Conheça os principais golpes e fique atento:

Boletos Falsos e golpe do DDA:

Antes de pagar um boleto, confirme os dados do beneficiário. Se houver divergências, não pague e contate o emissor. Nunca emita segunda via em site que não seja o da instituição financeira emissora do boleto.

Se receber um boleto de forma diferente da que costumeiramente o recebe de seu fornecedor, desconfie! Confirme junto ao beneficiário a legitimidade do documento antes de efetuar o pagamento, boletos falsos podem ser enviados por e-mail, mensagem de WhatsApp ou de texto informando sobre um suposto desconto e por isso solicitam que desconsiderem o pagamento do DDA. Dessa forma, ao efetuar o pagamento desse "novo boleto" os recursos são desviados para outro beneficiário e assim a dívida permanecerá.

Golpe do Motoboy:

O golpista entra em contato se passando por funcionário do Sicoob e relata sobre uma suposta compra no seu cartão. Durante essa ligação solicita que informe sua senha para bloquear o cartão e oferece mandar um motoboy para recolher o cartão.

Caso receba uma ligação suspeita com informações sobre o seu cartão, desligue o telefone, aguarde alguns minutos e entre em contato com a Central de Atendimento que consta no verso do cartão. Lembre-se: o Sicoob não envia ninguém para retirar cartões no seu endereço.

Golpe do WhatsApp:

Um novo golpe está ganhando força: a clonagem do WhatsApp. Por isso, ao receber qualquer solicitação de transação de familiar ou amigo, ligue pra pessoa por outro canal para confirmar se é ela mesmo.

Para você se proteger da clonagem, basta ativar a verificação em duas etapas. Saiba como em: www.sicoob.com.br/seguranca.

Ah, nunca informe seu código de verificação do WhatsApp para ninguém.

Mensagens falsas e links suspeitos:

Os fraudadores nesse caso conseguem seu endereço de e-mail ou número de telefone e enviam uma mensagem como se fosse o Sicoob, solicitando seus dados pessoais e senhas ou alertando sobre transações indevidas ou bloqueios da conta ou cartão. Ao clicar, você será direcionado a uma página falsa, criada para capturar suas informações ou permitir a instalação de softwares maliciosos (malwares), que podem alterar a configuração de segurança do computador e possibilitar o acesso remoto. Nunca clique no link ou responda a mensagens desse tipo.

Falso depósito:

O fraudador informa que efetuou depósito indevido e, após enviar o comprovante falso, solicita que o cooperado devolva o valor ou a diferença. Mas quando o envelope depositado é conferido, está vazio. Desconfie de contatos desta natureza e, antes de agir, confirme se os valores estão desbloqueados em sua conta.

SICOOB