

## RECOMENDAÇÕES DE SEGURANÇA

Com o avanço da tecnologia, você não precisa mais enfrentar filas nos caixas dos bancos para efetuar transferência de dinheiro, aplicações financeiras ou realizar pagamentos (água, luz, telefone, colégio, planos de saúde, etc). Essas operações agora podem ser realizadas nos terminais de autoatendimento ou, até mesmo, em sua casa, via internet banking.

Desfrutar dessas facilidades, entretanto, requer alguns cuidados, e é com o objetivo de garantir maior segurança na utilização dos canais de atendimento remoto (Internet Banking e terminais de auto-atendimento) que o Banco da Amazônia apresenta algumas orientações e dicas.

### Terminais de autoatendimento

O canal de autoatendimento pode ser utilizado para saques, pagamentos de contas, extratos, transferências, entre outros serviços. A seguir, algumas recomendações com vista a garantir mais segurança:

1. Antes de utilizar o caixa-eletrônico, faça uma verificação, compare com o equipamento do lado e evite prosseguir a operação caso encontre alguma anormalidade (monitor ou teclado com alguma diferença, fiação aparente, indício de cola ou fita adesiva, dispositivos obstruindo a saída do dinheiro, etc). Se for possível, avise alguém da agência.
2. Fora das agências, não aceite ajuda de estranhos caso o caixa eletrônico esteja "fora do ar": Procure outro caixa ou outra localidade;
3. Procure utilizar o caixa eletrônico sempre dentro do horário comercial. Caso não seja possível, procure os terminais de autoatendimento instalados em locais de grande movimentação e, de preferência, em ambientes internos (shoppings, supermercados, lojas de conveniência, postos de gasolina etc.);
4. Evite realizar saques no horário noturno. Quando isso não for possível, evite ir sozinho: leve sempre um ou mais acompanhantes adultos para simular fila atrás de você;
5. Fique atento à presença de pessoas há muito tempo nas salas de autoatendimento ou nas suas imediações. Caso perceba alguém nessa situação, utilizando vários equipamentos, não realize a operação. Procure outro local;
6. Ao digitar sua senha, procure manter seu corpo próximo à máquina a fim de evitar que a pessoa atrás de você a deduza pelo movimento dos seus dedos no teclado;
7. Nunca anote sua senha em papel ou cole no cartão eletrônico. Sua conta e senha são informações sigilosas. Não deixe que pessoa alguma tome conhecimento;

8. Em caso de dificuldades, solicite auxílio a um funcionário do banco, devidamente credenciado;
9. Caso não consiga concluir uma transação, pressione as teclas ANULA ou CANCELA;
10. Em caso de necessidade, só se comunique com o banco através de seu próprio celular. Dados referentes à sua conta e senha podem ficar perigosamente “registrados” na memória de aparelhos telefônicos deixados maliciosamente no recinto. Além do mais, você corre o risco de não estar falando com o setor de atendimento do banco;
11. Em caso de furto, roubo ou extravio de seu cartão, comunique imediatamente o fato à instituição financeira e procure uma delegacia de polícia para registrar o boletim de ocorrência;
12. Se seu cartão ficar retido ou preso na leitora, não digite novamente a sua senha: procure orientação do banco, informe a central de atendimento e, se o problema não for resolvido, chame a polícia e registre um boletim de ocorrência;
13. Ao utilizar o caixa eletrônico evite a proximidade de outra pessoa, principalmente estranha;
14. Evite realizar operações no caixa eletrônico sistematicamente nos mesmos horários: os golpistas estão sempre atentos às rotinas dos clientes;
15. A porta do banco é o local preferido dos golpistas e ladrões: portanto, cuidado! Esteja sempre atento ao deixar a agência;
16. Quando estiver na fila, evite qualquer aproximação de estranhos. E muito cuidado com as cortesias;
17. Nunca saia do banco com qualquer pacote nas mãos, mesmo que não seja dinheiro: isso chama muito a atenção dos golpistas;
18. Sempre que emitir ou receber seu extrato de contas verifique criteriosamente todos os lançamentos e, se perceber algo estranho, entre em contato imediatamente com o gerente de sua agência;
19. Se você perder seu cartão do banco ou algo errado vier a ocorrer com ele, bloqueie-o imediatamente via terminais de autoatendimento, teleamazonia ou internet banking e vá à delegacia de polícia mais próxima para registrar a ocorrência;
20. Se o caixa eletrônico reter seu cartão, não digite sua senha para tentar retirá-lo. Em lugar disso, tecele apenas ANULA para cancelar a operação e solicite ao segurança que chame imediatamente um empregado do banco. E não abandone o caixa eletrônico enquanto seu cartão permanecer retido no terminal.

