Recomendações de Segurança

O Banco BTG Pactual tem plena consciência do seu dever de proteger os dados dos seus clientes contra acessos indevidos. Mais do que uma obrigação regulatória ou legal, garantir o sigilo das informações que nos são confiadas é um princípio básico de uma organização que considera seus clientes como sócios. Atingimos este objetivo adotando os mais altos padrões de segurança em nossos sistemas. Isto, entretanto, não é o suficiente. Nossos clientes desempenham um papel fundamental no processo de garantir a proteção de suas próprias informações.

Existem boas práticas de segurança que devem ser adotadas quando se utilizam meios de comunicação eletrônica para acesso a informações pessoais ou a serviços não públicos. A adoção destas condutas não garante que uma pessoa não sofra um ataque bem sucedido, mas reduz significativamente a probabilidade de tal incidente ocorrer ou os danos decorrentes.

Recomendação 1 – Mantenha todos os softwares de seu computador permanentemente atualizados.

Softwares não estão livres de apresentarem falhas em seus códigos que originem vulnerabilidades que podem ser exploradas por um atacante. Todos os fornecedores de software disponibilizam atualizações periódicas de seus produtos para sanar eventuais vulnerabilidades.

A maioria dos sistemas operacionais assim como das principais aplicações possuem mecanismos automáticos para informar sobre a existência de atualizações no *website* do fornecedor. Garanta que estes mecanismos estejam corretamente configurados e funcionando em seu computador.

O grau de atualização de seu computador pode também ser verificado através de ferramentas especialmente desenvolvidas para este fim, comerciais ou não.

Recomendação 2 – Utilize softwares de segurança em seu computador pessoal.

O *kit* de segurança mínimo que deve estar presente em qualquer computador é composto de *firewall*, anti-vírus e anti-*spyware*. Um *firewall* bem configurado protege seu computador contra acessos indevidos provenientes de outros equipamentos na Internet. Muitos sistemas operacionais já possuem um *firewall* pré-instalado e um conjunto de perfis de conexão sugeridos: conexão à rede pública (Internet), conexão à rede protegida etc. Tenha certeza que seu *firewall* está ativo e utilizando o perfil correto ao conectar seu computador à rede.

Anti-vírus e anti-*spywares* protegem seu computador contra ameaças eletrônicas que conseguem alcançar o seu equipamento através de um *e-mail*, um *link* selecionado, um *pen drive* contaminado etc. Estes itens de proteção possuem uma base de assinaturas e a utilizam para identificar novos tipos de ataques. Esta base é atualizada automaticamente a partir do *website* do fornecedor na Internet. Os softwares emitem uma mensagem de erro caso esta atualização automática falhe. Force uma atualização manual nesta situação – não navegue na Internet com a base de assinaturas desatualizada.

Atualmente são comuns pacotes de segurança compostos de diversos itens de proteção - *firewall*, anti-vírus, anti-*spyware* e outros - integrados em um único produto. Recomendamos a compra de um destes pacotes, pois esses protegem de maneira mais completa o seu computador e possuem um custo final menor do que a aquisição de cada elemento em separado.

Recomendação 3 – Pratique uma navegação defensiva.

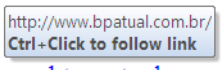
Ao acessar *websites* tenha certeza que está acessando o *website* correto. Verifique se o endereço que aparece no seu navegador corresponde efetivamente ao *website* que você deseja acessar.

Não instale programas baixados de *websites* que você desconheça. Alguns dos pacotes de segurança mencionados na **Recomendação 2** possuem um módulo de classificação de *websites* que informa se o mesmo é confiável ou não. Dê preferência à aquisição de pacotes de segurança que possuam este módulo.

Recomendação 4 – Não considere confiáveis todas as mensagens recebidas.

Nunca forneça informações pessoais por *e-mail* ou preenchendo formulários acessados por *links* contidos em *e-mail*s. O texto exibido em um *link* no corpo de uma mensagem pode não ser igual ao endereço do *website* que será acessado ao se selecionar o *link*. Chama-se camuflagem quando este recurso é utilizado para ludibriar pessoas.

A camuflagem é comumente utilizada por fraudadores para levar a vítima a acessar uma página na Internet pretensamente pertencente a um banco. Na verdade esta página falsa está hospedada em um servidor controlado pelo fraudador – a vítima acaba fornecendo suas credenciais que são depois utilizadas para acessar sua conta no *website* do banco.



http://www.btgpactual.com

O *website* que é efetivamente acessado pode ser obtido colocando-se o mouse sobre o *link*. Cuidado para não selecionar o *link* inadvertidamente!

Como boa prática de segurança prefira sempre digitar ou copiar o endereço para o navegador ao invés de selecionar *links*. Nunca abra arquivos anexados a *e-mails* ou instale softwares baixados via *link* contido no corpo de uma mensagem de origem não confirmada. E-mails suspeitos geralmente exploram a curiosidade, ambição ou o medo das pessoas como, por exemplo:

- Abordando questões relacionadas a bloqueio, desbloqueio ou renovação de contas, assinaturas, cartões etc.;
- Oferecendo empréstimos pessoais, assinaturas gratuitas, prêmios;
- Mencionando dívidas, multas, processos judiciais;
- Informando sobre vulnerabilidades detectadas no computador do destinatário e oferecendo correções para as mesmas;

- Comunicando sobre novos procedimentos de segurança do banco do destinatário e solicitando a instalação de módulos de segurança para um acesso mais seguro[1].

Observe que o fato de você receber um *e-mail* de um remetente conhecido não necessariamente indica que o *e-mail* é confiável. O e-mail, na verdade, pode ter sido enviado por outra pessoa - existem formas de se alterar parcialmente o endereço do remetente de forma a enganar o destinatário do *e-mail* em uma primeira leitura. Mesmo no caso em que o *e-mail* efetivamente tenha partido da caixa postal do remetente, este pode ter sido enviado por um vírus.

Recomendação 5 – Cuide com extremo cuidado das credenciais utilizadas para autenticar seus acessos a *websites* ou sistemas.

Seja qual for a credencial utilizada no momento da autenticação, cuide de sua segurança – nunca compartilhe suas credenciais com outras pessoas. Quando uma das partes da credencial for uma senha fixa, defina boas senhas – evite datas de aniversário, números de cpf, telefones, nomes de conhecidos, times de futebol etc.

Sempre que possível defina senhas com ao menos um ou mais números, caracteres especiais, letras maiúsculas, letras minúsculas e de tamanho razoável (mínimo de 7 caracteres). Para evitar que a senha de tão complexa não consiga ser memorizada, utilize uma regra para definir uma senha de fácil memorização. Exemplo:

> "**M**eu **f**ilho **a**niversaria **em 18** de **J**ulho." - senha: "**Mfa@18J**".

Troque a senha periodicamente – uma mesma senha não deve ser utilizada por mais de 90 dias. Não reutilize senhas antigas.

Quando uma das partes da credencial for um número gerado por um dispositivo do tipo *token* proteja o dispositivo contra acessos indevidos.

Recomendação 6 – Fique atento às informações associadas à sua conta em *websites* ou *sistemas* – estas informações podem denunciar acessos indevidos.

Reporte imediatamente ao responsável pelo *website* qualquer movimentação/operação anômala realizada.

Recomendação 7 – Não menospreze o *backup*.

Manter um backup atualizado dos dados armazenados em seu computador ainda é a melhor forma de protegê-los contra perda.

[1] Bancos eventualmente solicitam instalação de módulos de segurança após a autenticação do cliente em seus sites e não por *links* em e-mails.