente relevante e sensível. A urgência em acessar dados que impactam diretamente a vida profissional da vítima faz com que ela abra o anexo sem a devida verificação

de segurança, comprometendo o sistema.

A isca (baiting) é uma tática de engenharia social que capitaliza o desejo humano por recompensas ou informações exclusivas.

Ao apresentar uma isca irresistível, o fraudador consegue quebrar as barreiras de segurança da vítima, transformando a curiosidade em um vetor de ataque.

3. Cenários práticos de manipulação no dia a dia

Os ataques de Engenharia Social se manifestam em diversas plataformas, adaptando-se ao canal para maximizar a eficácia da manipulação psicológica

3.1. Telefone (*Vishing*)

O *Vishing* (Phishing por Voz) ocorre quando o fraudador liga para a cooperativa, muitas vezes se passando por um técnico, um colega de outra agência ou até mesmo um cooperado em situação de emergência.



Cenário de Exemplo: Um colaborador recebe uma ligação de alguém que se identifica como técnico de TI e diz: "Estamos com um problema urgente no sistema de acesso remoto e preciso que você me forneça seu login e a senha temporária que enviei por SMS para testar a conexão."

Como o fraudador manipula: Usa o medo de um sistema falhar e a urgência para que o colaborador entregue as credenciais sem questionar.

3.2. WhatsApp e SMS (*Smishing*)

O *Smishing* (Phishing por SMS/Mensagem) utiliza a familiaridade e a informalidade do WhatsApp ou SMS. Como essas plataformas são usadas para comunicação pessoal, as pessoas tendem a baixar a guarda.

Cenário de Exemplo: Um colaborador recebe uma mensagem no WhatsApp do número de um gerente conhecido, que diz: "Meu

celular quebrou e estou usando um provisório. Preciso que você me envie o número do seu token de segurança para eu conseguir acessar o sistema e aprovar um pagamento urgente."

Como o fraudador manipula: Explora a confiança na figura do gerente e a pressa de resolver um problema "urgente" para obter o código de segurança.

3.3. E-mail (*Phishing*)

O *Phishing* por e-mail é o mais clássico e ainda o mais eficaz. O fraudador envia e-mails que imitam comunicações internas, de bancos ou de serviços conhecidos, com o objetivo de roubar credenciais ou instalar malware.

Cenário de Exemplo: Um e-mail que parece ser do RH da cooperativa, com o assunto "Atualização Obrigatória do Sistema de Holerite". O e-mail contém um link que solicita o login e a senha do colaborador para "confirmar a identidade".

Como o fraudador manipula: Usa a autoridade do RH e a urgência de uma "Atualização Obrigatória" para levar o

colaborador a inserir suas credenciais em um site falso (página de *login* clonada).

4. O escudo contra a manipulação: Parar, Pensar e Verificar

A defesa mais eficaz contra a Engenharia Social é um processo mental simples, mas rigoroso, que

deve ser aplicado a toda e qualquer comunicação suspeita: **Parar, Pensar e Verificar.**

Ação	O Que Fazer	Por que Funciona?
Parar	Não aja imediatamente. Respire. Não clique em nada, não responda e não forneça nenhuma informação.	Quebra o ciclo de urgência e medo criado pelo fraudador, permitindo o retorno ao pensamento racional.
Pensar	Pergunte-se: <i>Essa comunicação faz sentido? Eu estava esperando por isso? O tom da mensagem é normal? O que a pessoa está pedindo viola alguma política de segurança?</i>	O pensamento crítico expõe as inconsistências na narrativa do fraudador (ex: um gerente nunca pediria um token por WhatsApp).
Verificar	Use um canal de comunicação diferente do que foi usado para o contato suspeito. Ligue para o número oficial do gerente ou envie um e-mail para o TI. Nunca responda ao e-mail ou número suspeito.	Confirma a legitimidade do pedido. Se for uma ligação, desligue e ligue de volta para o número oficial da pessoa ou setor.

Estudo de Caso Prático: A Transferência Rejeitada Um colaborador de uma cooperativa recebeu um e-mail urgente, supostamente do CEO, solicitando uma transferência imediata para um fornecedor. O colaborador *Parou* e *Pensou*: "O CEO nunca me pediria

isso por e-mail, e o e-mail dele parece estranho." Ele *Verificou* ligando para a secretária do CEO no ramal interno. A secretária confirmou que o CEO não havia enviado o e-mail, e o ataque foi neutralizado antes que qualquer perda financeira ocorresse.

5. Conclusão

A Engenharia Social é uma ameaça persistente porque explora a confiança, uma virtude fundamental no cooperativismo. No entanto, o conhecimento das táticas psicológicas e a aplicação rigorosa da regra **Parar, Pensar e Verificar** transformam o colaborador de alvo em um ativo de segurança. Ao entender a mente do fraudador, cada membro da cooperativa se torna um agente ativo na proteção da organização e, consequentemente, na manutenção da confiança dos cooperados.

Referências Bibliográficas

- [1] Rastek Soluções. **Engenharia social: como proteger sua empresa e colaboradores.** Disponível em: <https://rasteksolucoes.com.br/2023/01/engenharia-social-como-proteger-sua-empresa-e-colaboradores/>
- [2] MundoCoop. **Guerra invisível: saiba como as cooperativas enfrentam a ameaça cibernética.** Disponível em: <https://mundocoop.com.br/destaque/guerra-invisivel-saiba-como-as-cooperativas-enfrentam-a-ameaca-cibernetica/>
- [3] (Adicionar referências adicionais conforme aprofundamento da pesquisa, se necessário).