

Recomendações de Segurança no uso da Internet

Abaixo você encontra recomendações importantes, que o ajudarão a realizar as suas transações bancárias com mais segurança, bem como a utilizar outros sites da Internet com mais proteção.

» **Instale o Módulo de Proteção do Banco Santander** - O Módulo de Proteção é um software que trabalha de forma integrada ao navegador combatendo a ação de programas maliciosos instalados no seu computador sem seu consentimento, que capturam ou solicitam seus dados de acesso ao Internet Banking. Sua instalação é simples e rápida (aproximadamente 30 segundos) e pode ser realizada imediatamente através do link www.santander.com.br/mps.

» **Mantenha o antivírus atualizado** e instalado no computador que você utiliza para ter acesso aos serviços bancários. Mantenha também o sistema operacional atualizado e outras ferramentas de controle de segurança, como um firewall pessoal, e utilize e-mail com filtros Anti-Spam (para filtrar mensagens não solicitadas).

» **Troque a sua Senha de Internet periodicamente** - Não deixe suas informações e senhas de acesso ao internet banking juntamente com seu cartão do banco. Procure sempre decorar a senha, sem utilizar informações como datas de nascimento, números de telefones ou outras informações fáceis de serem descobertas.

» **Somente utilize equipamento efetivamente confiável.** Não realize operações financeiras ou digite dados sigilosos em equipamentos de uso público (por exemplo, em "cyber cafés", hotéis, e "lan houses"), em equipamentos que você não conheça ou em equipamentos que não tenham programas antivírus atualizados. Existem programas - denominados Cavalos de Tróia - utilizados por fraudadores - que têm por função capturar as informações do cliente quando digitadas no computador.

» **Nunca forneça mais de um código do seu Cartão de Segurança On-line na mesma tela.** Caso você encontre uma tela como a abaixo, não digite nenhum número e entre em contato com a Superlinha: é uma fraude. Veja o exemplo:



» **Não execute programas nem abra arquivos de origem desconhecida**, especialmente cartões de aniversário, Natal e outras datas comemorativas. Eles podem conter vírus, Cavalos de Tróia e outras aplicações maliciosas que, de modo oculto ou se passando por aplicações legítimas do Banco, podem capturar ou solicitar dados de acesso ao internet banking, permitindo a ação de fraudadores em sua conta.

» **Cuidado com e-mails não solicitados** ou de procedência desconhecida, especialmente se tiverem arquivos anexados. Correspondências eletrônicas também podem trazer programas desconhecidos que oferecem diversos tipos de riscos à segurança do usuário. É mais seguro remover os e-mails não solicitados e que você não tenha absoluta certeza que procedem de fonte confiável. Tome cuidado especialmente com arquivos e endereços obtidos em salas de bate-papo (chats), ICQ, MSN, IRC e Yahoo. Desconfie sempre de e-mails que alegam ser do seu banco e jamais clique em links que, teoricamente, o levariam para sites de bancos: prefira você mesmo digitar o endereço de acesso ao site.

Apenas abra esse tipo de mensagem se você fez uma transação ou solicitou uma informação a seu banco e recebeu o aviso de que receberia o conteúdo por e-mail.

» **Evite visitar sites para realizar download** (transferência de arquivos) de programas ilegais e com aparência duvidosa. Alguns desses sites instalam automaticamente ferramentas com características maliciosas e que podem ser utilizadas por fraudadores. Só faça downloads de sites que conheça e saiba que são confiáveis.

» **Utilize sempre as versões de browsers (programas navegadores) mais recentes**, pois elas incorporam melhores mecanismos de segurança. É necessário também que o browser esteja configurado para executar componentes ActiveX e que esteja com a opção de gravação de cookies habilitada. Cookie é o nome dado a um pequeno arquivo criado pelo site do Santander em seu browser. Nossos cookies não contém informações pessoais e não podem ser lidos por outros sites. Caso a opção de gravação de cookies esteja desabilitada, o site pode não funcionar completamente. Mantenha também seu sistema operacional sempre atualizado.

» **Quando for efetuar pagamentos** ou realizar outras operações financeiras, verifique se o site possui Certificado de Segurança. O Certificado de Segurança é uma garantia fornecida por uma entidade que confirma a identificação do titular do certificado e o nível de segurança do site. A entidade certificadora utilizada pelo Santander é a VeriSign, mundialmente reconhecida. Para visualizar o certificado de segurança de qualquer site, basta que você clique sobre o ícone do cadeado existente na parte inferior do seu navegador. Uma janela se abrirá contendo a confirmação da autenticidade desse site.

» **Acompanhe periodicamente os lançamentos em sua conta corrente.** Caso constate qualquer crédito ou débito irregular, entre em contato com o Banco imediatamente.

» **Caso desconfie que seu computador possa estar infectado por vírus** ou outros programas maliciosos entre em contato com a [Superlinha](#) e envie por e-mail cópias de evidências para análise (arquivos suspeitos, e-mails duvidosos ou cópias de tela de resultados de ferramentas de segurança) para o e-mail evidencias@santander.com.br.

» **Use somente provedores de acesso confiáveis.** A escolha de um provedor internet deve levar em conta também seus mecanismos, políticas de segurança e a confiabilidade da empresa. Se considerar necessário, solicite a visita de um técnico de sua confiança para avaliar a segurança de seu computador ou da rede de sua empresa.

» **Encaminhe essas dicas aos demais usuários dos computadores** em sua residência ou empresa e fique sempre atento a mudanças de comportamento e aparência nos serviços disponíveis no site do Banco.

» **Se estiver em dúvida** sobre a segurança ao acesso ou sobre algum procedimento que executou, entre em contato com o Banco imediatamente.