Proteja-se!

Secretaria de Tecnologia da Informação - SETIN
Coordenadoria de Gestão da Informação e Inteligência Organizacional - CINT
Seção de Segurança da Informação - SSEGI

Engenharia social

Nº 10, julho de 2014

Engenharia social é a habilidade de obter dados confidenciais através do uso da persuasão. Muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou dados.

A engenharia social pode utilizar meios computacionais ou não. Uma de suas formas mais comuns se apresenta através do envio de e-mails, cujo remetente se passa por uma pessoa ou empresa conhecida pelo usuário.

Esses e-mails, que podem ser classificados como *scam* ou como *phishing*, apresentam conteúdo que procura induzir o usuário a fornecer informações ou executar programas maliciosos em seu computador ou dispositivo móvel.

O ***scam*** é uma variante do *spam*; termo usado para se referir aos e-mails não solicitados enviados em massa; que contém um arquivo anexo ou link para download, cuja execução instala um código malicioso.

O ***phishing***, originário do termo inglês *fishing,* é um tipo de fraude eletrônica caracterizada por uma tentativa de obter dados confidenciais de pessoas ou empresas, que pode fazer uso, além do e-mail, de serviço de mensagens instantâneas ou redes sociais.

Há ainda uma variante do *phishing*, chamada de ***pharming***, cuja característica é o redirecionamento da navegação do usuário para uma página falsa, por meio de alterações no serviço de resolução de nomes (*Domain Name System* - DNS).

O ***vishing*** ou *voice phishing* é uma técnica que não utiliza meios computacionais, mas a telefonia para prática da engenharia social.

Importante

Fique atento às mensagens ou ligações, em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links. Elas podem ter sido enviadas de contas invadidas, perfis falsos ou podem ter sido forjadas.

Tenha cautela ao acessar links. Procure digitar o endereço diretamente no navegador, e não clique no link apresentado na mensagem.

Verifique se a página utiliza conexão segura. Sites de comércio eletrônico, bancos e instituições financeiras confiáveis sempre utilizam conexões seguras, geralmente representadas pelo protocolo "*https*" no início do endereço, bem como, pela figura de um cadeado.

Encerre sua conexão caso, ao digitar um endereço, seja redirecionado para outro site, o qual tente realizar alguma ação suspeita, como a abertura de um arquivo ou a instalação de um programa.

Utilize um filtro *antiphishing*, a maioria vem integrado aos principais navegadores e antivírus, e serve para alertar os usuários quando uma página suspeita de ser falsa é acessada.

Acesse a Política de Segurança da Informação em http://aplicacao.tst.jus.br/dspace/handle/1939/27977

Na intranet, todos os boletins podem ser acessados em http://autoatendimento.tst.jus.br/index.php?option=com_docman&Itemid=62

Participe! Caso tenha alguma dúvida, sugestão ou crítica envie para ssegi@tst.jus.br