Segurança no Uso da Internet

André Domingues Rocha de Oliveira

Fabrício Vieira Bonfim

Atualmente, o computador doméstico tem sido usado para diversas coisas e não apenas para trabalho. Compras, transações financeiras, contatos em sites de relacionamento, são algumas das diversas tarefas para as quais ele é usado, além dos trabalhos profissionais. Por isso, a preocupação com a sua segurança aumenta. Pois os prejuízos pelas perdas de dados e arquivos são muito maiores. É possível perder dinheiro, ter a identidade usada falsamente por um estranho, o acesso à internet ser usado por alguém não autorizado, perder dados e, até mesmo, ter a máquina comprometida a ponto de parar funcionar.

Pensando nisso, para evitar o transtorno de um computador invadido, exposição de dados confidenciais e a perda de dados, algumas precauções devem ser tomadas e algumas, das mais comuns, situações serão analisadas a seguir.

A primeira delas é o uso adequado de senhas. Para evitar que dados sejam invadidos de maneira mais simples, pela descoberta de uma senha. É necessário haver um cuidado ao criar uma senha, sem conter informações óbvias e fáceis de serem descobertas. Uma senha é considerada segura quando tem 8 caracteres, e entre eles é aconselhável haver letras, números e símbolos. Além disso, é aconselhável mudar a senha de tempos em tempos.

Outra dica é escolher uma frase e pegar a primeira, segunda ou última letra de cada palavra. Como o exemplo citado na cartilha de segurança: “batatinha quando nasce se esparrama pelo chão”, pode-se gerar a senha “!bqnsepC”. São senhas de fácil memorização e difícil de serem descobertas. Logo, uma precaução importante é saber escolher uma senha adequada, que não seja fácil a ponto de qualquer conhecido ou não, descobririr. Uma senha realmente difícil de ser descoberta, mas que o usuário lembre sempre.

Usar um programa de leitor de e-mails é outra situação a ser analisada, pois pode trazer sérios riscos ao computador, que não compensam a comodidade que ele oferece. A maioria desses problemas de segurança, se deve ao conteúdo das mensagens; uma vez que, alguns programas permitem que arquivos ou programas anexados a mensagem, sejam abertos e/ou executados automaticamente.

Mas, se o uso desse programa for necessário, é possível configurá-lo para que ele fique mais seguro. Pode-se desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens; desligar as opções de execução de *JavaScript* e de programas *Java*; e desligar, se possível, o modo de visualização de e-mails no formato HTML.

Outro fator a ser analisado é a vulnerabilidade da máquina. Este termo se refere a uma falha na implementação, no projeto, ou configuração de um *software* ou sistema operacional que, quando explorada por um estranho, ocasiona a violação da segurança de um computador.

Existem casos em que um *software* ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável. Deste modo, o usuário deve identificar, prevenir e corrigir as vulnerabilidades de sua máquina.

Para evitar transtornos, causados pela falta de segurança do computador, é essencial usar sempre um bom antivírus, que identifica e elimina a maior quantidade possível de vírus e outros tipos de *malware*.

Sendo assim, para proteger a máquina e usá-la com mais segurança é necessário, primeiramente, que o usuário se mantenha atualizado sobre as formas de invasão e combate. Pois sempre são

atualizadas as formas tanto de invasão, quanto de combate às mesmas. O usuário deve usar a internet, os artigos, fóruns, dentre outras ferramentas, para se manter informado sobre essas questões. Ele deve atentar-se as formas mais comuns de invasão, como as que foram descritas acima. Com o intuito de evitar e combater a insegurança sua máquina, protegendo seus dados e, consequentemente, sua segurança.