

GOLPE ELETRÔNICO

Usando como isca e-mails com promessas de dinheiro fácil, um remédio milagroso ou supostas necessidades de recadastramento de dados, um novo tipo de bandido usa o computador como arma para aplicar golpes na internet. O objetivo é roubar dados financeiros das vítimas. A fraude se chama phishing, junção dos termos password fishing (pescaria de senhas, em português). Veja como o golpe é aplicado:

• Como os criminosos descobrem seu e-mail

Listas de endereços de e-mail são vendidas pela internet. Também existem ferramentas que varrem a web em busca de endereços (por exemplo, os estampados em blogs). E há hackers especializados em invadir servidores para furtar informações de correio eletrônico.



• O que eles fazem com os endereços

Utilizando programas de envio de e-mail em massa (spam), distribuem mensagens fraudulentas a milhares de pessoas. Para não serem pegos, enviam os spams a partir de computadores de lan houses ou redes sem fio alheias. Mas o mais comum é o uso de botnets (redes de robôs). São PCs que, sem os donos saberem, foram contaminados e passaram a ser controlados à distância pelo hacker.

• Como controlam o computador alheio

1. Se a pessoa clicar em um link de um e-mail fraudulento, instalará no seu micro, sem saber, um cavalo-de-troia. Agindo silenciosamente, o cavalo-de-troia espiona o uso do computador. Quando a vítima acessa um banco pela internet, o programa envia os números das senhas diretamente para os bandidos.



2. A pessoa é remetida a uma página não-solicitada da internet. Pode ser um site que leve à instalação de um cavalo-de-troia no micro.

3. É encaminhada para a página clonada de um banco. Acreditando estar acessando sua conta, envia suas senhas para os criminosos.

• O que eles fazem com os dados da vítima

Limpam a conta bancária dela, transferindo o dinheiro para contas de laranjas ou quitando faturas de terceiros pela internet.

