**SEGURANÇA NA INTERNET**

* Para realizar transações financeiras e obter informações por computador via Internet, os Clientes devem conhecer os riscos a que podem estar sujeitos e as medidas preventivas que devem adotar para evitá-los.
* Mantenha sempre seu antivírus atualizado e instalado no computador que você utiliza, para realizar as transações bancárias;
* Troque sua senha do Internet Banking periodicamente, pelo menos duas vezes ao ano ou quando julgar necessário;
* Só utilize equipamento efetivamente confiável. Não realize operações em equipamentos que não tenham programas antivírus atualizados, nem em equipamentos públicos como Cybercafés, Lan Houses ou Internet Lounge;
* Use somente provedores confiáveis. A escolha de um provedor deve levar em conta também seus mecanismos, as políticas de segurança e a confiabilidade da empresa;
* Cuidado com e-mails não solicitados ou de procedências desconhecidas, especialmente se tiverem arquivos anexados. Nesse caso, é mais seguro "deletar" e-mails quando: não forem solicitados ou quando você não tiver certeza de que procedam de fontes confiáveis;
* Evite sites arriscados e só faça downloads (transferência de arquivos para o seu computador) de sites que conheça e saiba que são confiáveis;
* Quando efetuar pagamentos ou realizar outras operações financeiras, certifique-se de que está no site desejado, seja do Banco ou de outro qualquer, "clicando" sobre o cadeado ou sobre a chave de segurança que aparecem quando se entra na área de segurança do site;
* Acompanhe os lançamentos em sua conta-corrente. Caso constate qualquer crédito ou débito irregular, entre imediatamente em contato com a Central Banpará 3004-4444 - Belém e Região Metropolitana, Marabá e Santarém (fixo e celular) e 0800 285 8080 - Demais Localidades (fixo);
* Se estiver em dúvida sobre a segurança de algum procedimento que executou, entre em contato com o Banco. Prevenção é a melhor forma de segurança.
* Em caso de dúvida, procure o SAC Banpará - 0800 280 6605 para informações adicionais.

**MÁQUINAS DE AUTOATENDIMENTO**

* Como utilizar os caixas automáticos com mais segurança
* Atenção! Antes de iniciar qualquer transação, verifique na tela se o equipamento está ativo ou inoperante. Caso esteja inoperante, não insira seu cartão;
* Caso o caixa eletrônico participante da rede ou equipamento do Banco estiver inoperante, não aceite oferta de estranhos de passar seu cartão em terminal avulso, mesmo que se apresentem como funcionários do Banco. Fraudadores têm utilizado esse golpe para clonar (copiar os dados) cartões e obter senhas;
* Enquanto estiver operando o equipamento, mantenha o corpo próximo à máquina, para evitar que outros possam vê-lo digitando a senha ou descobri-la pelo movimento dos dedos no teclado;
* Procure sempre os caixas automáticos instalados em locais de grande movimentação e, preferencialmente, em ambientes internos como: loja de conveniência, shoppings etc.;
* Sempre que possível, faça suas operações no horário comercial quando o fluxo de pessoas é maior evitando o período noturno. Caso precise realmente sacar dinheiro à noite, esteja acompanhado de uma ou mais pessoas adultas para que fiquem fora da cabine, como se estivessem na fila;
* Esteja atento à presença de pessoas suspeitas ou curiosas no interior da cabine ou às proximidades. Na dúvida, não faça a operação. Nunca aceite ou solicite ajuda de estranhos, mesmo que não lhe pareçam suspeitos;
* Caso haja a retenção do cartão no caixa automático, tecle ANULA ou CANCELA e comunique-se imediatamente com o SAC Banpará - 0800 280 6605;
* Não utilize telefones de terceiros desconhecidos, principalmente os celulares para comunicar-se com o Banco, pois, você poderá não estar falando com um representante do Banco, além do risco de ficar sua conta e senha na memória do telefone;
* Esteja atento, desconfie de vantagens financeiras ou dramas familiares que lhe sejam apresentados por desconhecidos na fila do caixa automático;
* Jamais receba créditos de pessoas desconhecidas em sua conta. Esta prática é muito utilizada por meliantes nas proximidades das Agências e nos quiosques de autoatendimento.

