Cartilha de Segurança para Internet
Checklist

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Este *checklist* resume as principais recomendações contidas no documento intitulado "Cartilha de Segurança para Internet", que procura enumerar, explicar e fornecer um guia para 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. O documento original pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Para informações sobre *copyright* e distribuição, veja o documento original.

A numeração adotada neste *checklist* não possui relação com a adotada nas outras partes desta Cartilha.

---

1 Prevenção Contra os Riscos Envolvidos no Uso da Internet

1.1 Senhas

- ❒ elaborar sempre uma senha que contenha pelo menos oito caracteres, compostos de letras números e símbolos;
- ❒ 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 uma senha diferente para cada serviço;
- ❒ alterar a senha com freqüência.

1.2 Vírus e cavalos de tróia

- ❒ instalar e manter atualizado um bom programa antivírus;

- ❒ desabilitar no seu programa de *e-mail* a auto-execução de arquivos anexados às mensagens;
- ❒ não executar ou abrir arquivos recebidos por *e-mail*, mesmo que venham de pessoas conhecidas, mas caso seja 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 abrí-los ou executá-los, certifique-se que foram verificados pelo programa antivírus;
- ❒ procurar utilizar, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou PS;
- ❒ procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo ZIP ou GZ;
- ❒ procurar instalar um *firewall* pessoal, que em alguns casos pode bloquear o recebimento de um cavalo de tróia.

1.3 Vulnerabilidades

- ❒ manter o sistema operacional e demais *softwares* sempre atualizados;
- ❒ visitar regularmente os *sites* dos fabricantes de software para verificar a existência de vulnerabilidades nos *softwares* utilizados;
- ❒ aplicar todas as correções de segurança (*patches*) disponibilizadas pelo fabricante.

1.4 *Worms*

- ❒ instalar e manter atualizado um bom programa antivírus;
- ❒ manter o sistema operacional e demais *softwares* sempre atualizados;
- ❒ corrigir eventuais vulnerabilidades existentes nos *softwares* utilizados;
- ❒ procurar instalar um *firewall* pessoal, que em alguns casos pode evitar que uma vulnerabilidade existente seja explorada ou que o *worm* se propague.

1.5 *Backdoors*

- ❒ seguir as recomendações para prevenção contra infecções por vírus;
- ❒ não executar ou abrir arquivos recebidos por *e-mail*, mesmo que venham de pessoas conhecidas;
- ❒ não executar programas de procedência duvidosa ou desconhecida;

- ❒ procurar instalar um *firewall* pessoal, que em alguns casos pode evitar o acesso a um *backdoor* já instalado em seu computador;
- ❒ corrigir eventuais vulnerabilidades existentes nos *softwares* utilizados.

1.6 *Firewall*

- ❒ instalar um *firewall* pessoal em todos os computadores que tiverem acesso à Internet;
- ❒ verificar os registros de eventos (*logs*) para identificar possíveis ataques.

1.7 *E-mail*

- ❒ manter sempre a versão mais atualizada do seu programa de *e-mail*;
- ❒ desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- ❒ desligar as opções de execução do *JavaScript*, de programas *Java* e, se possível, o modo de visualização de *e-mails* no formato HTML.
- ❒ evitar abrir arquivos ou executar programas anexados aos *e-mails*, sem antes verificá-los com um antivírus;
- ❒ desconfiar de *e-mails* pedindo urgência na instalação de algum aplicativo ou correções de determinados defeitos dos *softwares* que você utilize.

1.8 *Browser*

- ❒ manter o seu *browser* sempre atualizado;
- ❒ desativar a execução de programas *Java* na configuração de seu *browser*, a menos que seja estritamente necessário;
- ❒ desativar a execução de *Javascripts* antes de entrar em uma página desconhecida e, então, ativá-la ao sair;
- ❒ permitir que programas *ActiveX* sejam executados em seu computador apenas quando vierem de *sites* conhecidos e confiáveis.
- ❒ manter maior controle sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet;
- ❒ certificar-se da procedência do *site* e da utilização de conexões seguras ao realizar transações via *Web*.

1.9 Programas de Troca de Mensagens

- ❒ manter seu programa de troca de mensagens sempre atualizado;
- ❒ não aceitar arquivos de pessoas desconhecidas, principalmente programas de computadores;
- ❒ evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- ❒ não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;
- ❒ configurar o programa para ocultar o seu endereço IP.

1.10 Programas de Distribuição de Arquivos

- ❒ manter seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- ❒ ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus ou cavalos de tróia;
- ❒ certificar-se que os arquivos obtidos ou distribuídos são **livres**, ou seja, não violam as leis de direitos autorais.

1.11 Compartilhamento de Recursos

- ❒ ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter vírus ou cavalos de tróia;
- ❒ estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador.

1.12 Cópias de Segurança

- ❒ procurar fazer cópias regulares dos dados do computador;
- ❒ criptografar dados sensíveis;
- ❒ armazenar as cópias em local acondicionado, de acesso restrito e com segurança física;
- ❒ considerar a necessidade de armazenar as cópias em um local diferente daquele onde está o computador.

2 Privacidade

2.1 Privacidade dos *e-mails*

- ❒ utilizar criptografia sempre que precisar enviar um *e-mail* com informações sensíveis;
- ❒ certificar-se que seu programa de *e-mail* grava as mensagens criptografadas, para garantir a segurança das mensagens armazenadas no disco.