## Canal Internet

O internet banking permite a realização de inúmeras operações financeiras, sem a necessidade de deslocamento até uma agência. Para usufruir dessa comodidade com segurança, entretanto, alguns cuidados são necessários, tais como:

1. Evite atalhos para acessar o site do Banco da Amazônia, principalmente aqueles obtidos em sites de pesquisa. Digite sempre o endereço [www.bancoamazonia.com.br](http://www.bancoamazonia.com.br);
2. Ao acessar o site do banco procure fazê-lo sempre no início da conexão ao provedor. Evite navegar em outras páginas ou ler "e-mails" antes de utilizar internet banking;
3. Não acesse sua conta a partir de equipamentos ou ambientes públicos ou desconhecidos, como cibercafés, escolas, bares. Eles podem estar com antivírus desatualizados ou até mesmo preparados para capturar seus dados;
4. Evite abrir e-mails de origem desconhecida. Evite também clicar em links ou abrir arquivos anexos ao e-mail, principalmente os executáveis (aqueles com extensão .exe, .com, .scr, .bat);
5. Tenha cuidado com e-mails sobre promoções ou vantagens, até mesmo aqueles que pareçam escritos por conhecidos;
6. Nunca responda a e-mails que solicitem seus dados bancários (número de conta, agência, senhas de acesso);
7. Existe um cadeado pequeno no canto da tela de acesso à Internet que normalmente está fechado. Ao clicar nesse cadeado, são exibidas informações sobre o certificado de segurança do ambiente, que garantem a autenticidade, confidencialidade e integridade às informações eletrônicas;
8. Não execute programas ou abra arquivos anexados sem antes submetê-los a antivírus atualizados, mesmo que procedam de pessoas de sua confiança. Eles podem conter vírus ou cavalos-de-tróia, sem que os remetentes se deem conta disso;
9. Use sempre provedores com boa reputação no mercado, assim como browsers e antivírus sempre atualizados. A escolha de um provedor deve levar em conta também a confiabilidade da empresa e as políticas de segurança adotadas por ela;
10. Verifique sempre a data e hora do seu último acesso sempre que utilizar a conta pela internet;
11. Clique no botão "Sair" sempre que terminar o uso do internet banking;

12. O Banco da Amazônia não envia mensagens de correio eletrônico a seus clientes, nem autoriza qualquer parceiro comercial a fazê-lo em seu nome. Qualquer dúvida entre em contato com o **SAC (0800-727-7228) ou Help Desk (0800-280-3595)**;
13. O Banco da Amazônia não envia e-mails com arquivos executáveis (arquivos com extensões .exe, .com, .scr, .bat e outras);
14. Nunca revele sua senha em lugar nenhum, nem atenda a qualquer pedido de cadastramento ou recadastramento sob nenhum argumento;
15. Só informe seus dados pessoais, como CPF e RG, a sites reconhecidos e de procedência confiável. Na dúvida, não hesite em negá-los.

### **Algumas recomendações para evitar fraudes na internet**

**Proteja seu computador** – Assim como tomamos precauções de segurança, em nossa casa ou no automóvel, precisamos proceder com nosso computador. Para isso, é necessária a utilização de pelo menos três tipos de programas de proteção:

1. **Antivírus:** este programa protegerá seu computador contra os “vírus de computador” e suas variantes, como os worms. É importantíssimo que o antivírus seja atualizado frequentemente de acordo com as recomendações do fabricante. O ideal é que o programa permita a busca constante e automática por atualizações na internet, com frequência no mínimo diária;
2. **Firewall pessoal:** este programa irá manter uma barreira lógica entre seu computador e a Internet, evitando que atacantes façam acessos não autorizados;
3. **Anti-Spam:** este programa irá filtrar o conteúdo indesejado de e-mails, descartando automaticamente aqueles que forem considerados “Spam”;

**Não esqueça:** a eficiência desses programas depende de sua correta instalação e configuração em seu computador. Recomendamos confiar tais procedimentos a alguém que detenha conhecimento técnico.

**Participação de sorteios:** evite participar de sorteios com ofertas tentadoras e milagrosas. Ações como essas normalmente são armadilhas para roubar informações e dados confidenciais;

**Ofertas tentadoras:** não aceite ofertas tentadoras feitas por e-mail: geralmente, elas provêm de endereços falsos. Certifique-se sempre da procedência do e-mail e, em caso de dúvida, contate a empresa através do atendimento on-line ou telefone fixo;

**Programas de invasão:** cuidado com mensagens beneficentes ou que contenham imagens de catástrofes, pornografia, acidentes etc. É muito comum que golpistas explorem a curiosidade do internauta para perpetrar seus golpes. Quase sempre, arquivos com tais imagens carregam programas de invasão (trojans) que se instalam no seu computador e, posteriormente, roubam senhas e outros dados confidenciais. Remova tais mensagens mesmo que o remetente seja uma pessoa conhecida;

**Emails:** nunca abra anexos de e-mails com texto suspeito mesmo que provenham de amigos ou conhecidos. Neste caso, contate antes o remetente e confirme o envio por parte dele. Em muitos casos, ele nem se dá conta que seu computador está infectado;

Entretanto, mesmo que com todos estes cuidados você ainda venha a ser vítima de fraude, faça o seguinte:

**Notifique o Serviço de Atendimento ao Cliente – SAC, pelo telefone 0800–727–7228 ou Help Desk do Internet Banking, pelo telefone 0800–280–3595.**

Mesmo que levado por uma simples suspeita, não hesite em contatar o SAC ou Help Desk. Agindo com rapidez, você poderá evitar sérios problemas. Dê ciência ao seu gerente da possível fraude e, se for o caso, solicite o bloqueio imediato de sua conta.

#### **Formalize seu alerta ao Banco**

Sempre que contatar com o SAC ou Help Desk anote o número de atendimento (toda ligação feita para os serviços de atendimento de instituições financeiras é gravada e possui um número para verificação) e sempre solicite um comprovante de sua solicitação de bloqueio de sua conta ou cancelamento do cartão.

#### **E faça sempre um registro de ocorrência policial (Boletim de Ocorrência)**

Registre ocorrência junto às autoridades policiais do bairro em que você mora e leve-a ao Banco.