PRIVACIDADE

Cuidados com dados pessoais em páginas Web, blogs e sites de redes de relacionamentos

♻ Evite disponibilizar seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc.);
♻ Evite disponibilizar dados sobre o seu computador ou sobre os *softwares* que utiliza;
♻ Evite fornecer informações sobre o seu cotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao caixa eletrônico, entre outros);
♻ Nunca forneça informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja sendo realizada uma transação (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o *site*;
♻ Criptografe todos os dados sensíveis, principalmente se for um *notebook*;
♻ Sobrescreva os dados do disco rígido antes de vender ou se desfazer do seu computador usado.

Cuidados com telefones celulares, PDAs e outros aparelhos com bluetooth

♻ Mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário;
♻ Fique atento às notícias, principalmente àquelas sobre segurança, veiculadas no *site* do fabricante do seu aparelho;
♻ Aplique todas as correções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
♻ Caso você tenha comprado uma aparelho usado, restaurar as opções de fábrica antes de inserir quaisquer dados.

Informações adaptadas de: http://cartilha.cert.br/

Tiragem: 200 exemplares . Bento Gonçalves, RS . Outubro 2011 . **Formatação:** Alessandra Russi
Elaboração: João H. R. Figueiredo **Revisão:** Giovani Capra

RECICLANDO IDEIAS

5

SEGURANÇA NA INTERNET

PREVENÇÃO CONTRA RISCOS E CÓDIGOS MALICIOSOS

Contas e senhas

♻ As senhas devem conter pelo menos oito caracteres, entre letras, números e símbolos;
♻ Jamais utilize como senha seu nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários.

Vírus, worms, bots e botnets

♻ Instale e mantenha atualizado um bom programa antivírus;
♻ Atualize, preferencialmente diariamente, as assinaturas do antivírus;
♻ Mantenha o sistema operacional e demais *softwares* sempre atualizados.

Programas de e-mails

♻ Não clique em *links* no conteúdo do *e-mail.* Se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu navegador;

Embrapa
Uva e Vinho

- Desconfie sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado e o arquivo anexo pode ser, por exemplo, um vírus ou um cavalo de Tróia;
- Baixe programas diretamente do *site* do fabricante.

Browsers

- Certifique-se da procedência do *site* e da utilização de conexões seguras ao realizar transações via *Web*;
- Somente acesse sites de instituições financeiras e de comércio eletrônico digitando o endereço diretamente no seu *browser*, nunca clicando em um *link* existente em uma página ou em um *e-mail*;
- Sempre que for fornecer usuário e senha teste se o protocolo 'https' está disponível. Isso garante que seus dados transmitidos não são vistos por alguém que está 'grampeando' a sua conexão (por exemplo, acessar o *site* usando: https://www.exemplo.com, no lugar de http://www.exemplo.com).

Programas de troca de mensagens

- Não aceite arquivos de pessoas desconhecidas;
- Utilize um bom antivírus, sempre atualizado, para verificar todo e qualquer arquivo ou s*oftware* obtido, mesmo que venha de pessoas conhecidas;
- Evite fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- Não forneça, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito.

Compartilhamento de recursos

- Estabeleça senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador;
- Compartilhe apenas com o usuário que vai acessar seus dados, evitando que eles estejam visíveis por toda a rede.

Cópias de segurança

- Faça cópias dos dados do computador regularmente;
- Armazene as cópias em local acondicionado, de acesso restrito e com segurança;
- Considere a necessidade de armazenar as cópias em um local diferente daquele onde está o computador, para evitar a perda caso aconteça algum dano físico ao ambiente (por exemplo, um incêndio).

Fraude

Engenharia social é um método de ataque em que uma pessoa faz 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 informações. Para se prevenir:

- Não forneça dados pessoais, números de cartões e senhas através de contato telefônico;
- Fique atento a *e-mails* ou telefonemas solicitando informações pessoais;
- Não acesse sites ou siga *links* recebidos por *e-mail* ou presentes em páginas sobre as quais não se saiba a procedência;
- Sempre que houver dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entre em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.

Cuidados ao realizar transações bancárias ou comerciais

- Realize transações somente em *sites* de instituições que você considere confiáveis;
- Certifique-se de que o endereço apresentado em seu *browser* corresponde ao *site* que você realmente quer acessar, antes de realizar qualquer ação;
- Certifique-se de que a página faz uso de conexão segura (ou seja, que os dados transmitidos entre seu *browser* e o *site* serão criptografados);
- Não acesse *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros.

Boatos

- Sempre verifique se a procedência da mensagem e se o fato sendo descrito é verídico;
- Verifique em *sites* especializados e em publicações da área se o *e-mail* recebido já não está catalogado como um boato.