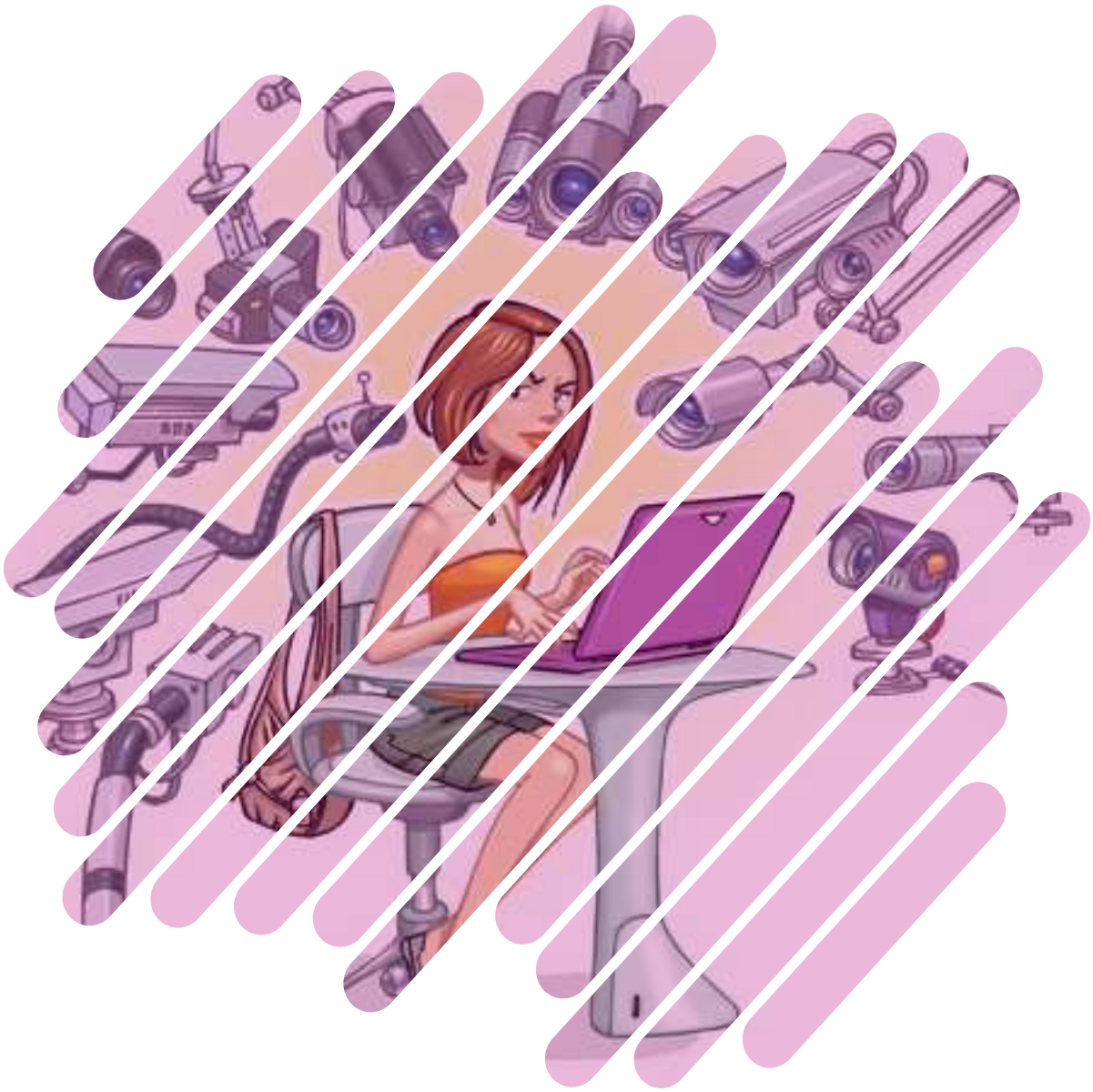
Cartilha de Segurança para Internet

FASCÍCULO

PRIVACIDADE



Apoio de Divulgação:

