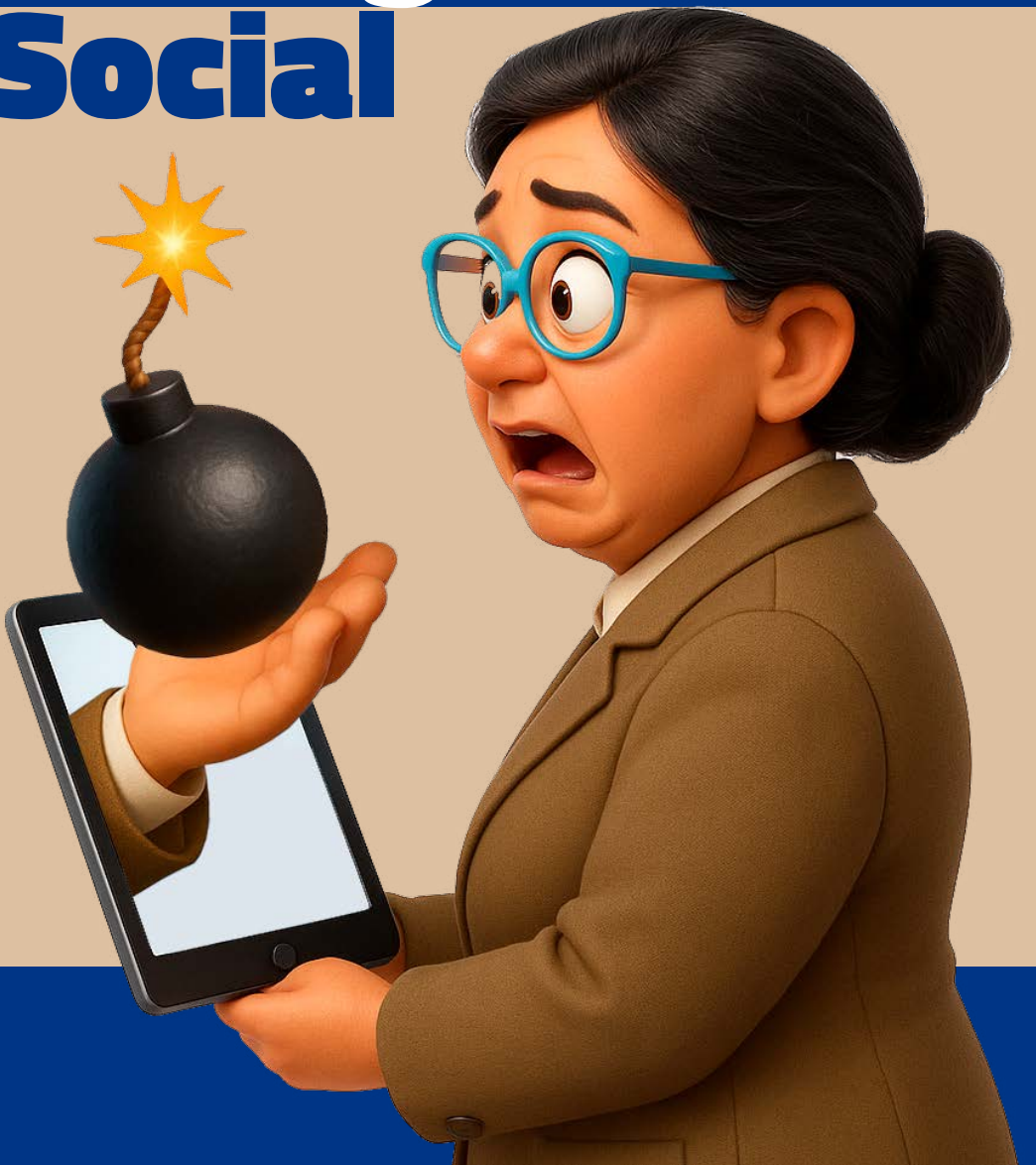
Cartilha Interativa de Engenharia Social



Introdução

Proteja-se e proteja sua instituição contra ataques de engenharia social.

