Cartilha de Segurança para Uso da Internet

Precauções Contra os Riscos Envolvidos com o Uso de Computadores em Rede

Este documento procura enumerar, explicar e fornecer uma série de procedimentos que visam aumentar a segurança de um computador e de posturas que um usuário pode adotar para garantir sua segurança na Internet. Um documento mais detalhado pode ser obtido em NIC BR Security Office

1. Senhas

- Construir senhas que contenham, pelo menos, oito caracteres compostos de letras números e símbolos.
- Jamais entrar com uma senha em uma máquina que várias outras pessoas compartilham (como terminais públicos em bibliotecas e laboratórios).
- Jamais utilizar, como senha, seu nome, sobrenome, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras constantes em dicionários.
- Utilizar senhas diferentes para cada serviço (email pessoal, email profissional, banco, etc);
- Alterar a senha com freqüência.

2. Vírus, Cavalos de Tróia, Spyware e Worms

- Instalar e manter atualizado um bom programa antivírus.
- Manter o sistema operacional e demais softwares sempre atualizados.
- Não executar ou abrir arquivos recebidos por e-mail, mesmo que venham de pessoas conhecidas. Se for inevitável, certifique-se que o arquivo foi verificado pelo programa antivírus.
- Não abrir arquivos ou executar programas de procedência duvidosa ou desconhecida e mesmo que você conheça a procedência e queira abrir ou

executar os mesmos, certifique-se que foram verificados pelo programa antivírus.
- Desconfiar de e-mails pedindo urgência na instalação de algum aplicativo ou correções de determinados defeitos dos softwares que você utilize.

3. Compartilhamento de Recursos

Não é recomendado o uso de compartilhamento de recursos, como impressoras ou discos, pela rede. Havendo necessidade, siga os conselhos abaixo:

- Tenha um bom antivírus instalado em seu computador.
- Sempre estabeleça senhas para os compartilhamentos.
- Não acesse recursos compartilhados de máquinas que várias outras pessoas podem utilizar (como terminais públicos em bibliotecas e laboratórios).

4. Privacidade: Cuidados com seus Dados Pessoais

- Não fornecer seus dados pessoais (como nome, e-mail, endereço e números de documentos) para terceiros.
- Nunca fornecer 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.

5. Fraude

5.1. Falsidade Ideológica

- Não fornecer dados pessoais, números de cartões e senhas através de contato telefônico.
- Ficar atento a e-mails ou telefonemas solicitando informações pessoais.
- Não acessar sites ou seguir 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, entrar em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.

5.2. Cuidados ao realizar transações bancárias ou comerciais

- Estar atento e prevenir-se dos ataques de falsidade ideológica.
- Realizar transações somente em sites de instituições que você considere confiáveis.

- Certificar-se de que o endereço apresentado em seu browser corresponde ao site que você realmente quer acessar, antes de realizar qualquer ação.
- Procurar sempre digitar em seu browser o endereço desejado. Não utilize links em páginas de terceiros ou recebidos por e-mail.
- Certificar-se que o site faz uso de conexão segura, ou seja, que os dados transmitidos entre seu browser e o site serão criptografados e utiliza um tamanho de chave considerado seguro;
- Não acessar sites de comércio eletrônico ou Internet Banking através de computadores de terceiros.

5.3. Boatos

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

6. Spam

6.1. **Como previnir**

- Evitar responder a um spam ou evitar o envio de e-mail solicitando a remoção da lista.
- Não seja um "clicador compulsivo". Não execute arquivos anexados em e-mails sem examiná-los previamente com antivírus, bem como, não clique em URLs incluídas em e-mails.
- Fazer uso do Sistema Anti-Spam oferecido para usuários da UNIVAP.

6.2. Como reclamar

- Para reclamar o recebimento de um spam, é necessário que seja enviada a mensagem recebida acompanhada do seu cabeçalho completo(header) para o endereço spam@univap.br

6.3. Maiores informações

- Antispam.br - mantido pelo Comitê Gestor da Internet no Brasil (CGI.br).
- Cartilha de Segurança para Internet - mantido pelo Comitê Gestor da Internet no Brasil (CGI.br).

Revisão #3
Criado 2024-09-24 15:45:31 -03 por Kajita
Atualizado: 2024-09-26 13:52:47 -03 por Kajita