PortoBank

# Dicas de combate a fraudes

Com toda certeza você conhece ou já foi vítima de algum golpe financeiro, certo? Segundo a pesquisa, cerca de 20% da população brasileira já foi vítima de algum golpe financeiro somente no último ano, conforme relatório da BioCath.

Pensando nisso, conheça os golpes mais comuns e as principais dicas para se proteger:

**Boleto falso:** Fraudadores realizam o envio de boletos alterados se passando pela Porto por meio de e-mails, links e/ou WhatsApp.

Fique atento se:

• O código de barra apresentar divergências como numeração diferente do habitual (no caso de cartão de crédito Porto a numeração deve ser iniciar com 39994.08580.), valor e data de vencimento;

• Confira se o nome do beneficiário e CNPJ estão corretos, e se o boleto foi recebido por canal oficial da Porto;

**Golpe do PIX:** Dado o crescimento de transações realizadas via PIX aqui estão algumas dicas práticas para usar o PIX, de forma mais segura:

**1. Cuidado com Links e Mensagens Suspeitas**

• Não clique em links enviados por desconhecidos: Criminosos podem se passar por empresas confiáveis para roubar seus dados.

• Verifique mensagens que pedem dados pessoais ou senhas: Instituições financeiras não solicitam informações confidenciais por WhatsApp, SMS ou e-mail.

**2. Atenção ao Registrar e Confirmar Chaves PIX**

• Cadastre suas chaves apenas no app oficial Porto: Nunca compartilhe dados como CPF, e-mail ou número de celular em sites ou aplicativos desconhecidos.

• Confira os dados do destinatário antes de confirmar uma transferência: Evite erros ao enviar dinheiro.

**PISHING:** É o envio de mensagens eletrônicas com o intuito de obter dados pessoais. As mensagens podem ser recebidas por e-mail, WhatsApp, redes sociais, dentre outros canais. Dentre o conteúdo da mensagem, há a inserção de um link fraudulento que uma vez clicado realiza a coleta informações como por exemplo: senhas bancárias, número de cartões de crédito até a instalação de programas espiões como spyware.

As dicas abaixo, te ajudam a se prevenir desta prática:

• Fique atento ao receber mensagens de empresas contendo links suspeitos ou não estando relacionado ao site oficial da Porto;
• Mensagens com erros gramaticais e/ou ortográficos;
• Mensagens com ações imediatas e urgentes;
• Realize atualizações periódicas em seu antivírus, firewall e antispyware, e os mantenha sempre ativos;
• Nunca forneça dados pessoais na criação da senha, sempre utilize dados que não estejam vinculados a você;
• Nunca forneça seus dados pessoais a desconhecidos ou links suspeitos;
• Desconfie das extensões ".exe", ".scr" e ".zip", pois podem ser programas espiões;

**Golpe da Central de Atendimento:** Fraudadores realizam contato com clientes fazendo se passar por funcionários da Porto, com intuito de enganar as vítimas e obter informações confidenciais como senhas e dados bancários. Esta prática tem crescido bastante nos últimos anos, devido ao crescimento de transações digitais.

Fique atento se:

• O contato ocorre de forma inesperada, com urgência e em tom ameaçador;
• Caso o contato ocorra por mensagem, evite interagir. Entre em contato apenas pelos canais oficiais da Porto;

• Não clique em links enviados por números desconhecidos;
• Não compartilhe e nem confirme informações pessoais ou senhas;

**Consórcio:** Desconfie sempre de propostas que ofereçam benefícios fora do padrão, como contemplações garantidas.

Fique atento, e:

• Proteja Suas Informações Pessoais: nunca compartilhe dados pessoais ou financeiros com terceiros não autorizados;
• Desconfie de contatos por telefone, e-mail ou redes sociais solicitando informações sigilosas;
• Use senhas fortes e evite senhas relacionadas a datas ou informações fáceis de deduzir;
• Evite Pagamentos não autorizados e realize pagamentos apenas por meio das plataformas oficiais da administradora;
• Verifique boletos antes de efetuar pagamentos: confira CNPJ, razão social e dados bancários;
• Não aceite intermediários ou terceiros para realizar pagamentos;
• Fique Atento a contatos suspeitos: cuidado com ligações ou mensagens prometendo vantagens, contemplações imediatas ou descontos exclusivos;
• Certifique-se de que qualquer contato seja feito por canais oficiais da administradora;
• Relate contatos suspeitos à administradora para evitar possíveis fraudes;
• Acompanhe Regularmente Seu Consórcio: Monitore seu extrato de pagamento e a situação de sua cota frequentemente. Acesse nosso App ou Portal de Clientes;
• Atualize seus dados cadastrais apenas nos canais oficiais;
• Guarde todos os comprovantes de pagamento e contratos;

**Golpe de Empréstimos e Financiamentos:** No caso de empréstimos e financiamentos, os golpistas utilizam táticas como ofertas em redes sociais, sites falsos, e-mails e WhatsApp. As condições apresentadas costumam ser diferenciadas e muito atrativas, mas é exigido o pagamento antecipado de algumas parcelas.

Após receber o valor solicitado, o golpista desaparece, e o crédito ou financiamento nunca é disponibilizado na conta da vítima.

Para se precaver de golpes, fique atento:

• Desconfie de anúncios atrativos: taxas de juros muito atrativas e condições muito facilitadas;
• Solicitação de pagamento antecipado de parcelas, sempre entre em contato com os canais oficiais da Porto;
• Nunca click em link enviado por terceiros solicitando a captura de selfie, o link sempre será enviado pela Porto;
• Nunca realize a captura de selfie se um terceiro informar que é necessário para cancelamento da operação, a selfie solicitada sempre será para contratação do produto e não para cancelar, e o envio será realizado pela Porto, para cancelamento entre em contato com os nossos canais oficiais;
• Em caso de negociação de dívida, mesmo sendo com Assessorias parceiras, o boleto será emitido e o beneficiário do pagamento é o CNPJ da Porto, nunca será em nome de PF ou em nome de qualquer outra instituição, fique atento ao beneficiário antes de confirmar o pagamento.

**Todo cuidado é Porto.**