Equipe de TI do Hospital Dr. Hélio Angotti divulga alerta contra ataques cibernéticos

Esta semana, o Hospital de Câncer de Barretos foi alvo de ataque de *hackers*, em ação semelhante à que ocorreu simultaneamente em outros países. Os “piratas” do ciberespaço sequestram dados das empresas atacadas e exigiram quantias em *bitcoins* (moeda digital).

Cerca de 1.000 computadores de várias unidades do Hospital de Barretos foram afetados e os *hackers* exigiram US$ 300 por PC, como resgate. Isto é, US$ 300 mil no total, ou R$ 1 milhão. O pior: cerca de 6.000 pacientes com atendimento comprometido. A Radioterapia foi o setor mais prejudicado.

Todo cuidado é pouco e, como se vê, nem mesmo os hospitais são poupados. Muito pelo contrário, eles possuem dados em quantidade e qualidade capazes de torna-los vulneráveis, ao menos descuido com a segurança cibernética.

Por isso, a Assessoria de Comunicação e a equipe de Tecnologia da Informação (TI) do Hospital Dr. Hélio Angotti elaboraram uma campanha disparada por e-mail e redes sociais, alertando para o perigo. As dicas de segurança valem tanto para os PCs utilizados nas estações de trabalho dentro da instituição quanto para os acessados em casa.

Para quem não teve tempo de ver os alertas da campanha, abaixo estão as dicas divulgadas ao longo da semana. Confira!

Vamos evitar ataques cibernéticos. Veja dicas valiosas da nossa TI!

ANTIVÍRUS

O antivírus não é único responsável pela segurança do computador, mas é um primeiro passo para se proteger. Quanto melhor e mais atualizado o antivírus, maior a proteção. Os pagos que existem no mercado são superiores aos gratuitos, já que oferecem amplo suporte. Mas um antivírus gratuito já ajuda na prevenção e alertas.

SISTEMA OPERACIONAL ATUALIZADO

Quando o sistema está desatualizado é muito mais fácil para os hackers conseguirem se infiltrar no PC. Atualize sempre seu sistema. As atualizações podem ser automáticas ou manuais. Uma das melhores formas de manter seu computador livre de agressores é aplicando patches (correções) e outras verificações de software assim que eles se tornam disponíveis.

NÃO ACESSE LINKS DESCONHECIDOS

Em e-mails, sites, programas de conversa, ou praticamente tudo o que se acessa na internet pode, vez ou outra, conter algum link de caráter malicioso. Atenção, cuidado e precaução em qualquer situação é essencial e auxilia na proteção de seus dados e sistema operacional.

NÃO ENVIAR DADOS PESSOAIS POR E-MAIL

Tente, o máximo possível, não enviar seus dados pessoais, senha de conta e dados bancários, entre outros. Afinal, se o hacker tiver acesso a senha do seu e-mail, acessa também todos os dados enviados ou recebidos.

SENHAS IMPROVÁVEIS E DIFERENTES EM CADA SITE

Coloque senhas diferentes em sites de compras, banco, emails, e outros serviços. Mesmo que alguém descubra sua senha e login de um determinado site, não será possível acessar outros com a mesma combinação. Com isso você minimiza os danos em caso de algum acesso indevido.

CUIDADO EM DOWNLOADS

Downloads são um dos grandes motivos de entrada de vírus nas máquinas. Fique muito atento aos botões de download; alguns sites pode dar a entender que o download será feito por um link que, na verdade, acarretará em vírus.

ATENÇÃO NA INSTALAÇÃO DE PROGRAMAS

Preste atenção a todos os softwares adicionais que o programa indica durante a instalação. Evite aceitar tudo durante o processo, pois muitos softwares indicam instalação de outras coisas adicionais que, mesmo que não tenha códigos maliciosos, podem deixar seu computador mais lento e vulnerável.

ARQUIVOS “.EXE” E “.SCR”

Um truque simples para verificar se o link contém vírus é passar o mouse sobre ele (sem clicar) e verificar – no canto inferior esquerdo a barra de status do navegador – qual o local que você será encaminhado se clicar nele.
Caso se trate de um “.exe” quer dizer que é um executável, ou seja, um programa, provavelmente, e não site. Então, a possibilidade de ser um malware (programa malicioso) é muito grande. Não clique nele sem ter certeza do que se trata. Evite links que aparecem com extensão “.scr” e links com endereços que você não conheça ou tenham nomes estranhos.

CUIDADO COM SITES DESCONHECIDOS

É comum, principalmente quando se recorre a buscadores, ser encaminhado para sites desconhecidos de compras, para assistir a vídeos, ou outras ações. Alguns usuários possuem malícia o suficiente para conseguir operar em tais sites sem adquirir vírus, mas para leigos evitar tais páginas, pelo menos no início, é essencial.

ATENÇÃO A E-MAILS DE BANCO FALSOS

É comum, golpes com e-mails que tenha a logo ou a aparência do seu banco para lhe induzir ao erro. Verifique sempre qual o endereço do remetente para garantir sua segurança; deve ser do tipo “algumnome@seubanco.com.br”. E o banco nunca solicita envio de dados por e-mail ou download de atualizações por e-mail. Sempre que receber e ficar em dúvida, confirme com seu gerente antes de clicar em qualquer link.

Paulo Ferreira
Assessor de Comunicação
paulo.ferreira@helioangotti.com.br
55 34 3328 9918
55 34 9 92047205
Hospital Dr. Hélio Angotti - Hospital de Câncer de Uberaba
Salve Vidas! Acesse www.helioangotti.com.br
https://.facebook.com/hhelioangotti