

STI alerta para e-mails falsos

Conhecidos como phishing scam ou scam, são utilizados para persuadir as vítimas

Provavelmente você já deve ter recebido algum e-mail, em nome de uma empresa, serviço ou instituição, solicitando para clicar em um link no texto da mensagem. No entanto, o link não apontava para o que a mensagem oferecia, mas sim para um site falso com o mesmo layout de um site verdadeiro ou para um arquivo executável contendo vírus, visando capturar informações do computador da vítima.

Esse tipo de e-mail é conhecido como phishing scam ou simplesmente scam. Os temas mais utilizados para persuadir as vítimas são:

Cartões virtuais: Mensagens com links para a visualização de falsos cartões virtuais. Desconfie sempre que receber cartões virtuais de remententes desconhecidos;

Informações financeiras: Mensagens, geralmente em nome de bancos, financeiras ou operadoras de cartão de crédito, solicitando ao usuário o cadastramento de informações. Instituições financeiras não enviam e-mails sem a solicitação ou a autorização prévia do cliente;

Atualizações de software: Mensagens solicitando ao usuário que clique em um link para instalar um determinado software com o suposto objetivo de atualizar seu computador. Somente efetue o download de softwares a partir dos sites oficiais de instituições conhecidas;

Notificações de pendências: Mensagens, geralmente em nome de instituições financeiras, órgãos da justiça ou do governo, solicitando ao usuário que clique em um link para regularizar uma suposta pendência judicial, um débito ou algum documento. Instituições financeiras e órgãos da administração direta e indireta não enviam notificações via e-mail;

Relacionamentos: Mensagens contendo convites para sites de relacionamento (Ex.: Orkut), fotos ou mensagens de teor íntimo. Desconfie sempre que receber mensagens de remententes desconhecidos.

Sempre desconfie de mensagens de remetentes desconhecidos ou contendo erros de ortografia e gramática.

A Secretaria de Tecnologia da Informação, através da Divisão de Segurança da Informação, elaborou uma cartilha contendo dicas sobre como utilizar o correio eletrônico de forma segura. O documento está disponível em Cartilha de SI - Correio eletrônico.

A Divisão de Segurança da Informação recomenda a leitura desse e de outros documentos relacionados à Segurança da Informação, disponíveis na Intranet - Informática - Manuais on line - Política de Segurança da Informação .

Veja exemplos de e-mails falsos que circulam na Internet:

0 visualizações nos últimos 30 dias

Tribunal Regional do Trabalho 13ª Região - Paraíba

Av. Corálio Soares de Oliveira, S/N, Centro - João Pessoa/PB - (próximo à Praça da Independência) - 58013-260 - CNPJ: 02.658.544/0001-70 Fone: (83) 3533-6000
