Guia de segurança do cardionauta

Nesta edição finalizamos nosso especial sobre segurança e métodos de prevenção com orientações sobre Comércio eletrônico e Internet Banking.

Normalmente, não é uma tarefa simples invadir programas e fraudar dados num servidor de uma instituição bancária ou comercial. Assim, os invasores têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

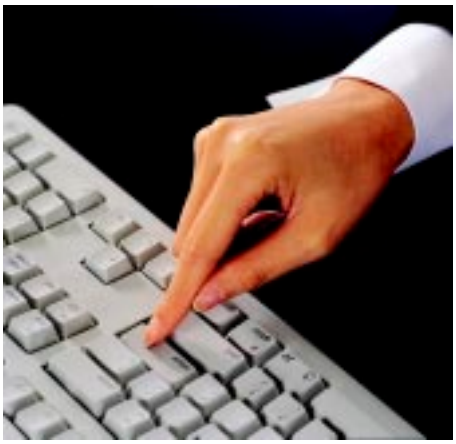
Um usuário deve ter muitos cuidados ao acessar sites de comércio eletrônico ou Internet Banking. Dentre eles, podem-se citar:

- realizar transações somente em sites de instituições confiáveis;
- certificar-se de que o endereço do site corresponde àquele que realmente se quer acessar;
- antes de aceitar um novo certificado, verificar junto à instituição que mantém o site sobre sua emissão e quais são os dados nele contidos;
- procurar sempre digitar em seu navegador o endereço desejado. Não utilize links em páginas de terceiros ou recebidos por e-mail;
- certificar-se de que o site faz uso de conexão segura, ou seja, que os dados transmitidos entre seu navegador e o site serão criptografados utilizando um tamanho de chave considerado seguro;
- verificar o certificado do site, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade;
- não acessar sites de comércio eletrônico ou Internet Banking através de computadores de terceiros;
- desligar sua Webcam (caso você possua alguma) ao acessar um site de comércio eletrônico ou Internet Banking.

Existem dois itens que podem ser visualizados na janela do seu navegador, que significam que as informações transmitidas entre o navegador e o site visitado estão sendo criptografadas. O primeiro pode ser visualizado no local onde o endereço do site é digitado. O endereço deve começar com https:// (diferente do http:// nas conexões normais). O segundo item a ser visualizado corresponde a algum desenho ou sinal no rodapé, indicando que a conexão é segura.

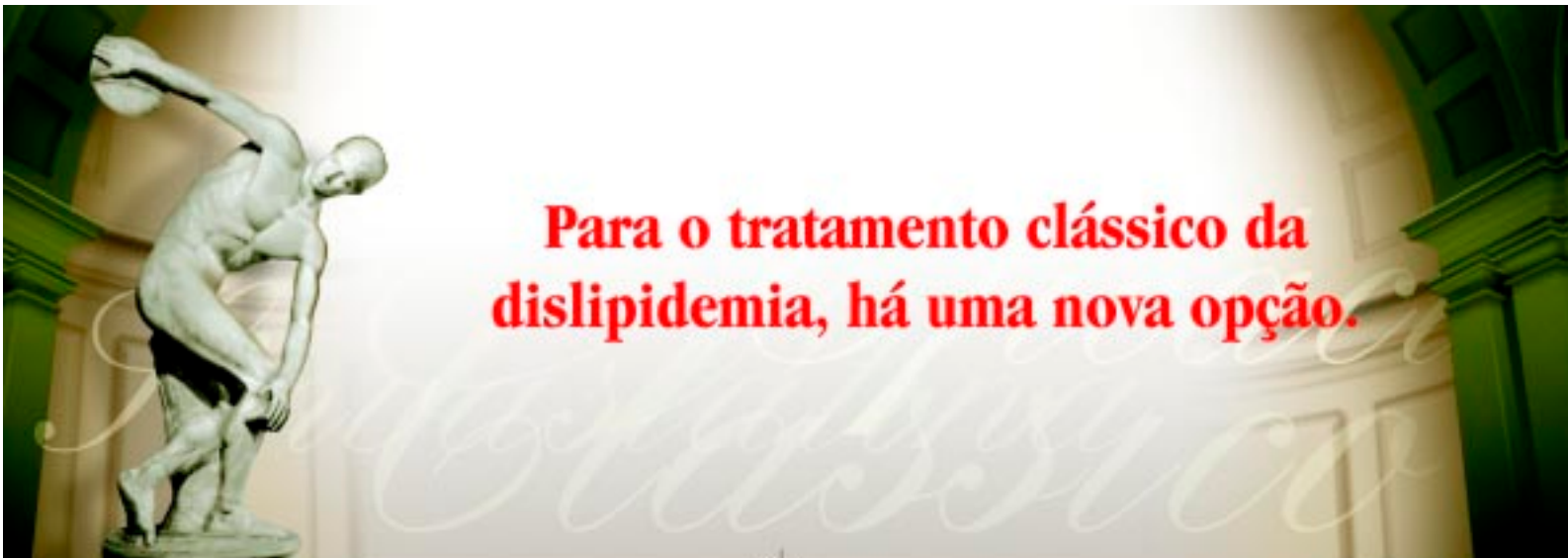
Normalmente, o desenho mais adotado é de um "cadeado fechado" (se o cadeado estiver aberto, a conexão não é segura). Ao clicar sobre o cadeado, será exibida uma tela que permite verificar as informações referentes ao certificado emitido para a instituição que mantém o site, bem como informações sobre o tamanho da chave utilizada para criptografar os dados.

Proteja o seu computador pessoal mantendo sempre atualizado o antivírus, instale



um software contra spyware e evite a instalação de aplicativos P2P como o Kazaa. Uma dica simples para uma segurança adicional: antes de usar o internet banking ou comprar pela internet, no seu internet explorer, vá em Ferramentas>>Opções de Internet>>clique excluir arquivos para excluir todo o conteúdo offline. Clique também em excluir cookies. Na aba conteúdo, clique Autocompletar e cancele todas as opções.

Aproveite para limpar as senhas e formulários. Repita o procedimento antes de sair da internet.

Apesar de existirem todas estas situações de risco, os cuidados são relativamente simples e os ataques virtuais são menos freqüentes se considerarmos os assaltos que sofremos na vida real.

Augusto Uchida