A engenharia social representa uma das principais ameaças à segurança da informação no ambiente judiciário. Diferentemente dos ataques puramente tecnológicos, essas técnicas exploram o fator humano, aproveitando-se da confiança, da boa-fé e da disposição natural das pessoas em ajudar.

No contexto do Poder Judiciário, onde circulam informações sensíveis e decisões que afetam direitos fundamentais, a proteção contra esses ataques é essencial para preservar a integridade, a confiabilidade e a imagem do sistema de justiça.

O que é Engenharia Social?

Conjunto de técnicas de manipulação psicológica usadas por criminosos para enganar pessoas e obter informações confidenciais, acesso a sistemas ou ações indevidas.

A engenharia social explora fatores psicológicos humanos como:

- **Confiança:** Criminosos se passam por colegas, autoridades ou instituições confiáveis
- **Medo:** Criam situações de ameaça para pressionar decisões precipitadas
- **Urgência:** Impõem prazos apertados para impedir reflexão crítica
- **Autoridade:** Fingem representar figuras de poder ou órgãos institucionais
- **Reciprocidade:** Oferecem “favores” para criar obrigação moral
- **Validação Social:** Alegam que “outros já fizeram” para normalizar a ação

O que caracteriza principalmente a engenharia social?

Manipulação psicológica para obter informações confidenciais

Ataques técnicos avançados para invadir sistemas

Invasão física às instalações para roubar equipamentos

Fundamentos da Segurança da Informação

Os três pilares fundamentais da segurança da informação são:

- **Confidencialidade:** Acesso apenas por pessoas autorizadas
- **Integridade:** Dados não podem ser alterados indevidamente
- **Disponibilidade:** Acesso garantido quando necessário

Proteção de dados não é apenas uma questão técnica, mas também comportamental. Seus hábitos diários importam!

Principais Técnicas de Engenharia Social

1. Phishing (Isca Digital)

Mensagens falsas simulando comunicações legítimas, usadas para roubar credenciais ou instalar malware.

Exemplo no TJPA:

Assunto: Atualização Urgente - Sistema PJe

Prezado(a) Servidor(a),

O sistema PJe passará por manutenção emergencial. Para evitar interrupções, clique no link abaixo e confirme suas credenciais até as 18h de hoje.

[Link malicioso]

Atenciosamente, Suporte Técnico PJe

2. Vishing (Voice Phishing)

Golpes por telefone com criminosos se passando por funcionários de instituições.

Exemplo bancário:

"Olá, aqui é João da Central de Segurança do Banco XYZ. Detectamos movimentações suspeitas em sua conta. Pode me informar os últimos quatro dígitos do seu cartão para confirmar a titularidade?"

Exemplo no Judiciário:

"Bom dia, aqui é da Corregedoria. Estamos auditando acessos ao sistema. Preciso que o(a) senhor(a) confirme seu login e senha para verificar possíveis irregularidades."

3. Smishing (SMS ou WhatsApp)

Mensagens de texto com links maliciosos ou pedidos urgentes.

Exemplo:

TJPA - Sua conta será bloqueada em 2h por acesso irregular. Regularize em: [link]. Código: TJ2025

4. Pretexting (Criação de Cenários)

Situações falsas e convincentes para extrair informações.

Exemplo:

"Doutor, sou Dr. Silva, OAB 12345. Tenho audiência urgente hoje e perdi meus dados do sistema. Pode me ajudar com o login? É um habeas corpus muito importante."

5. Baiting (Isca Física)

Uso de dispositivos infectados para comprometer sistemas.

Exemplos:

- Pen drives deixados no estacionamento do tribunal
- CDs com títulos como "Jurisprudência Atualizada 2025"

6. Quid Pro Quo (Troca de Favores)

Ofertas de ajuda em troca de acesso ou dados.

Exemplo:

"Sou do suporte técnico. Estamos atualizando os antivírus. Posso fazer a instalação remota? Só preciso de seu usuário e senha."

7. Tailgating / Piggybacking (Carona Física)

Acesso indevido a áreas restritas ao acompanhar pessoas autorizadas.

