

**Cartilha de segurança
para evitar fraudes:**
Boletos Falsos

TRAMONTINA

01

Objetivos da cartilha

A proteção de dados é uma prioridade na Tramontina, sendo investido fortemente em segurança da informação e uso de boas práticas técnicas e administrativas para evitar qualquer tipo de acesso ou uso indevido de nossos bancos de dados.

Seguindo este propósito de contribuir com a segurança de nossos clientes, fornecedores e parceiros, a Tramontina elaborou esta cartilha com **dicas e cuidados de segurança para evitar golpes com boletos falsos**.



02

Como ocorre a falsificação dos boletos?

Existem várias maneiras, dentre as principais, destaca-se:

1. Utilização de vírus no computador que modificam a linha digitável do código de barras do boleto (bolwares). Estes vírus podem estar em arquivos baixados nos dispositivos, e agem usualmente no momento da impressão do documento.

2. Manipulação da linha digitável do código de barras e envio através de correspondência, aplicativos de mensagens, SMS ou e-mail.

3. Criação de páginas fraudulentas na internet, que induzem o indivíduo a erro sobre o pagamento, por exemplo propagandas adulteradas e atrativas aos usuários.

03

Cuidados antes de pagar um boleto



1. Remetente do e-mail

Se receber o boleto via e-mail, você deve **sempre conferir o nome do remetente** (@tramontina.com). Caso não seja este o remetente, fale imediatamente com o seu contato na Tramontina ou com a equipe DPO através do e-mail dpo@tramontina.com ou via chamado juntamente com nosso SAC via link: <https://institucionaltramontina.zendesk.com/hc/pt-br/requests/new>.

2. Logotipo do banco

Confirme a logotipo com o nome do banco emissor, devem ser iguais.

3. Últimos dígitos

Confira os últimos dígitos do código de barras – estes correspondem ao valor a ser pago.

4. Código do banco

Verifique se **os primeiros dígitos do código de barras** correspondem efetivamente ao **código do banco** emissor do boleto. A consulta a estes códigos pode ser feita através do site da FEBRABAN (<http://buscabanco.com.br/>).

5. Dados do beneficiário/ titular da conta

Verifique se o CNPJ ou CPF **corresponde efetivamente aos dados do beneficiário**, além de checar o valor e a data de vencimento. Independentemente da forma de pagamento, **estas informações são apresentadas antes de completar a transação.**

03

Cuidados antes de pagar um boleto



6. Formato do boleto

Solicitar que o envio do boleto ocorra através do formato PDF também minimiza os riscos de sofrer o golpe, já que, desta forma, a adulteração é mais difícil de ocorrer.

7. Usar leitura automática do código de barras

É recomendável realizar o pagamento por meio da leitura automática do código de barras. Nos boletos falsos, em regra, ***não há compatibilidade entre a linha digitável e o código de barras, o que força a vítima a digitar manualmente a sequência*** – a qual foi adulterada. Verifique cuidadosamente os dados do documento caso haja dificuldades na hora da leitura do código.

8. Antivírus

Mantenha sempre um antivírus atualizado no computador, evitando assim um possível bolware.

9. WI-FI

Evite utilizar wi-fi público ao realizar o download de boletos, as quais são mais propensos a ataques e, assim, possíveis falsificações.

10. Emissão ou remissão do boleto

Prefira realizar a emissão do boleto diretamente no site ou aplicativo da empresa, ao invés de acessar links enviados por e-mail.

11. Descontos e promoções

Fique atento a promoções ou descontos inesperados.

Na dúvida, ligue para o seu contato na Tramontina e confirme o valor e demais dados do documento.

04

Dicas para evitar golpes

1. Mensagens com links

Se receber mensagens via e-mail, WhatsApp ou mensagem de texto, contendo **links para fornecimento de dados pessoais certifique-se com o contato daquela instituição se realmente há a necessidade de fornecimento ou confirmação dessas informações. Fique atento! A maioria dos golpes acontece desta forma.**

2. Cuidado com ligações

Lembre-se que bancos, instituições financeiras ou empresas no geral **não entram em contato para alteração de cadastro ou solicitação de dados pessoais**. Se você receber um telefonema não solicitado do seu banco ou outra empresa pedindo dados, nunca revele sua senha, detalhes de login, números de conta ou dados pessoais.

3. Senhas

Cuide e armazene com segurança suas senhas; Troque-as periodicamente; Use senhas difíceis e não anote ou salve senhas em cadernos, arquivos, no celular ou no próprio navegador.

4. Autenticação de duplo fator

Ative a verificação em duas etapas nas contas que oferecem esse recurso, caso ainda não tenha feito

5. Ao realizar um pagamento

Suspeite de informações divergentes, erros de digitação e dificuldades na leitura do código de barras dos boletos bancários. **Qualquer suspeita, avise à sua instituição financeira.**

6. Cadastros e fornecimento de dados

Ao preencher cadastros questione-se sobre a real necessidade de fornecer todos os dados e da instituição retê-los.

7. Descarte de documentos

Não jogue fora nada com seu nome, endereço ou detalhes financeiros sem destruí-lo primeiro, de modo a impossibilitar eventual leitura e coleta de seus dados pessoais e financeiros.

05

Passo a passo após a descoberta do golpe

1. Denuncie o golpe

Sempre que você ou sua empresa for vítima de golpe, o primeiro passo será sempre procurar a polícia civil para registrar um boletim de ocorrência com urgência, o que pode ser feito inclusive de forma online. Em algumas localidades, principalmente nas capitais, existem delegacias especializadas em crimes cibernéticos.

2. Avise a sua instituição financeira

Entre em contato direto com a instituição financeira para verificar a possibilidade de ressarcimento de eventuais valores objetos da fraude. Caso não tenha sucesso no contato direto com a sua instituição financeira, você poderá entrar em contato direto com o Banco Central (https://www.bcb.gov.br/acessoinformacao/registrar_reclamacao).

3. Avise a instituição financeira de destino dos valores

O aviso à instituição financeira para onde os seus valores foram enviados poderá auxiliar na tentativa de localizar a procedência do golpe, e eventualmente bloquear valores remanescentes da conta.

06

Dúvidas e contato DPO

Em caso de dúvidas acerca desta cartilha, você pode entrar em contato com a equipe do DPO através do e-mail: dpo@tramontina.com.

É dever de todos colaborar com a nova **cultura de proteção de dados**.



TRAMONTINA

o prazer
de fazer bonito