IDG NOW! tecnologia em primeiro lugar http://www.idgnow.com.br

SEGURANÇA >

Segurança: 5 dicas para você não ser vítima de golpes por email

(http://idgnow.uol.com.br/seguranca/2011/04/07/seguranca-5-dicas-para-voce-nao-ser-vitima-de-golpes-por-email)

Por CSO/EUA

Publicada em 08 de abril de 2011 às 09h00

Links anexos, arquivos que devem ser baixados e outra miríade de artifícios fazem parte do arsenal de cibercriminosos.

A técnica de tentar infectar uma máquina com base em emails contendo arquivos anexos ou tentando se passar por outra pessoa é quase milenar. Ainda assim, e possivelmente por força de sua permanência no meio digital, essas técnicas foram refinadas e passam a representar um perigo maior do que o de anos passados.

Segundo o departamento para emergências de informática dos EUA (US-Cert), os emails do tipo phishing foram responsáveis por 53% dos incidentes de segurança na América do Norte, em 2010.

Ocorre que os ataques via email da atualidade são feitos sob medida para atingir um determinado usuário dentro de uma organização específica. Depois da recente invasão e do furto de dados de clientes ocorrido nos servidores da Epsilon, especialistas sugerem a clientes de bancos que se preparem para uma onda de ataques baseadas nas informações obtidas no ataque.

Os dias em que phishers (quem envia os emails falsos) mandavam uma centena de emails iguais para várias caixas de entrada e com mensagens sem o mínimo de personalização ou lotadas de erros de grafia são – quase – página virada na história. Os criminosos digitais perceberam que com um pouco mais de trabalho e levantamento de informações sobre a vítima, é possível armar esquemas que passam confiança aos olhos do usuário menos experiente. Afinal de contas, infectar uma máquina é suficiente para comprometer a segurança de toda a rede corporativa.

Leia também: Golpes de phishing são mais eficazes entre usuários de smartphone

“Vemos cada vez mais cenários em que dois ou três emails são enviados contendo arquivos maliciosos”, avisa Jim Hansen, da empresa de segurança digital PhishMe.

Com o objetivo de oferecer aos usuários uma forma de se defenderam desse tipo de ataque, a PhishMe desenvolveu um treinamento que visa mudar o comportamento das pessoas em casos de eventuais ataques via phishing email.

Veja quais são as dicas:

Ceticismo é bom
Tenha sempre prontas as perguntas: de quem veio esse email? “Casos seja alguém desconhecido, as chances de ser uma mensagem absolutamente inútil/maléfica são grandes”, adverte Hansen. Sempre vale a pena investigar o domínio de envio do email no Google antes de prosseguir na abertura da mensagem. O domínio é toda a parte que fica do lado direito da @. Exemplo: *atendimento@dominio22997765.com.br*

“Sei que somos, todos nós, pessoas bastante ocupadas, mas não custa prestar atenção na hora de verificar seus emails”, completa.

Com anexos, todo cuidado é pouco
“Se, ao abrir um email, você for orientado a fazer o download de arquivos – sejam estes de qual natureza forem – não o faça”, adverte Hansen. Para ele, na melhor das hipóteses, o usuário receberá uma dúzia de mensagens irrelevantes, poucas horas depois de abrir os anexos. “Já na pior”, continua Hansen, “você estará abrindo o seu computador para um hacker”.

Não interessa se a mensagem for enviada por alguém desconhecido ou alguém que você conheça bem – confirmar com a pessoa o envio, antes de abrir, o anexo, é fundamental.

Ignore instruções – sejam estas quais forem
“Cada vez que uma mensagem instrui um usuário a realizar uma ação, vale a pena dobrar o cuidado com essa mensagem”, diz Hansen. Para o consultor, se uma coisa parece boa demais para ser verdade, é mentira.

“Normalmente, o criminoso apela para uma tática baseada em dois princípios: recompensa ou autoridade”, diz.

Nos golpes em que o hacker tenta se passar por uma autoridade, ele irá tentar persuadir o usuário a tomar alguma medida em nome de um órgão ou departamento de Estado ou da própria empresa. A mensagem pode dizer que seu computador está

infectado, e que você deve clicar imediatamente em um link para executar a desinfecção automática do computador. Em outra modalidade, na mesma linha, a mensagem diz ser do RH e pede que você complete um formulário online. Existem, ainda, os casos em que quem envia a mensagem afirma ser de seu banco e que sua conta corrente fora invadida, em seguida irá pedir para o usuário confirmar seus dados, incluindo a senha.

Nos casos em que são oferecidas recompensas, existe uma miríade de golpes. Desde prêmios em dinheiro, a iPads – todas vão requerer que o usuário complete algum formulário obscuro.

“Não dê atenção a essas tentativas”, adverte Hansen.

Verifique o link
Para onde aponta o link da mensagem? “Quase todas as mensagens malintencionadas apresentam um link em que o usuário é persuadido a clicar”, diz Hansen. Apesar de teoricamente esse link apontar para sua conta no Facebook ou sua conta bancária, o destino desse atalho pode ser bem menos relevante que isso.

A maneira mais fácil de descobrir a autenticidade do atalho é encostar com o mouse em cima do link e observar, no rodapé da janela de navegação ou do cliente de email, para onde esse link realmente aponta.

Possivelmente, o atalho exibido mostre um número IP, como 192.168.1.1 – já é um bom indicativo de que você não vai gostar do que se esconde atrás desse atalho.

Ainda: com a popularização de encurtadores de URL como o bit.ly, ficou quase impossível descobrir o real destino do link na mensagem. Existe, porém, uma maneira de verificar o destino do atalho: Copie o link encurtado, que deverá se parecer com *bit.ly/ju897897hyt* e cole-o na barra de endereços do navegador, adicionando um sinal de adição ao seu final. O resultado final será *bit.ly/ju897897hyt+*. Ao pressionar enter depois de inserir esse atalho, o usuário é levado até a página do encurtador, onde poderá verificar o destino do link, sem correr qualquer risco. Nessa página, também verá quantas vezes o link foi clicado desde sua criação. Saiba que se for, de fato, um atalho para uma página de banco ou sua página do Facebook, o número de cliques deverá ser zero.

Lembre-se do telefone
Faz tempo que não usa seu telefone para sua finalidade original, não faz? Bem, para muitos de nós, esse método arcaico de comunicação remete aos tempos da inquisição. Mesmo assim, tem sua utilidade nos dias de hoje.

Hansen sugere: “se você desconfia da autenticidade da mensagem e, ainda assim, ela urge que você tome uma atitude, passe a mão no telefone e ligue para a pessoa que – em tese – lhe enviou essa mensagem. Sim, se preferir pode mandar uma mensagem texto pelo telefone”.

(Joan Goodchild)