Exemplos:

- Alguém vestido de técnico espera para entrar com um servidor
- Pessoa se passa por entregador e solicita acompanhamento até área interna

8. Shoulder Surfing (Bisbilhotagem)

Observação discreta de senhas ou dados sensíveis.

Exemplos:

- Espiar a digitação de senhas em elevadores ou cafés
- Uso de câmeras ou ângulos estratégicos para capturar telas

Cenários Específicos do Ambiente Judicial

E-mails Institucionais Fraudulentos

- **Situação 1: Falsa Comunicação da Corregedoria**

Assunto: Processo Disciplinar - Resposta Obrigatória

Foi aberto processo administrativo contra você. Para evitar suspensão, acesse o link abaixo e apresente defesa em 24h.

[Link malicioso]

- **Situação 2: Suposta Atualização de Sistema**

Assunto: Nova Versão do SEEU - Instalação Obrigatória

O sistema SEEU será descontinuado. Baixe a nova versão no anexo e instale hoje para não comprometer seu acesso.

[Anexo com malware]

- **Situação 3: Falso Comunicado sobre Benefícios**

Assunto: Gratificação Especial - Cadastro Necessário

Foi aprovada gratificação de R$ 2.000 para servidores. Cadastre-se no link abaixo informando CPF, conta bancária e código de segurança.

[Link malicioso]

Ligações de Supostos Agentes Bancários

- **Cenário 1: Urgência Falsa**

"Detectamos tentativa de empréstimo em seu nome. Para bloquear, informe o código do seu token agora."

- **Cenário 2: Oferta Irresistível**

"Servidor público pré-aprovado para cartão sem anuidade e limite de R$ 50 mil. Qual sua renda líquida?"

- **Cenário 3: Problema com PIX**

"Seu CPF foi usado em transações suspeitas. Para proteger, preciso da senha para reativar seu PIX."

Mensagens de Texto (SMS/ WhatsApp)

- **Exemplo 1: Problemas com CPF**

RECEITA FEDERAL: Seu CPF foi suspenso por irregularidades. Regularize em 6h: [link].

- **Exemplo 2: Suposto Benefício**

GOVERNO FEDERAL: Você tem direito ao Auxílio Servidor 2025 – R$ 1.200. Solicite hoje: [link].

- **Exemplo 3: Entrega Fraudulenta**

CORREIOS: Encomenda retida. Taxa de R$ 8,50 para liberação: [link]. *Código: BR123456789.*

Ataques Direcionados a Magistrados

- **Situação 1: Falso Assessor**

"Sou o novo assessor do Desembargador Silva. Ele precisa da sua análise urgente. Pode me passar seu e-mail e senha para encaminhar os autos?"

