Várias formas de enganar internautas

Os estelionatários virtuais têm diversas estratégias para induzir o internauta a clicar num link que descarrega um programa nocivo no computador ou a entregar seus dados confidenciais. Veja abaixo quais são os tipos mais comuns e fique atento. Na dúvida, não clique em nada. E nunca entregue seus dados confidenciais por e-mail.

CARTÕES E MENSAGENS - Esse tipo de e-mail falso engana muita gente, pois geralmente a aparência é convincente, com desenhos. Se quiser mesmo abrir o cartão, vá ao site oficial do serviço e dê o número do cartão, que deve vir na mensagem de e-mail. Não clique no link.

NOTIFICAÇÕES FINANCEIRAS CADASTRAIS - Esses temas também são recorrentes em e-mails falsos. São avisos de pagamentos, débitos e cobranças, problemas no CPF, entre outros problemas do tipo. Não acredite em mensagens do tipo "O seu CPF consta na Serasa" ou "Seu CPF foi cancelado pela Receita Federal". Entidades e empresas sérias não resolvem assuntos tão importantes por e-mail.

TEMAS ADULTOS - O sexo é um dos maiores atrativos da internet. Certamente, também engana muita gente, que clica em links que prometem fotos, mas na verdade só servem para instalar softwares nocivos.

NOTÍCIAS SENSACIONALISTAS - "Osama bin Laden foi preso!" ou "Veja aqui imagens em primeira mão" são exemplos de iscas usadas por estelionatários virtuais para capturar senhas bancárias. Se você quer se informar, procure sites de notícias de credibilidade.

SOFTWARES ÚTEIS - Há golpes virtuais que oferecem downloads de programas ou atualizações do sistema. Não acredite nisso. Faça downloads apenas de sites oficiais.

PRÊMIOS E PROMOÇÕES - Se alguém o abordasse, dizendo que ganhou um prêmio milionário, você acreditaria? Na internet, a cautela deve ser a mesma que nas ruas. Não acredite em presentes sensacionais ou promoções incríveis que chegam no seu correio eletrônico.

PIADAS - Tem gente que não resiste a uma piadinha recebida por e-mail. Mas aqueles que clicam nos links nem sempre têm uma história engraçada para contar depois

Para não ter senha da conta bancária roubada, fique atento ao lidar com correio eletrônico: nunca clique em mensagens suspeitas

Kátia Arima e Rodrigo Martins

Depois de voltar de férias, a publicitária Évora Ferraz abriu o site do seu banco e ficou chocada: sua conta estava zerada - e não era ela que tinha gastado tudo. "Quase caí dura. Liguei tremendo para o banco, na hora", disse. Mais tarde, ela descobriu que havia sido vítima de uma fraude pela internet.

A publicitária suspeita que os criminosos obtiveram sua senha quando ela digitou seus dados no site do banco. "Estava muito lento, acho que estava sendo monitorada", disse ela, que foi ressarcida pelo banco.

Casos como o de Évora são cada vez mais comuns. Criminosos estão usando a internet para conseguir informações bancárias alheias. De posse dos dados, eles realizam transferências de valores pela internet, pagam contas e fazem saques.

Para conseguir as senhas bancárias dos internautas, os criminosos virtuais não invadem o sistema do banco, que é bastante protegido. "Eles vão pelo caminho mais fácil, que é explorar a ingenuidade do internauta", afirma o diretor do Instituto de Peritos em Tecnologias Digitais e Telecomunicações (IPDI), Otávio Luiz Artur.

As quadrilhas têm especialistas em informática, que criam vários tipos de e-mails falsos e os enviam em massa, para diversos destinatários (spams). Grande parte dos e-mails falsos induz o internauta a clicar num link, que pode instalar um ou vários programas maliciosos.

Esses softwares-espiões (spywares) podem monitorar o teclado da vítima e até capturar telas quando ela estiver usando o site do banco. Depois, toda essa informação é enviada para o criminoso pela internet, pois um programa tipo cavalo de Tróia (trojan), que foi instalado quando o internauta clicou no link do e-mail, abre a brecha.

O link pode também levar o internauta a uma página falsa. Tudo o que for digitado nos campos abertos cairá nas mãos dos criminosos. Outro método de furtar senhas são as páginas clones. O internauta clica num link de um e-mail falso, que coloca um arquivo no seu computador. Quando a vítima digitar o site do banco, esse arquivo a redirecionará para um site falso, com a aparência do verdadeiro. As informações digitadas nessa página serão enviadas para o criminoso.

