

Proteja-se contra o Phishing



Neste informativo, você encontrará **orientações práticas** para **identificar tentativas de golpe**, entender o que o Banco Paulista nunca solicita e **saber como agir rapidamente** em caso de suspeita.





O que é Phishing?

O Phishing é uma técnica de "pesca" digital. Criminosos enviam **mensagens falsas** para fisgar seus dados bancários, senhas ou induzir a instalação de vírus.

Eles **se passam por instituições de confiança** para ganhar sua atenção através do medo ou da curiosidade.

Para sua segurança, tenha em mente que nossa política de comunicação **é rigorosa**:

- **Não solicitamos senhas**, códigos de token por telefone, SMS ou WhatsApp.
- **Não enviamos links diretos** para páginas de login ou sincronização de dispositivos.
- **Não pedimos para baixar arquivos** (.exe, .zip, .pdf com senha) para "atualizar" o sistema de segurança.

Como identificar uma mensagem suspeita?



Os golpistas estão cada vez mais sofisticados, mas a **maioria** comete **estes erros**:

- **Urgência Artificial:** Mensagens que exigem ação imediata (ex: "Sua conta será bloqueada em 30 minutos" ou "Multa pendente detectada"). O objetivo é impedir que você pense com calma.
- **Links Mascaraados:** O texto do link diz uma coisa, mas o destino é outro. Sempre passe o mouse (ou pressione levemente no celular) sobre o link para ver o endereço real.
- **Saudações Genéricas:** Em vez do seu nome, usam termos como "Prezado Cliente" ou "Usuário do Sistema".
- **Erros de Escrita:** Fique atento a letras trocadas, falta de acentuação ou logotipos com baixa resolução e cores levemente alteradas.

Checklist de Proteção Ativa

Se receber qualquer comunicação duvidosa, **siga estes passos:**

- 01. Desconfie do Remetente:** Verifique se o e-mail possui um domínio oficial (ex: @bancopaulista.com.br) e não um genérico como @gmail.com ou @outlook.com.
- 02. Não use o "Atendimento" sugerido:** Se a mensagem pede para ligar em um número 0800, não ligue. Use apenas os números que constam no site oficial.
- 03. Princípio da Navegação Direta:** Nunca clique em links. Se quiser verificar sua conta, feche a mensagem e abra manualmente o aplicativo ou digite o endereço do banco no navegador.
- 04. Autenticação em Duas Etapas (2FA):** Ative-a em todos os seus aplicativos (WhatsApp, E-mail e Redes Sociais). Isso cria uma barreira extra mesmo que sua senha seja roubada.

Suspeitou de algo ou foi vítima?

Não hesite. O tempo é crucial em casos de fraude:

- **Bloqueie o remetente** imediatamente.
- **Não compartilhe** a mensagem para "avisar amigos"; isso pode espalhar o link malicioso.
- **Fale conosco:** Se chegou a inserir dados em um site suspeito, entre em contato pelo chat ou ligue para nossa Central.

Canais de Atendimento

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