UFPE

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

QUANTO MAIS INFORMAÇÕES VOCÊ DISPONIBILIZA NA INTERNET, MAIS DIFÍCIL SE TORNA PRESERVAR A SUA PRIVACIDADE

Nada impede que você abra mão de sua privacidade e, de livre e espontânea vontade, divulgue suas informações. Entretanto, a sua privacidade pode ser exposta independentemente da sua vontade, por exemplo quando:

- alguém divulga informações sobre você ou imagens onde você está presente, sem a sua autorização prévia
- um *site* que você utiliza altera as políticas de privacidade, sem aviso prévio, expondo informações anteriormente restritas
- um impostor se faz passar por você, cria um *e-mail* ou perfil falso em seu nome e o utiliza para coletar informações pessoais sobre você
- um atacante invade a sua conta de *e-mail* ou de sua rede social e acessa informações restritas
- alguém coleta informações que trafegam na rede sem estarem criptografadas, como o conteúdo dos *e-mails* enviados e recebidos por você
- um atacante ou um código malicioso obtém acesso aos dados que você digita ou que estão armazenados em seu computador
- um atacante invade um computador no qual seus dados estão armazenados, como, por exemplo, um servidor de *e-mails*
- seus hábitos e suas preferências de navegação são coletadas pelos *sites* que você acessa e repassadas para terceiros
- um aplicativo instalado em seu computador ou em seu dispositivo móvel coleta seus dados pessoais e os envia ao desenvolvedor/fabricante
- recursos do seu computador, como diretórios, são compartilhados sem as configurações de acesso adequadas.

PRIVACIDADE: PRESERVE A SUA

RISCOS PRINCIPAIS

Preservar a sua privacidade pode ajudá-lo a se proteger dos golpes e ataques aplicados na Internet. A divulgação e a coleta indevida de informações pessoais pode:

- Comprometer a sua privacidade, de seus amigos e familiares
  - mesmo que você restrinja o acesso a uma informação, não há como controlar que ela não será repassada
- Facilitar o furto da sua identidade
  - quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista criar uma identidade falsa em seu nome, pois mais convincente ele poderá ser
  - a identidade falsa criada pelo golpista pode ser usada para atividades maliciosas, como efetuar transações financeiras, acessar *sites*, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas
- Facilitar a invasão de suas contas de usuário (por exemplo, de *e-mail* ou de rede social)
  - caso você use dados pessoais para elaborar suas senhas ou como resposta de dicas/questões de segurança, elas podem ser facilmente adivinhadas
- Fazer com que propagandas direcionadas sejam apresentadas
- Causar perdas financeiras, perda de reputação e falta de crédito
- Colocar em risco a sua segurança física
- Favorecer o recebimento de *spam*

CUIDADOS A SEREM TOMADOS

AO ACESSAR E ARMAZENAR SEUS *E-MAILS*

» Configure seu programa leitor de *e-mails* para não abrir imagens que não estejam na própria mensagem
  - o fato da imagem ser acessada pode ser usado para confirmar que o *e-mail* foi lido

» Use programas leitores de *e-mails* que permitam que as mensagens sejam criptografadas
  - mensagens criptografadas somente poderão ser lidas por quem conseguir decodificá-las

» Armazene *e-mails* confidenciais em formato criptografado
  - isso pode evitar que sejam lidos por atacantes ou pela ação de códigos maliciosos
  - você pode decodificá-los sempre que desejar lê-los

» Use conexão segura quando acessar *e-mails* por meio de navegadores *web*
  - mesmo que você restrinja o acesso a uma informação, não há como controlar que ela não será repassada

» Use criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor

» Seja cuidadoso ao acessar seu *webmail*
  - digite a URL diretamente no navegador
  - tenha cuidado ao clicar em *links* recebidos por meio de mensagens eletrônicas

AO MANIPULAR SEUS DADOS

» Mantenha seus *backups* em locais seguros e com acesso restrito

» Armazene dados sensíveis em formato criptografado

» Cifre o disco do seu computador e dispositivos removíveis, como disco externo e *pendrive*

» Ao usar serviços de *backup online*, leve em consideração a política de privacidade e de segurança do *site*