OLHO VIVO
Para não cair em golpes virtuais, olhe com desconfiança para os e-mails que você recebe em nome de empresas e instituições ou pessoas desconhecidas. Senhas, números de cartão de crédito e outras informações confidenciais nunca serão solicitadas por e-mail. Caso receba um e-mail suspeito, delete-o imediatamente, antes mesmo de abrir anexos ou clicar em links.

Se quiser checar a origem do e-mail, entre em contato por telefone com a empresa ou instituição citada. Mas não ligue para nenhum número que venha na própria mensagem.

Procure saber qual é a política de segurança do seu banco. Há instituições que nunca enviam e-mail para os clientes, como o Banco do Brasil.

Na hora de digitar uma senha, verifique se o site é seguro para transações financeiras, observando se há um ícone de cadeado fechado no pé da página. Na barra de endereços, também dá para matar a dúvida, pois um endereço que começa com "https://" é seguro.

Evite ao máximo clicar em links recebidos por e-mail. Passando o mouse sobre o link, sem clicar, dá para ver o nome do arquivo no pé da página. Nunca clique em arquivos com extensão ".exe", ".com", ".scr" e ".pif", alerta José Antunes, gerente de engenharia de sistemas da empresa de segurança McAfee. Para ver a extensão dos arquivos, é preciso habilitar seu computador. Clique em Meu Computador, Opções de Pasta, Modo de Exibição e desabilite o item Ocultar Extensões.

Os e-mails falsos tentam seduzir o internauta, oferecendo prêmios, promoções, fotos, piadas, softwares úteis. Não acredite nesses "presentinhos".

Outro tipo de e-mail falso são as notificações financeiras e cadastrais. Essas mensagens pedem, em nome de empresas e instituições financeiras, que o internauta atualize seus dados ou clique num link para resolver suas pendências.

Muitos caem nos e-mails falsos de apelo sentimental, com mensagens do tipo "você está sendo traído" ou "eu te amo" e clicam em links que instalam programas nocivos.

Cartões virtuais falsos também pegam muita gente, pois a aparência costuma ser convincente. Se você ficar na dúvida, verifique se o serviço de cartões é confiável e busque o site verdadeiro. Para ter acesso ao cartão sem correr riscos, entre no site do serviço e digite o número dele, que deve vir no e-mail recebido.

Instituições financeiras

SERASA: não envia e-mails para notificação ou verificação de pendências financeiras cadastradas em seu banco de dados.
BANCO DO BRASIL: o Banco de Brasil não envia nenhum e-mail a seus clientes. Se receber algum em nome do banco, é falso.
BRADESCO: o banco envia e-mails para os clientes, mas nunca com arquivos anexados. Também não solicita informações pessoais.
BANCO REAL: não envia nunca e-mails para seus clientes. Para transações pela internet, criou a tabela de senhas.
ITAÚ: envia e-mails para os clientes. Para fazer transações pela internet, agora há um cartão de segurança.
UNIBANCO: envia e-mails para seus clientes, mas nunca solicita dados, nem anexa arquivos na mensagem de e-mail.

SAUDAÇÃO IMPESSOAL
Como são enviados em massa, para tentar fisgar o maior número possível de internautas, os e-mails falsos costumam ser impessoais. A saudação é genérica como "Oi" ou "Prezado Cliente". Se o seu nome não for mencionado, desconfie.

Atualmente, os criminosos virtuais estão mais cuidadosos, tentam criar um visual convincente, copiando logotipos e desenhos - mas nem sempre conseguem. É comum encontrar erros de português no texto do e-mail.

Junto com o bom senso do internauta, os antivírus também podem ajudar na guerra contra golpes virtuais. "É essencial que ele seja sempre atualizado", alerta o especialista em segurança da Symantec, Lúcio Costa.Também é recomendado o uso do firewall, programa que filtra a comunicação de programas instalados no seu computador - inclusive os nocivos - com a internet. E deixe o anti-spam ativado para bloquear o e-mails não solicitados.

Caso verifique saques irregulares na sua conta, avise imediatamente o banco. "Eles costumam ressarcir os clientes, para não fazer alarde", afirma o advogado especialista em direito da informática Omar Kaminsky. "Mas é importante fazer o boletim de ocorrência", disse.

=>Esse conteúdo foi tirado do encarte de informática do Estadão de 05/09/2005. Colaboração: Cássio Resende de Assis Brito, Divisão de Processamento de Dados.