

Não caia na armadilha da Engenharia Social



Neste informativo, você entenderá **como golpistas utilizam a Engenharia Social** para induzir decisões precipitadas, entender o que o Banco Paulista nunca solicita e saber **como agir em caso de suspeita**.





O que é Engenharia Social?

A sua segurança é **prioridade** para o Banco Paulista.

Mais do que um golpe técnico, a Engenharia Social é uma **manipulação psicológica**. O golpista não invade o sistema, ele tenta convencer você a entregar as chaves.

Se alguém solicitar qualquer um dos itens abaixo, **desligue imediatamente**:

- **Solicitação de Senhas ou Tokens:** Nunca pedimos sua senha silábica, numérica ou códigos enviados por SMS/Push.
- **Acesso Remoto:** Nunca pediremos para você baixar aplicativos como AnyDesk ou TeamViewer para "limpar" seu celular.
- **Transferências de Teste:** Nunca solicitamos que você faça uma TED para "testar" o sistema ou estornar um valor.

Não caia na armadilha da Engenharia Social

Como os golpistas manipulam suas emoções?



Os criminosos utilizam "**gatilhos**" para fazer você **agir sem pensar**. Fique atento se a mensagem ou ligação causar:

- **Senso de Urgência Extrema:** "Sua conta será bloqueada agora", "Detectamos uma invasão" ou "Você tem 5 minutos para confirmar". O objetivo é gerar pânico para que você não raciocine.
- **Autoridade Falsa:** Eles se identificam como "Gerente de Segurança", "Setor de Fraudes" ou até policiais, usando termos técnicos para parecerem legítimos.
- **Falsa Cortesia ou Benefício:** Promessas de prêmios ou aumento de limite imediato.
- **O Golpe da "Conta Segura":** Um dos mais comuns hoje. Dizem que sua conta está em risco e que você deve transferir seu dinheiro para uma "conta de segurança" temporária. Isso não existe.

Checklist de Proteção Ativa

Para se manter seguro no dia a dia, **adote estes hábitos:**

- 01. Desconfie do Identificador de Chamadas:** Criminosos podem mascarar o número de telefone para que apareça o número real do banco no seu visor (técnica de spoofing). Se tiver dúvida, desligue e ligue você para o número oficial do Banco Paulista.
- 02. Cuidado com Redes Wi-Fi Públicas:** Evite acessar o aplicativo do banco em redes de aeroportos, shoppings ou cafés. Use sempre os dados móveis (4G/5G).
- 03. Verifique Links Encurtados:** Antes de clicar, use sites de expansão de links ou observe se o endereço final é realmente o domínio oficial do Banco Paulista.
- 04. O "Minuto de Silêncio":** Antes de realizar qualquer ação solicitada por telefone ou mensagem, respire e espere um minuto. Quase todos os golpes de engenharia social falham se a vítima parar para pensar por 60 segundos.



Suspeitou de algo? Saiba como agir:

Se você percebeu que compartilhou informações ou realizou uma transação suspeita:

- 1. Encerre o contato** imediatamente.
- 2. Acesse o App Oficial** e utilize o chat para relatar o ocorrido.
- 3. Altere suas senhas** de acesso e de transações imediatamente através de um dispositivo seguro.

Canais de Atendimento

Ouvidoria: 0800 772 6116
ouvidoria@bancopaulista.com.br
De segunda a sexta-feira, das 9h às 18h.