**E-MAILS: PROTEJA VOCÊ E SEU COMPUTADOR**

* As várias formas de ataque feitas a seu computador podem causar danos irreparáveis, o e-mail é uma das formas passíveis de contaminação. Para sua proteção, formulamos algumas dicas de como evitar essas intrusões.
* O seu endereço de e-mail deve ser privativo, não o publique em grupos de discussão, fóruns e salas de bate-papo. Essa regra vale também para qualquer outra informação pessoal como: nome completo, endereço, telefone, local de trabalho, números de documentos (RG, CPF...);
* A sua conta de e-mail pessoal e/ou profissional deve ser reservada a esses fins. Como alternativa, crie outra conta para usos diversos nos serviços gratuitos de webmail como o Gmail, BOL, Yahoo etc.;
* Nunca responda a e-mails desconhecidos e/ou não solicitados (SPAM), nem mesmo para pedir sua remoção de listas de envio ou para reclamar ou solicitar quaisquer informações. O seu endereço de e-mail é confirmado exatamente pela sua resposta;
* Nunca abra ou execute qualquer arquivo anexo a mensagens de origens desconhecidas ou não solicitadas. Os cuidados devem ser redobrados quando a extensão do arquivo for do tipo EXE, SCR, PIF, COM, BAT, CMD, DPR. Não esqueça de configurar o seu programa cliente de e-mail (Outlook, Eudora...) de forma a não abrir automaticamente os anexos, pois na maioria dos casos esses programas são vírus, trojans ou worms;
* Os e-mails do tipo ameaçadores como cobranças, cancelamento de documentos, ações judiciais, devem ser deletados imediatamente com a tecla <SHIFIT> pressionada para não ficarem na lixeira. Também desconfie de mensagens que aparentem ter sido enviadas por bancos, repartições públicas, lojas famosas e programas televisivos. Não acredite e não leve a sério esses tipos de mensagens. Os respectivos órgãos e empresas nunca as enviam por e-mail, com esses intuitos;
* Não participe de qualquer tipo de corrente na rede, sejam pirâmides financeiras, sejam supostas ou reais campanhas de solidariedade, apague-as. Desconfie também de qualquer oferta que lhe chegue pela rede onde exista a solicitação de um pagamento adiantado;
* Não confie em mensagem que "parecem" ter sido enviadas por seus contatos. Use seu senso crítico e um pouco de desconfiança pois existem muitos casos de fraude com e-mails que usam maliciosamente os nomes de pessoas conhecidas da vítima;
* Recuse-se a abrir qualquer mensagem suspeita onde não esteja claramente definida a identidade de quem a envia (endereços falsos, endereços omissos ou incompletos, assuntos com erros ou incongruentes...).
* A mesma regra vale para sites que proponham vendas de produtos ou serviços, mas que tenham poucos dados.

**USANDO SEU CARTÃO MAGNÉTICO**

* Jamais entregue o seu cartão a outras pessoas e nem permita que pessoas estranhas o examinem sob qualquer pretexto;
* Em caso de roubo ou extravio, faça o cancelamento nos quiosques de autoatendimento ou através da Central de Atendimento;
* Se você não tiver a prática de memorizar sua senha, procure deixar sempre a anotação em local diferente da do cartão;
* Jamais utilize como SENHA números que contenham quaisquer ligações com você ou seus familiares;
* Ao utilizar seu cartão para efetuar pagamentos, procure mantê-lo ao seu alcance visual;
* Em caso de pagamento com boleto avulso, havendo rasura pelo agente, solicite a inutilização das vias e do carbono à sua vista;
* Ao substituir o seu cartão, destrua o anterior, inutilizando a tarja magnética, o local da assinatura e a numeração;
* Não exponha seu cartão ao calor nem a campos magnéticos como celular, rádio, alarme de veículos, equipamentos de vídeos e similares, pois esses equipamentos podem provocar a desmagnetização de sua tarja.