Cartilha de Segurança para Internet

FASCÍCULO

COMPUTADORES

cert.br nic.br cgi.br

MANTER SEU COMPUTADOR SEGURO É ESSENCIAL PARA SE PROTEGER DOS RISCOS ENVOLVIDOS NO USO DA INTERNET

Um grande risco que você pode correr ao usar a Internet é o de achar que não corre riscos, pois supõe que ninguém tem interesse em usar o seu computador ou que, entre os diversos computadores existentes, o seu dificilmente será localizado.

É justamente este tipo de pensamento que é explorado pelos atacantes, pois, ao se sentir seguro, você também pode achar que não precisa se prevenir. Esta falsa ilusão de segurança costuma terminar quando começam a acontecer os primeiros problemas.

Muitas vezes os atacantes estão interessados em conseguir acesso a grandes quantidades de computadores, independente de quais são e das configurações que possuem, e isso pode incluir o seu.

Por isto, acreditar que seu computador está protegido por não apresentar atrativos para um atacante pode ser um grande erro.

Seu computador pode ser invadido ou infectado, por exemplo, por meio:

- da ação direta de atacantes
- da exploração de contas de usuário sem senha ou com senha fraca
- da exploração de vulnerabilidades existentes nos programas instalados
- da auto-execução de mídias removíveis infectadas, como *pen drives*
- do acesso a páginas *web* maliciosas, utilizando navegadores vulneráveis
- da ação de códigos maliciosos, recebidos pela rede, obtidos em mensagens eletrônicas, via mídias removíveis, em páginas *web* ou de outros computadores.

PRESERVE A INTERNET: PROTEJA SEU COMPUTADOR

RISCOS PRINCIPAIS

Muito provavelmente é em seu computador que a maioria dos seus dados está gravada e, por meio dele, que você acessa *e-mails* e redes sociais e realiza transações bancárias e comerciais. Caso ele seja comprometido, você pode enfrentar problemas como:

- Invasão de privacidade
- Furto de identidade
- Vazamento de informações
- Perda de dados
- Perdas fincanceiras
- Ficar sem acesso ao computador

Além disso, seu computador ainda pode ser usado para atividades maliciosas, como:

- Infectar, invadir e atacar outros computadores
- Aplicar golpes em outros usuários
- Servir de repositório para dados fraudulentos
- Propagar códigos maliciosos
- Disseminar *spam*
- Esconder a real identidade e localização de um atacante

CUIDADOS A SEREM TOMADOS

MANTENHA OS PROGRAMAS ATUALIZADOS

» Tenha sempre as versões mais recentes dos programas instalados

» Remova as versões antigas e os programas que você não utiliza mais

INSTALE AS ATUALIZAÇÕES DISPONÍVEIS

» Configure os programas para serem atualizados automaticamente

» Programe as atualizações automáticas para serem baixadas e aplicadas em um horário em que o computador esteja ligado e conectado à Internet

» Cheque periodicamente por novas atualizações, usando as opções disponíveis nos programas

USE APENAS PROGRAMAS ORIGINAIS

» Ao comprar um computador pré-instalado, certifique-se de que os programas são originais solicitando ao revendedor as licenças de uso

» Caso deseje usar um programa proprietário, mas não possa adquirir a licença, procure por alternativas gratuitas ou mais baratas, e que possuam funcionalidades semelhantes às desejadas

AO INSTALAR APLICATIVOS DESENVOLVIDOS POR TERCEIROS

» Verifique se as permissões de instalação e execução são coerentes

» Seja cuidadoso ao:
- permitir que os aplicativos acessem seus dados pessoais
- selecionar os aplicativos, escolhendo aqueles bem avaliados e com grande quantidade de usuários

USE MECANISMOS DE PROTEÇÃO

» Instale um antivírus (*antimalware*)
- mantenha-o atualizado, incluindo o arquivo de assinaturas
- configure-o para verificar todos os formatos de arquivos
- sempre verifique os arquivos recebidos antes de abri-los ou executá-los

» Assegure-se de ter um *firewall* pessoal instalado e ativo

» Crie um disco de emergência de seu antivírus e use-o se desconfiar que:
- o antivírus instalado está desabilitado/comprometido, ou
- o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc.)

» Crie um disco de recuperação do seu sistema e certifique-se de tê-lo por perto no caso de emergências

» Seja cuidadoso ao clicar em *links*, independente de como foram recebidos e de quem os enviou
- antes de clicar em um *link* curto procure usar complementos que possibilitem que o *link* de destino seja visualizado
- não considere que mensagens vindas de conhecidos são sempre confiáveis
  - o campo de remetente pode ter sido falsificado, ou
  - elas podem ter sido enviadas de contas falsas ou invadidas

» Desabilite a auto-execução de mídias removíveis e de arquivos anexados

PROTEJA SUAS CONTAS DE ACESSO E SENHAS

» Crie uma conta padrão e use-a nas tarefas rotineiras
  - use a conta de administrador somente quando necessário e pelo menor tempo possível
  - use a opção de “executar como administrador” quando necessitar de privilégios administrativos

» Mantenha a conta de convidado desabilitada

» Assegure-se de que:
  - todas as contas de acesso existentes tenham senha
  - não existam contas de uso compartilhado
  - a conta de acesso e a senha sejam solicitadas na tela inicial
  - a opção de *login* automático esteja desabilitada

» Seja cuidadoso ao elaborar suas senhas
  - use senhas longas, compostas de diferentes tipos de caracteres
  - não utilize:
    - sequências de teclado
    - dados pessoais, como nome, sobrenome e datas
    - dados que possam ser facilmente obtidos sobre você

AO USAR O SEU COMPUTADOR EM LOCAIS PÚBLICOS

» Utilize travas que dificultem que ele seja aberto ou furtado

» Mantenha-o bloqueado, para evitar que seja indevidamente usado quando você não estiver por perto

» Utilize criptografia de disco
  - em caso de perda ou furto isso dificultará o acesso aos seus dados

» Configure-o para solicitar senha na tela inicial
  - isso dificulta que alguém reinicie seu computador e o acesse diretamente

SEJA CUIDADOSO AO USAR COMPUTADORES DE TERCEIROS

- Utilize opções de navegar anonimamente
- Não efetue transações bancárias ou comerciais
- Não utilize opções como “Lembre-se de mim” e “Continuar conectado”
- Não permita que suas senhas sejam memorizadas pelo navegador *web*
- Limpe os dados pessoais salvos pelo navegador
- Assegure-se de sair (*logout*) de suas contas de usuário
- Seja cuidadoso ao conectar mídias removíveis, como *pen drives*
- Ao retornar ao seu computador:
  - altere as senhas usadas
  - verifique seu *pen drive* com um antivírus

OUTROS CUIDADOS

- Faça regularmente *backup* dos seus dados
- Mantenha a data e a hora corretas
  - veja como manter seu computador sincronizado em **www.ntp.br**
- Verifique as configurações de segurança oferecidas pelos programas instalados em seu computador e adapte-as as suas necessidades
- Ao compartilhar recursos do seu computador:
  - estabeleça senhas e permissões de acesso adequadas
  - compartilhe seus recursos pelo tempo mínimo necessário
- Ao enviar seu computador para serviços de manutenção:
  - selecione empresas com boas referências
  - não permita a instalação de programas não originais
  - se possível faça *backup* dos seus dados antes de enviá-lo

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

cartilha.cert.br/cc

outubro / 2020