Orientação nº 44/SEE/SREA/DAFI
Processo Nº 1260.01.0019941/2026-07

ALERTA ÀS CAIXAS ESCOLARES: PREVENÇÃO A GOLPES E FRAUDES BANCÁRIAS

A Superintendência Regional de Ensino alerta os gestores das Caixas Escolares para a necessidade de reforçar os procedimentos de segurança na movimentação das contas bancárias e na utilização do gerenciador financeiro.

Os golpes têm se tornado cada vez mais sofisticados. Criminosos podem conhecer o nome do diretor, da escola, da Caixa Escolar, da agência bancária, de fornecedores ou de servidores e utilizar essas informações para tornar a abordagem convincente. O conhecimento desses dados, entretanto, não comprova que o contato seja legítimo.

Principais golpes e abordagens utilizadas

1. Falso gerente ou falsa central de atendimento

O criminoso entra em contato por telefone, WhatsApp, SMS ou e-mail, identifica-se como gerente ou funcionário do banco e informa, por exemplo:

- existência de transação suspeita;
- tentativa de invasão ou bloqueio da conta;
- necessidade de atualização cadastral ou de segurança;
- vencimento de módulo, certificado ou chave de acesso;
- necessidade de cancelar ou estornar uma operação.

Em seguida, solicita senhas, códigos de segurança, leitura de QR Code, instalação de programa ou realização de transferência para uma suposta “conta segura”.

Nenhum funcionário de banco solicita senha, token, código de confirmação ou transferência para regularizar problema na conta. O número exibido na chamada também pode ser falsificado, fazendo parecer que a ligação partiu da agência bancária.

2. Golpe do acesso remoto

O fraudador orienta a instalação de programas para acessar ou controlar o computador à distância, alegando que realizará uma atualização, verificação de segurança ou correção do gerenciador bancário.

Nenhuma solicitação de instalação de programa ou de acesso remoto deve ser atendida durante contato telefônico, por mensagem ou por e-mail. O banco não precisa controlar o computador da escola para verificar movimentações ou solucionar problemas na conta.

3. E-mails e páginas bancárias falsas

São enviados e-mails, mensagens ou anúncios contendo links que direcionam para páginas semelhantes às do banco. Nessas páginas, o usuário é induzido a informar agência, conta, senha, token ou outras credenciais.

O acesso ao banco deve ser realizado somente pelo aplicativo oficial ou pelo endereço digitado diretamente no navegador. Não devem ser utilizados links recebidos por e-mail, SMS, WhatsApp ou mecanismos de busca.

Também não se deve abrir arquivo recebido como suposta atualização bancária, comprovante, nota fiscal, orçamento, intimação ou documento de fornecedor sem verificar previamente sua procedência.

4. Falsificação de mensagens de gestores, servidores ou fornecedores

Criminosos podem utilizar foto, nome ou dados de pessoas conhecidas para solicitar pagamentos urgentes, alteração de dados bancários, envio de documentos ou fornecimento de códigos.

Toda solicitação de pagamento ou alteração de conta bancária recebida por mensagem deve ser confirmada diretamente com a pessoa ou empresa, por outro canal já

conhecido. Não se deve utilizar para confirmação o telefone informado na própria mensagem suspeita.

5. Troca de boletos, chaves Pix e dados bancários

Boletos, notas fiscais, contratos e mensagens eletrônicas podem ser adulterados para direcionar o pagamento a outro beneficiário.

Antes de confirmar qualquer operação, devem ser conferidos:

- nome ou razão social do beneficiário;
- CPF ou CNPJ;
- banco e dados da conta;
- valor e finalidade do pagamento;
- correspondência entre o favorecido e o fornecedor contratado.

A operação deve ser interrompida sempre que o sistema apresentar beneficiário diferente daquele constante no processo de aquisição ou contratação.

6. Falso suporte técnico ou falsa atualização do sistema

O contato pode alegar que o gerenciador financeiro, o computador, o certificado ou o módulo de segurança está desatualizado. O objetivo é induzir o usuário a instalar programa malicioso, abrir um link ou informar suas credenciais.

Atualizações somente devem ser realizadas pelos canais oficiais da instituição financeira e, quando necessário, com apoio do Núcleo de Tecnologia Educacional - NTE ou do suporte técnico oficialmente responsável.