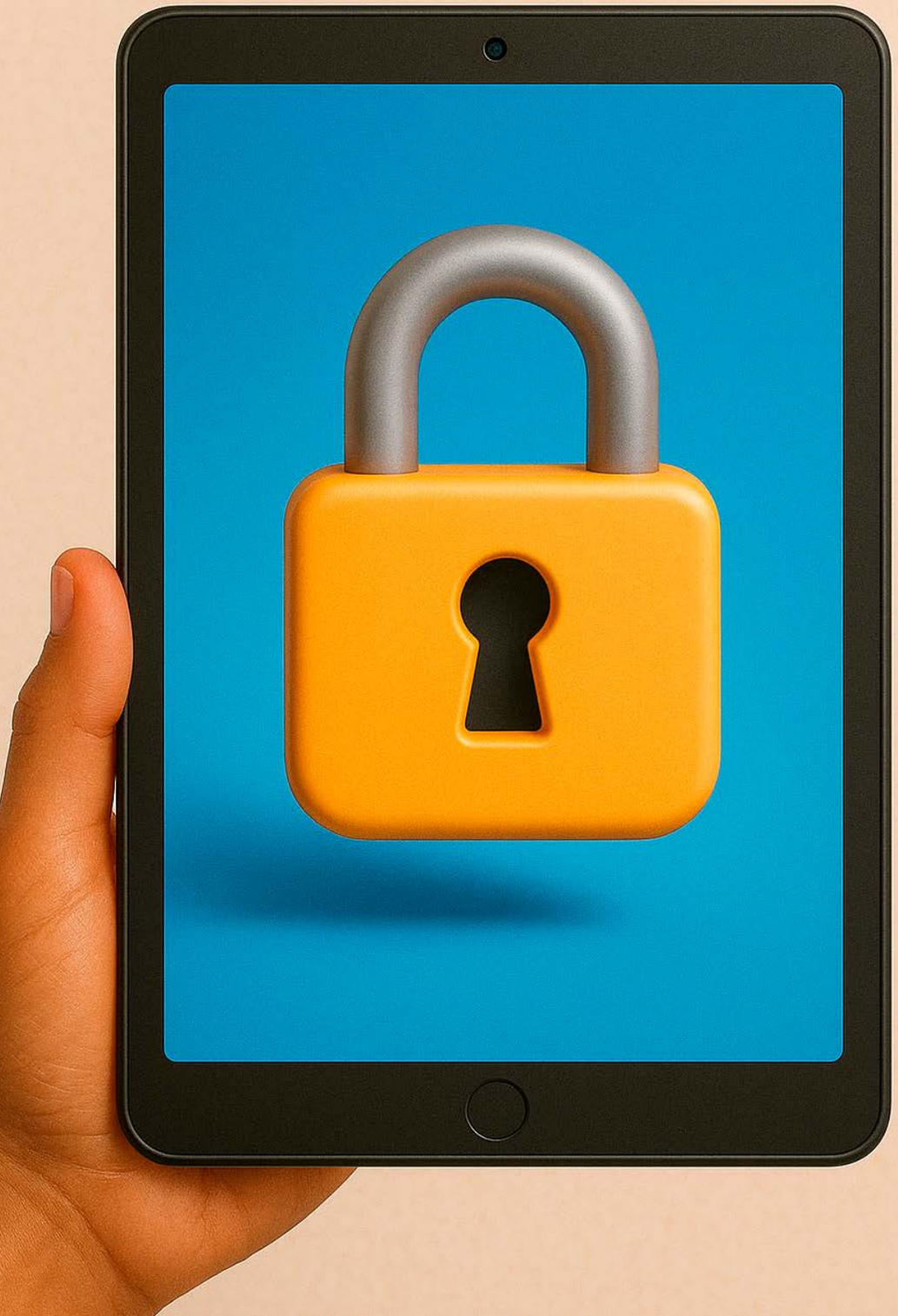
- **Situação 2: Suposto Colega**

"Sou o Juiz Antônio da 2ª Vara. Preciso consultar o processo XYZ para decisão liminar. Pode acessar e me enviar a petição inicial?"

Ciclo de um Golpe de Engenharia Social

1. **Coleta de Informações:** O atacante (golpista) pesquisa dados em redes sociais, sites corporativos e outras fontes públicas
2. **Criação de Vínculo:** Estabelece contato usando identidade falsa com base nos dados coletados
3. **Exploração da Relação:** Induz a vítima a entregar dados sensíveis ou clicar em links maliciosos
4. **Execução da Fraude:** Usa as informações obtidas para acessar sistemas, dados ou contas bancárias

Cuidado com informações que você compartilha publicamente! Um atacante (golpista) pode montar um perfil detalhado sobre você a partir de posts em redes sociais.



Sinais de Alerta e Prevenção

Sinais de Alerta

- Urgência excessiva
- Links estranhos ou com erros de ortografia no endereço
- Erros ortográficos e gramaticais no texto
- Ameaças ou pressão psicológica
- Pedidos fora do comum ou de informações sensíveis
- E-mails genéricos (“Prezado cliente”) são sinal de alerta

Estratégias de Proteção

1. Verificação Contínua

- Nunca forneça dados pessoais, bancários ou senhas por telefone, e-mail ou mensagem
- Confirme a identidade por canais oficiais
- Desconfie de urgência excessiva — instituições sérias não pressionam por decisões imediatas
- Verifique links e e-mails antes de clicar ou abrir anexos

