**Recomendações de segurança contra ataques cibernéticos - STI/UFC**

1. Mantenha o sistema de seu computador atualizado. Em algumas máquinas, a opção de atualização do sistema operacional Windows é feita automaticamente; em outras, é preciso checar se há opção de atualização disponível. Para verificar, basta acessar o Painel de Controle do computador, selecionar a opção Windows Update ou Atualização e Segurança – o termo pode variar de uma máquina para outra – e solicitar a atualização do sistema. A STI recomenda que se adote, se possível, a versão Windows 10;

2. Alguns sistemas Windows não possuem atualização disponível, geralmente, por se tratar de versões antigas. Para esses casos, após o ataque cibernético da última semana, a Microsoft lançou correções de emergência. No catálogo de atualização da Microsoft há uma lista de links para download de atualizações de vários sistemas;

3. Em último caso, desative o SMB. Caso não consiga fazer a atualização de seu sistema, é preciso desativar o Server Message Block (SMB), que foi a "porta de entrada" do vírus do ciberataque global. O tutorial com orientações sobre como fazer a desativação pode ser visto on-line;

A atualização do software de antivírus também é importante. Recomenda-se, ainda, a realização regular de backup: tenha cópia de seus arquivos mais importantes, mantendo-os salvos em um dispositivo de armazenamento externo.
Documentos não solicitados enviados por e-mail são suspeitos. Nunca clique em links desses documentos, a menos que verifique a fonte. O principal vetor dessa infecção são os spams, não importando quão segura é nossa rede.

Fonte:Secretaria de Tecnologia da Informação da UFC. Disponível em: http://ufc.br/noticias/noticias-de-2017/9653-sti-divulga-recomendacoes-de-seguranca-contra-ataques-ciberneticos. Acesso em: 07 maio 2020.

Atualizado em: 07/05/2020