



Dicas de Segurança

A SEGURANÇA DE SEU CARTÃO VISA

- Nunca anote sua senha – memorize-a!
- Nunca diga a sua senha a ninguém pessoalmente, por telefone ou por e-mail.
- Ao escolher sua senha, não opte por números e letras que possam ser facilmente identificados. Evite utilizar iniciais, números de telefone ou datas de nascimento.
- Certifique-se de assinar o cartão logo que recebê-lo.
- Faça uma relação de número de contas e números de telefone para comunicar cartões perdidos ou extraviados. Mantenha essa lista em um lugar seguro.
- Certifique-se de receber seu cartão após a efetuar a compra, e verifique se é realmente o seu cartão.
- Nunca forneça o número do seu cartão por telefone, a menos que você tenha realizado a chamada por iniciativa própria.
- Sempre verifique o montante da transação antes de assinar o comprovante.
- Ninguém deverá ter acesso a seu cartão. Se um familiar pegar emprestado o seu cartão sem seu conhecimento, você é responsável pelas compras ou pelo dinheiro retirado.
- Não deixe seu cartão em lugares de fácil acesso sem supervisão, como no porta-luvas do carro ou na gaveta do escritório.
- Informe imediatamente seu banco no caso de roubo ou perda de cartão. Quando viajar para fora do país, leve consigo os números de telefones gratuitos do Centro de Assistência Global a Portadores de Cartão Visa.

SEGURANÇA NAS COMPRAS ON-LINE (INTERNET)

- Dê preferência a lojas virtuais que possuam o protocolo de segurança **Verified by Visa**.
- Utilize somente sites seguros e que permitem a transmissão segura da informação. Identifique as chaves de segurança como o símbolo do “cadeado fechado” na barra inferior do site ou no endereço (URL), que começam com https://. Estes sinais indicam que somente você e o site podem ver a informação relacionada ao pagamento.
- Forneça seu número de conta, somente quando a tenha iniciado.
- Mantenha um registro de suas transações e revise constantemente seus extratos.
- Antes de fazer uma compra, verifique a página do estabelecimento, as políticas de entrega e devolução para certificar-se que os artigos podem ser devolvidos, caso não se encontrem em condições satisfatórias.



SEGURANÇA NO CAIXA AUTOMÁTICO

- Analise o local: se o Caixa Automático está mal iluminado ou em uma área deserta, utilize outro Caixa Automático.
- Tenha o cartão à mão para evitar ter que procurá-lo no bolso ou na carteira.
- Certifique-se que ninguém próximo a você possa ver sua senha e o montante da transação.
- Não conte o dinheiro enquanto estiver no Caixa Automático, guarde imediatamente o dinheiro, o cartão e o recibo da transação.
- Depois de completar a transação, lembre-se de retirar o cartão e o recibo da transação.
- Se o seu cartão ficar retido no Caixa Automático, desconfie de quem lhe oferece ajuda, mesmo que pareça um segurança do banco. Não aceite ajuda de estranhos e relate o evento o mais rápido possível a seu banco .
- Não utilize um Caixa Automático que possui uma aparência estranha como, por exemplo, com dispositivos sobrepostos.
- Evite que alguém possa ver sua senha enquanto utiliza o Caixa Automático ou faz uma compra em um comércio. Nunca a escreva.

CONTRA O PHISHING

“Nunca clique em atalhos recebidos em um e-mail não solicitado”.

- Nunca abra e-mails não solicitados, apague-os.
- Nunca forneça dados pessoais e/ou informação financeira em transações que você não iniciou.
- Proteja suas senhas. Nunca as escreva nem as forneça, a menos que você tenha iniciado a transação.
- Em casa, utilize ferramentas de segurança na internet como anti-spam, firewalls e antivírus.
- Não passe sua senha através de e-mail.
- A Visa nunca enviará mensagens eletrônicas para seu e-mail, já que a empresa não detém seu endereço eletrônico.
- Seu banco também não solicitará informações através de e-mail, a menos que você tenha autorizado.

O que os fraudadores buscam?

- Informação pessoal: nomes, endereços, números de telefone, etc.
- Informação financeira: números de conta bancária, número de cartões, senhas, etc.

Os fraudadores tentarão enganá-los para obter o maior número informações possível. Esta informação será utilizada para roubar sua Identidade ou o seu dinheiro.