2. Análise Crítica

- Questione propostas excessivamente vantajosas
- Fique atento a erros gramaticais em mensagens oficiais
- E-mails genéricos (“Prezado cliente”) são sinal de alerta
- Verifique cuidadosamente o endereço de e-mail do remetente

3. Proteção de Informações

- Evite divulgar dados funcionais em redes sociais
- Não poste fotos com documentos, telas ou crachás visíveis
- Evite responder pesquisas telefônicas ou online sobre trabalho
- Proteja conversas confidenciais em locais públicos

Checklist de Segurança

- Verifique cuidadosamente o endereço de e-mail do remetente
- Nunca compartilhe senhas, mesmo com suporte técnico
- Use autenticação em duas etapas em todas as contas importantes
- Instale aplicativos apenas de fontes oficiais e confiáveis
- Confirme solicitações suspeitas por canais alternativos (telefone oficial)
- Bloqueie seu computador sempre que se ausentar da estação de trabalho
- Atualize suas senhas regularmente e use gerenciador de senhas

Segurança no Setor Público

Medidas essenciais para instituições públicas:

- Política de senhas robusta e atualizada regularmente
- Monitoramento constante de acessos e atividades suspeitas
- Treinamentos regulares para todos os servidores (Educação e treinamento contínuo)
- Canal dedicado para reportar incidentes de segurança
- Classificação adequada das informações por nível de sigilo
- Implementação de políticas de segurança
- Monitoramento e resposta a incidentes

Cuidado com informações que você compartilha publicamente! Um atacante (golpista) pode montar um perfil detalhado sobre você a partir de posts em redes sociais.

Base Legal

- Súmula 479 do STJ;
- Código de Defesa do Consumidor - CDC (Lei nº 8.078/1990);
- Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018);
- Lei de Acesso à Informação - LAI (Lei nº 12.527/2011).

Responsabilidade do Servidor:

Servidores públicos podem responder administrativa, civil e até penalmente por negligência na proteção de dados sob sua guarda (Arts. 23, 26 e 42 da Lei Geral de Proteção de Dados - Lei 13.709/2018).

Recomendações Finais:

- Utilize autenticação multifator (MFA) nos sistemas disponíveis
- Em caso de dúvida, contate o suporte institucional ou a Ouvidoria
- Lembre-se: o compartilhamento indevido de dados pode violar a Lei Geral de Proteção de Dados (LGPD)

Para saber mais

Cultura de Prevenção

Saiba Mais:

- Cartilha de Segurança da Informação (CNJ)
- Guias, Folderes e Cartilhas da Agência Brasileira de Inteligência
- Curso Básico de Segurança Cibernética - Unidade 03: Golpes Digitais (EJPA/TJPA)

Referências

- LOTUFO, Larissa. Engenharia Social. In: SLEIMAN, Cristina et al. Segurança digital: proteção de dados nas empresas. Organização: Patricia Peck Pinheiro. São Paulo: Atlas, 2021. Cap. 7, p. 96-101.
- MITNICK, Kevin D.; SIMON, William L. A arte de enganar: controlando o fator humano na segurança da informação. Tradução de Kátia Aparecida Roque. Revisão técnica de Olavo José Anchieschi Gomes. São Paulo: Pearson Education do Brasil, 2003.

Esta cartilha é produto do Projeto Cartilhas Interativas de Prevenção à Engenharia Social, institucionalizado pela Portaria n.º 4487/2025-GP, de 23 de setembro de 2025, e executado pela Corregedoria-Geral de Justiça, em parceria com a Presidência do TJPA, sob a Coordenação-Geral da Exma. Desa. Elvina Gemaque Taveira, Corregedora-Geral de Justiça.

Conteúdo:
Dilcele Fernandes de Oliveira Pother Furtado

Revisão Técnica:
Monique Soares Leite

Departamento de Comunicação / Coordenadoria de Imprensa
Edição de arte:
Airton Nascimento


TRIBUNAL DE JUSTIÇA
DO
ESTADO DO PARÁ
1874
NON SIBI
AD JUSTITIA
SEMPER FIDELIS