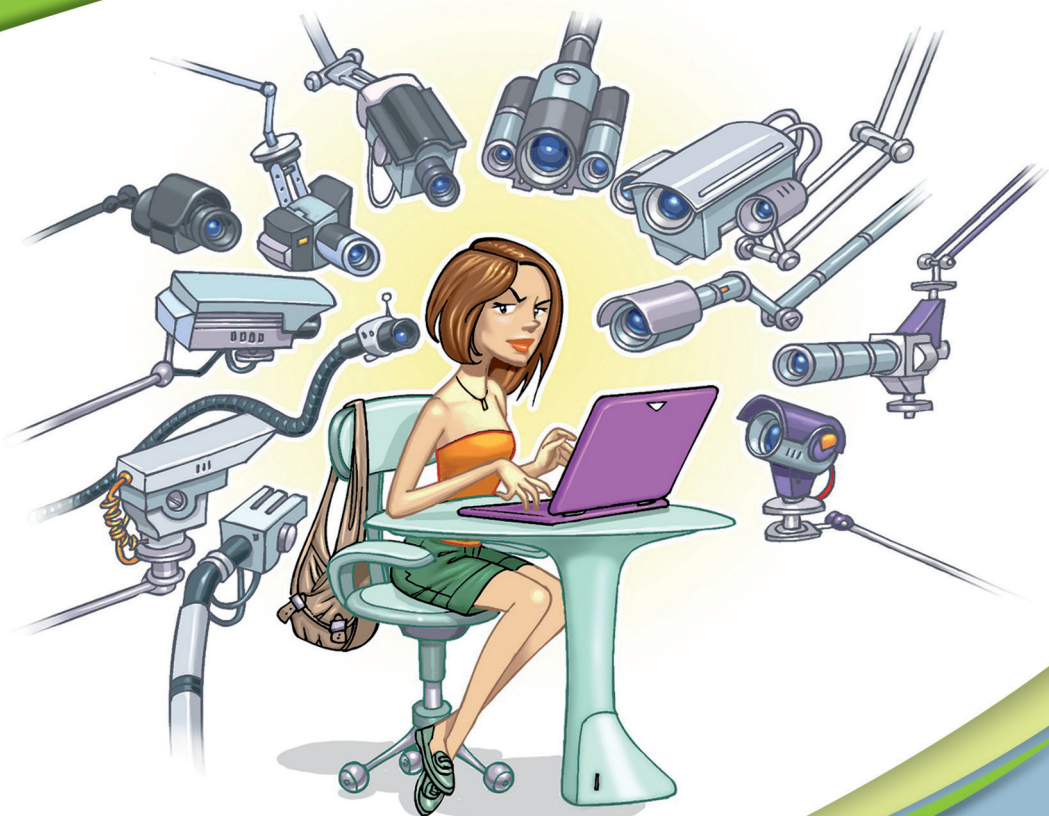


Cartilha de Segurança para Internet

Publicação
cert.br

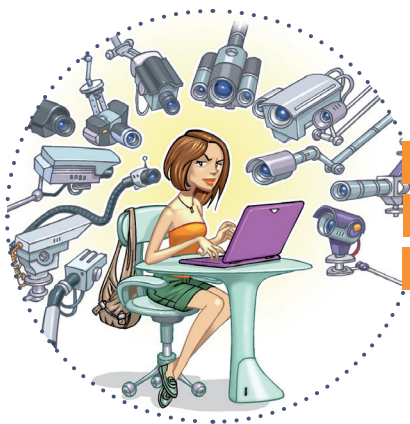
Fascículo Privacidade



<https://cartilha.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

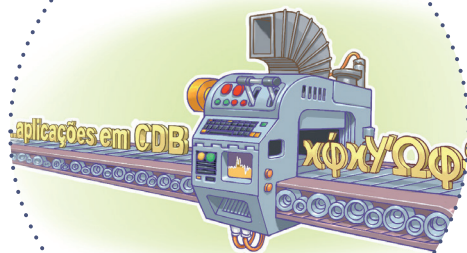


Riscos principais

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 *pen-drive*
- ✓ ao usar serviços de *backup online*, leve em consideração a política de privacidade e de segurança do *site*.



Ao navegar na Web:

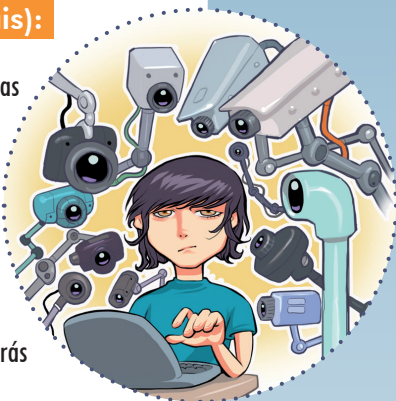
- ✓ seja cuidadoso ao usar *cookies*, por meio de uma ou mais das seguintes opções:
 - defina um nível de permissão superior ou igual a “médio”
 - configure para que os *cookies* sejam apagados assim que o navegador for fechado
 - configure para que *cookies* de terceiros não sejam aceitos
 - isso não 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.

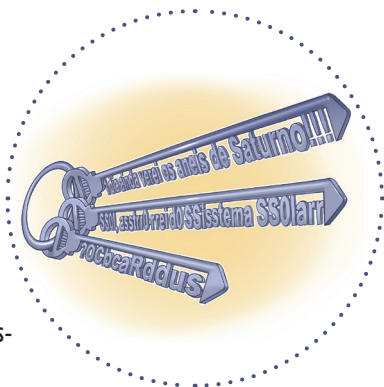
Ao divulgar informações na Web (redes sociais):

- ✓ 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*, *anti-malware* 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.





Consulte a **Cartilha de Segurança** para mais detalhes sobre os cuidados a serem tomados para proteger a sua privacidade:

<https://cartilha.cert.br/privacidade/>



INTERNET
SEGURA.BR

Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!

<http://internetsegura.br/>

cert.br

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

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 <https://www.cert.br/>.

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (<http://www.nic.br/>) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (<http://www.registro.br/>), estudar e tratar incidentes de segurança no Brasil - CERT.br (<https://www.cert.br/>), estudar e pesquisar tecnologias de redes e operações - CEPTRO.br (<http://www.ceptro.br/>), produzir indicadores sobre as tecnologias da informação e da comunicação - CETIC.br (<http://www.cetic.br/>) e abrigar o escritório do W3C no Brasil (<http://www.w3c.br/>).

cgi.br

Comitê Gestor da
Internet no Brasil

O Comitê Gestor 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 de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (<http://www.cgi.br/principios>). Mais informações em <http://www.cgi.br/>.