Coluna

Agosto - 2019 - ed. 117

Segurança.doc

Frederico Guerra é
assessor de Segurança da
Informação do TRE-RJ

Precisamos falar sobre *phishing*

Phishing é um método de fraude digital no qual são enviadas, aleatoriamente, mensagens não autorizadas em nome de empresas e instituições confiáveis, com o objetivo de induzir pessoas a fornecerem ou facilitarem a obtenção de dados bancários, de cartão de crédito, de senhas de acesso ou de outras informações pessoais ou sigilosas. À primeira vista pode parecer que os comunicados foram feitos especialmente para quem os recebeu, pois empregam o nome de lojas e instituições com as quais boa parte da população possui algum tipo de relacionamento. Porém, na modalidade comum, o *phishing* é disparado para e-mails obtidos em listas de spam. Precisamos falar sobre phishing ou gerados por computadores. As mensagens podem se apresentar de diversas formas, como avisos de cancelamento de acesso, alerta de gastos no cartão de crédito ou uma promoção imperdível naquela loja de comércio eletrônico que você costuma comprar. Apesar de as abordagens serem variadas, elas seguem mais ou menos o mesmo roteiro: há um comunicado, em padrão compatível com o da comunicação oficial das pessoas jurídicas, para que os destinatários, em razão de um evento plausível, pratiquem uma ação urgente, clicando em links, fornecendo login e senha ou abrindo arquivos anexos, sob pena de sofrerem as consequências de sua omissão.

Com isso os golpistas pretendem, por meio da manipulação de estados emocionais de medo e urgência que interfiram na nossa capacidade de reflexão, nos convencer a instalar arquivos maliciosos ou fornecer, em páginas falsas, informações que serão utilizadas para roubo de identidade, desfalque em contas bancárias, fraudes de cartão de crédito e venda de dados. Há, ainda, uma variante mais perigosa chamada *spear phishing*, na qual o ataque é direcionado para pessoas específicas, utilizando dados previamente coletados. Nessa hipótese, os fraudadores podem se passar por pessoas conhecidas, autoridades ou funcionários do lugar onde as vítimas trabalham. Caso receba no e-mail institucional alguma mensagem não solicitada com esse perfil, fique atento a estas dicas: nunca clique nos links fornecidos, preencha formulários, digite senhas ou abra arquivos anexos; selecione-a como spam e depois apague. Isso ajuda a aprimorar o filtro de e-mails, impedindo que a mensagem chegue para outros; se achar que é mesmo verdadeira, confirme com o suposto remetente sem utilizar os meios fornecidos na mensagem; caso tenha clicado no link ou executado o arquivo, deixe a vergonha de lado e entre em contato com a Central de Serviços de TI.