CUIDADOS COM A INTERNET: *CRIMES VIRTUAIS*

CONSELHO SUPERIOR
DE TECNOLOGIA
DA INFORMAÇÃO
FECOMERCIO

70 anos
FECOMERCIO

70 anos FECOMERCIO

Presidente: Abram Szajman

Diretor Executivo: Antonio Carlos Borges

Presidente do Conselho Superior de Tecnologia da Informação: Renato Opice Blum

Marketing: Luciana Fischer e Adriano Sá

Assessoria de Imprensa: Ana Paula Vieira Rogers MTB: 27666

CUIDADOS COM A INTERNET

É impossível prever quando e como serão praticados atos criminosos pela Internet.
Eles ocorrem de muitas formas e a todo o momento. Mas a verdade é que cada um de nós pode contribuir para a diminuição de riscos, através da adoção de hábitos preventivos que, comprovadamente, funcionam.

Seguem abaixo alguns deles, úteis tanto a empresários quanto a internautas em geral:

1 Nunca acesse contas bancárias ou verifique dados confidenciais em sistemas coletivos de acesso à Internet (praças de acesso gratuito, *lan houses*, *cyber* cafés, etc). As informações podem ser acessadas por outros usuários através da utilização de programas de captação de senhas e dados. Além disso, os sites navegados **ficam registrados no histórico da máquina**, o que facilita a prática de fraudes.

2 > MANTENHA SENHAS DIFERENCIADAS E COM TROCAS PERIÓDICAS PARA CONTAS BANCÁRIAS. Não utilize a mesma senha para mais de uma conta.

3 > FAÇA COMPRAS SOMENTE EM SITES DE SUA CONFIANÇA E QUE TENHAM CREDIBILIDADE COMPROVADA. Grande parte das reclamações junto a órgãos de proteção ao consumidor se refere a problemas de **falta de entregas de produtos**.

4 > Em compras através dos conhecidos sites de leilão, tome todas as precauções para confirmar a **identidade do vendedor** (endereço, telefone, referências), bem como a veracidade das informações sobre o produto. NEM SEMPRE UM BOM PREÇO É SINAL DE UM BOM NEGÓCIO.

5 > JAMAIS ABRA ARQUIVOS ANEXOS ENVIADOS POR E-MAILS DE DESCONHECIDOS (aliás, mesmo com e-mails de amigos é melhor ser cauteloso). Existem PROGRAMAS QUE SÃO ENVIADOS COMO ANEXOS E PODEM SE AUTO-INSTALAR EM SEU COMPUTADOR PARA CAPTURAR SENHAS E OUTROS DADOS IMPORTANTES. Sem falar, claro, no risco do anexo ser um programa contendo vírus, que é **capaz de destruir todos os seus arquivos**.

6 > Atenção com a divulgação de dados pessoais em sites de relacionamento: MUITOS CRIMINOSOS TÊM SE UTILIZADO DAS INFORMAÇÕES QUE A PRÓPRIA VÍTIMA LANÇA NA INTERNET (horários, preferências, profissão, empresa onde trabalha) para aplicar golpes e, em situações extremas, até para a prática de seqüestros.

7 > BANCOS E INSTITUIÇÕES DE RENOME NÃO ENCAMINHAM E-MAILS SOLICITANDO INFORMAÇÕES, avisando sobre pendências financeiras ou exigindo atualização de cadastro. Se você receber tal mensagem, **delete imediatamente** e comunique ao banco/instituição para as averiguações necessárias (evitando que outras pessoas sejam lesadas).

8 > Ao clicar em links fornecidos por sites ou enviados em e-mails, CONFIRME SEMPRE NA BARRA DE ENDEREÇO PARA VER SE VOCÊ FOI ENCAMINHADO AO SITE QUE PRETENDIA. Existem muitos **links falsos** espalhados pela Internet que direcionam para sites fraudulentos. Por exemplo: você recebe um e-mail falso de um banco falando sobre uma promoção que pode ser visualizada através de um link. Ao clicar, você acha que foi para o site do banco, mas na verdade, pode ter sido direcionado a um site "fantasma" **para captação de dados para utilização em fraudes**.

9 > Cuidado com a utilização do e-mail corporativo (aquele fornecido pelos empregadores e que tem o nome da empresa após o @). Ele é uma ferramenta de trabalho de propriedade da empresa e, desde que o empregado seja devidamente avisado, **pode ser monitorado pelo empregador**.

10 > Ao empresário, cabe aqui um alerta: **o empregador pode ser responsabilizado pelos danos que seu empregado, no exercício da função, causar a terceiros, inclusive pela Web**. O Estatuto da Criança e do Adolescente, por exemplo, prevê que é crime fornecer equipamentos ou sistemas para a prática de pedofilia. Assim, se o empregado pratica crimes através do e-mail ou sistema eletrônico da empresa, o empregador eventualmente poderá ser responsabilizado por isso.

11 > Pouca gente sabe, mas um e-mail ou página de um site impresso pode ser uma prova fraca para a comprovação de crime eletrônico. O ideal mesmo é que, flagrada a prática de um crime (calúnia, pedofilia, pirataria, entre outros) a autoridade policial especializada seja imediatamente avisada. A alternativa é a lavratura de "ata notarial", através da qual o funcionário de

um cartório de notas pode atestar que no dia/hora/minuto havia determinada imagem ou informação circulando indevidamente pela Internet. Como a ata do cartório tem fé pública, a prova da existência do crime fica mais robusta, facilitando a responsabilização dos infratores.

12 > Se você tem um site na Internet, cuidado com a utilização de programas de captação de dados sem autorização do cliente ou exigência de cadastro prévio para a venda de produtos. O Código do Consumidor é claro no sentido de que o consumidor **tem que ser consultado** sobre a criação de cadastro com seus dados e proíbe que as vendas em geral sejam condicionadas a cadastros prévios de dados dos consumidores.

13 > As regras de **direitos autorais** (que proíbem cópias parciais ou integrais de conteúdos) também valem na Internet. Portanto, constitui crime a cópia de qualquer conteúdo sem a expressa autorização do autor. A exposição de conteúdo na Rede, por si só, não significa autorização para cópia sem citação de fonte ou para sua modificação.

CONSELHO SUPERIOR
DE TECNOLOGIA
DA INFORMAÇÃO
FECOMERCIO

70 anos FECOMERCIO

WWW.FECOMERCIO.COM.BR