Polícia Federal alerta para golpes na internet

O cardiologista Iran Castro, que é o presidente do 60º Congresso da SBC, teve um contratempo com falsos e-mails na internet, nitidamente enviado por golpistas, e decidiu comunicar o fato a Polícia Federal, que prontamente agradeceu a mensagem e enviou algumas recomendações bastante úteis. As dicas encaminhadas pela Divisão de Comunicação Social do Departamento de Polícia Federal são as seguintes:

- Tomar o máximo cuidado com mensagens e promessas de dinheiro fácil – se dinheiro fosse fácil, o trabalho perderia sentido.
- Utlização de um antivírus sempre atualizado.
- Não abrir arquivos anexos sem um bom antivírus instalado e atualizado.
- Não clicar em hiperlinks de e-mails que direcionem a um arquivo executável (aqueles .exe).
- Os bancos e instituições financeiras mantêm uma política de não enviar mensagens por e-mails, portanto, atenção com mensagens de instituições financeiros circulando, são falsificações de hackers, com o intuito de instalar programas para capturar senhas e informações pessoais e bancárias dos usuários.
- Informe-se com seu banco sobre a política de segurança em transações bancárias via internet.
- Utilização de filtros anti-spam.
- Enfim, cuidado com mensagens de remetentes desconhecidos.

Guia de segurança do cardionauta

Este artigo traz, em dois capítulos de forma simplificada, os diversos riscos envolvidos no uso da internet e seus métodos de prevenção. Serão comentadas as dicas para aumentar a segurança do seu computador, como uso de antivírus e *firewalls*, uso adequado de programas de e-mail, de troca de mensagens (comunicadores), navegação, distribuição de arquivos, uso de comércio eletrônico e de Intenet Banking.

Vírus:

São programas desenvolvidos para alterar, nociva e clandestinamente, aplicativos instalados em um computador. Eles têm comportamento semelhante ao do vírus biológico: multiplicam-se, precisam de um hospedeiro e esperam o momento certo para o ataque.

Medidas de proteção contra vírus:

- instalar e manter atualizado um bom programa antivírus;
- desabilitar no seu programa de e-mail a auto-execução de arquivos anexados às mensagens;
- não executar ou abrir arquivos recebidos por e-mail antes de verificá-lo pelo programa antivírus;
- não abrir arquivos ou executar programas de procedência duvidosa ou desconhecida;
- procurar utilizar, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, tais como RTF ou PDF;
- no caso de arquivos comprimidos, procurar não utilizar o formato executável.

Utilize o formato tipo arquivo.ZIP.

E-mail:

Grande parte dos problemas de segurança envolvendo e-mails estão relacionados aos conteúdos das mensagens. Para configurar seu programa de e-mail (ex: Outlook) de forma mais segura:

1. Desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;

2. Desligar as opções de execução do JavaScript e de programas Java;

3. Desligar, se possível, o modo de visualização de e-mails no formato HTML.

Estas configurações podem evitar que o seu programa de e-mail propague automaticamente vírus e cavalos de tróia.

Cavalos de Tróia:

São sistemas que instalam programas para possibilitar que um invasor tenha controle total sobre um computador. Tais programas permitem que o invasor, de forma imperceptível, veja e copie todos os arquivos armazenados no computador e descubra todas as senhas digitadas pelo usuário. As principais medidas preventivas contra a instalação de cavalos de tróia são semelhantes às medidas contra a infecção por vírus, além da instalação de um firewall.

Firewalls:

São dispositivos que podem ser constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso entre redes de computadores. O firewall pessoal é um software ou programa utilizado para proteger um computador contra acessos não autorizados vindos da internet, e constitui um tipo específico de firewall.

Na próxima edição do Jornal SBC, a seção Cardionautas trará explicações sobre segurança em comércio eletrônico e Internet Banking, salas de bate-papo, comunicadores tipo ICQ, Odigo, Messanger, Navegação na Internet, Backdoors, Vulnerabilidade e Worms.

Augusto Uchida