AO NAVEGAR NA WEB

» Seja cuidadoso ao usar *cookies*, por meio de uma ou mais das seguintes opções:

- defina um nível de permissão superior ou igual a "médio"
- configure para que os *cookies* sejam apagados assim que o navegador for fechado
- configure para que *cookies* de terceiros não sejam aceitos
  - isso não deverá prejudicar a sua navegação, pois serão bloqueados apenas conteúdos relacionados a publicidade
- você pode também configurar para que, por padrão:
  - os *sites* não possam definir *cookies* e criar listas de exceções, cadastrando *sites* considerados confiáveis e onde o uso é realmente necessário, ou
  - os *sites* possam definir *cookies* e criar listas de exceções, cadastrando os *sites* que deseja bloquear

» Quando disponível, procure utilizar:

- navegação anônima, principalmente ao usar computadores de terceiros
  - dessa forma, informações sobre a sua navegação, como *sites* acessados, dados de formulários e *cookies*, não serão armazenadas

AO COMPARTILHAR RECURSOS DO SEU COMPUTADOR

» Estabeleça senhas para os compartilhamentos e permissões de acesso adequadas

» Compartilhe seus recursos pelo tempo mínimo necessário

AO DIVULGAR INFORMAÇÕES NA WEB (REDES SOCIAIS)

» Esteja atento e avalie com cuidado as informações divulgadas em sua página *web*, rede social ou *blog*
  - elas podem ser usadas em golpes de engenharia social, para obter informações sobre você, para atentar contra a segurança do seu computador ou contra a sua segurança física
  - considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa

» Pense bem antes de divulgar algo, pois não é possível voltar atrás

» Divulgue a menor quantidade possível de informações, tanto sobre você como sobre seus amigos e familiares
  - oriente-os a fazer o mesmo

» Sempre que alguém solicitar dados sobre você ou quando preencher algum cadastro, reflita se é realmente necessário que aquela empresa ou pessoa tenha acesso àquelas informações

» Ao receber ofertas de emprego pela Internet que solicitem o seu currículo, tente limitar a quantidade de informações nele disponibilizada
  - apenas forneça mais dados quando estiver seguro de que tanto a empresa como a oferta são legítimas

» Fique atento a ligações telefônicas e *e-mails* pelos quais alguém, geralmente falando em nome de alguma instituição, solicita informações pessoais sobre você, inclusive senhas

» Seja cuidadoso ao divulgar a sua localização geográfica
  - com base nela, é possível descobrir a sua rotina, deduzir informações (como hábitos e classe financeira) e tentar prever seus próximos passos ou de seus familiares

» Verifique a política de privacidade dos *sites* que você utiliza e fique atento às mudanças, principalmente aquelas relacionadas ao tratamento de dados pessoais, para não ser surpreendido com alterações que possam comprometer a sua privacidade

» Use as opções de privacidade oferecidas pelos *sites* e seja o mais restritivo possível

» Mantenha seu perfil e seus dados privados

» Seja seletivo ao aceitar seus contatos e ao se associar a grupos e comunidades

PROTEJA SUAS CONTAS E SENHAS

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

» Evite reutilizar suas senhas, não use a mesma senha para acessar diferentes *sites*

» Não forneça suas senhas para outra pessoa, em hipótese alguma

» Ao usar perguntas de segurança para facilitar a recuperação de senhas, evite escolher questões cujas respostas possam ser facilmente adivinhadas

PROTEJA SEU COMPUTADOR E SEUS DISPOSITIVOS MÓVEIS

» Mantenha o seu computador/dispositivo móvel seguro
  - com a versão mais recente de todos os programas instalados
  - com todas as atualizações aplicadas

» Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, *antimalware* e *firewall* pessoal

» Ao instalar aplicativos desenvolvidos por terceiros:
  - seja cuidadoso ao permitir que os aplicativos acessem seus dados pessoais, como listas de contatos e localização geográfica
  - verifique se as permissões necessárias para a instalação e execução são coerentes, ou seja, um programa de jogos não necessariamente precisa ter acesso à sua lista de chamadas
  - seja seletivo ao selecionar os aplicativos, escolhendo aqueles bem avaliados e com grande quantidade de usuários

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