Medidas obrigatórias de segurança

As senhas, tokens, códigos de segurança e demais credenciais bancárias **são pessoais, sigilosos e intransferíveis**. Não podem ser fornecidos a servidores, contadores, fornecedores, técnicos de informática, familiares ou qualquer outra pessoa.

A movimentação bancária da Caixa Escolar deve ser realizada exclusivamente pelos responsáveis formalmente autorizados. O Estatuto estabelece que o Presidente ou seu substituto legal e o Tesoureiro são os responsáveis pela movimentação das contas, sendo vedada a delegação dessa função.

Devem ser observados os seguintes cuidados:

1. Utilizar, preferencialmente, computador destinado às atividades administrativas, protegido por senha individual e com sistema operacional e antivírus atualizados.
2. Não realizar operações bancárias em computador compartilhado com alunos, prestadores de serviço ou pessoas não autorizadas.
3. Bloquear a tela sempre que houver necessidade de se afastar do computador, ainda que por poucos minutos.
4. Encerrar completamente a sessão do gerenciador financeiro após cada utilização. Não basta minimizar ou fechar apenas a janela do navegador.
5. Não deixar senhas anotadas em papéis, agendas, gavetas, arquivos digitais desprotegidos ou próximas ao computador.
6. Não permitir que terceiros operem o gerenciador financeiro, mesmo sob supervisão do diretor ou do tesoureiro.
7. Não salvar senhas bancárias no navegador.

8. Não conectar dispositivos desconhecidos, como pen drives, ao computador utilizado para movimentação bancária.

9. Confirmar os dados do beneficiário antes de cada autorização, inclusive nas operações destinadas a fornecedores habituais.

10. Ativar, quando disponibilizadas pelo banco, notificações de movimentação, limites transacionais e demais ferramentas de segurança.

11. Conferir regularmente os extratos e as movimentações das contas. O Tesoureiro deve monitorar as contas e comunicar imediatamente qualquer indício de irregularidade.

12. Manter disponíveis e atualizados os contatos oficiais da agência, do gerente e dos canais de atendimento do banco.

Diante de uma ligação ou mensagem suspeita

O gestor deverá:

- interromper imediatamente o contato;
- não clicar em links;
- não instalar programas;
- não fornecer senhas, códigos ou dados bancários;
- não realizar transferências, pagamentos ou testes;
- entrar em contato com a agência utilizando telefone obtido anteriormente ou divulgado no canal oficial do banco;
- comunicar a situação ao Tesoureiro e à Superintendência Regional de Ensino.

Não se deve retornar a chamada pelo número recebido nem utilizar contatos enviados pelo próprio interlocutor.

Em caso de suspeita de acesso indevido ou movimentação não reconhecida

A Caixa Escolar deverá agir imediatamente:

1. Contatar o banco pelos canais oficiais e solicitar o bloqueio preventivo das credenciais e das movimentações.

2. Alterar as senhas em equipamento seguro.

3. Solicitar ao banco o rastreamento, bloqueio ou contestação da operação, inclusive a abertura do Mecanismo Especial de Devolução — MED, quando cabível em transações Pix.

4.

Preservar comprovantes, mensagens, e-mails, números de telefone, registros de chamadas e demais evidências.

5. Registrar boletim de ocorrência.

6. Comunicar formalmente a Superintendência Regional de Ensino, apresentando relato dos fatos e documentação disponível.

A rapidez da comunicação é essencial para aumentar a possibilidade de bloqueio ou recuperação dos valores. O banco deve ser acionado tão logo seja identificada qualquer movimentação suspeita.

Atenção

A urgência é uma das principais ferramentas utilizadas pelos golpistas. Expressões como “faça imediatamente”, “a conta será bloqueada”, “o valor será perdido”, “não desligue o telefone” ou “não informe ninguém” devem ser tratadas como sinais de fraude.

Na dúvida, não realize a operação. Interrompa o contato, confira as informações e procure os canais oficiais da instituição financeira.

A segurança dos recursos públicos depende tanto das ferramentas disponibilizadas pelos bancos quanto da atuação cuidadosa dos gestores responsáveis pela movimentação financeira da Caixa Escolar.

Henrique Alves de Souza Mourão
Diretor Administrativo e Financeiro - DAFI
Superintendência Regional de Ensino - Metropolitana A
Secretaria de Estado de Educação de Minas Gerais

Documento assinado eletronicamente por **Henrique Alves de Souza Mourão**, **Diretor Administrativo e Financeiro**, em 21/07/2026, às 10:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **144968455** e o código CRC **3D23CD7B**.