2.2 *Cookies*

- ❒ desabilitar *cookies*, exceto para *sites* confiáveis e onde sejam realmente necessários;
- ❒ considerar o uso de *softwares* que permitem controlar o envio e recebimento de informações entre o *browser* e o *site* visitado.

2.3 Privacidade na Disponibilização de Páginas *Web*

- ❒ evitar colocar seus dados pessoais (*e-mail*, telefone, endereço, etc) em páginas *Web* ou *blogs*;
- ❒ evitar colocar dados sobre o seu computador ou sobre os *softwares* que utiliza em páginas *Web* ou *blogs*;
- ❒ evitar 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, etc) em páginas *Web* ou *blogs*.

2.4 Cuidados com seus Dados Pessoais

- ❒ procurar 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*.

2.5 Cuidados com os Dados Armazenados em um Disco Rígido

- ❒ criptografar todos os dados sensíveis, principalmente se for um *notebook*;
- ❒ sobrescrever os dados do disco rígido antes de vender ou se desfazer do seu computador usado.

3 Fraude

3.1 Engenharia social

- ❒ 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.

3.2 Cuidados ao realizar transações bancárias ou comerciais

- ❒ seguir todas as recomendações sobre utilização do *browser* de maneira segura;
- ❒ estar atento e prevenir-se dos ataques de engenharia social;
- ❒ 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;
- ❒ antes de aceitar um novo certificado, verificar junto à instituição que mantém o *site* sobre sua emissão e quais são os dados nele contidos;
- ❒ 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;
- ❒ verificar o certificado do *site*, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade;
- ❒ não acessar *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros;
- ❒ desligar sua *webcam* (caso vecê possua alguma), ao acessar um *site* de comércio eletrônico ou *Internet banking*.

3.3 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.

4 Banda Larga e Redes Sem Fio

4.1 Proteção de um computador utilizando banda larga

- ❒ instalar um *firewall* pessoal e ficar atento aos registros de eventos (*logs*) gerados por este programa;
- ❒ instalar um bom antivírus e atualizá-lo freqüentemente;
- ❒ manter o seu *software* (sistema operacional, programas que utiliza, etc) sempre atualizado e com as últimas correções aplicadas;
- ❒ desligar o compartilhamento de disco, impressora, etc;
- ❒ mudar a senha padrão do seu equipamento de banda larga (modem ADSL, por exemplo) pois as senhas destes equipamentos podem ser facilmente encontradas na Internet com uma simples busca. Esse fato é de conhecimento dos atacantes e bastante abusado.

4.2 Proteção de uma rede utilizando banda larga

- ❒ instalar um *firewall* separando a rede interna da Internet;
- ❒ caso seja instalado algum tipo de *proxy* (como AnalogX, wingate, WinProxy, etc) configurá-lo para que apenas aceite requisições partindo da rede interna;
- ❒ caso seja necessário compartilhar recursos como disco ou impressora entre máquinas da rede interna, devem-se tomar os devidos cuidados para que o *firewall* não permita que este compartilhamento seja visível pela Internet.

4.3 Cuidados com um cliente de rede sem fio (*wireless*)

- ❒ possuir um *firewall* pessoal;
- ❒ possuir um antivírus instalado e atualizado;
- ❒ aplicar as últimas correções em seus *softwares* (sistema operacional, programas que utiliza, etc);

- ❒ desligar compartilhamento de disco, impressora, etc;
- ❒ desabilitar o modo *ad-hoc*. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais;
- ❒ usar WEP (*Wired Equivalent Privacy*) sempre que possível;
- ❒ considerar o uso de criptografia nas aplicações, como por exemplo o uso de PGP para o envio de *e-mails*, SSH para conexões remotas ou ainda o uso de VPNs;
- ❒ habilitar a rede *wireless* somente quando for usá-la e desabilitá-la após o uso.

4.4 Cuidados com uma rede sem fio doméstica

- ❒ mudar configurações padrão que acompanham o seu AP;
- ❒ usar sempre que possível WEP (*Wired Equivalent Privacy*);
- ❒ trocar as chaves WEP que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- ❒ desligar seu AP quando não estiver usando sua rede.

5 SPAM

- ❒ considerar a utilização de um *software* de filtragem de *e-mails*;
- ❒ verificar com seu provedor ou com o administrador da rede se é utilizado algum *software* de filtragem no servidor de *e-mails*;
- ❒ evitar responder a um SPAM ou enviar um *e-mail* solicitando a remoção da lista.

6 Incidentes de Segurança e Uso Abusivo da Rede

6.1 Registros de eventos (*logs*)

- ❒ verificar sempre os *logs* do *firewall* pessoal e de IDSs que estejam instalados no computador;
- ❒ verificar se não é um falso positivo, antes de notificar um incidente.

6.2 Notificações de incidentes

- ❒ incluir *logs* completos (com data, horário, timezone, endereço IP de origem, portas envolvidas, protocolo utilizado, etc) e qualquer outra informação que tenha feito parte da identificação do incidente;
- ❒ enviar a notificação para os contatos da rede e para os grupos de segurança das redes envolvidas;
- ❒ manter nbso@nic.br na cópia das mensagens.