cartilha de **privacidade** de **dados**

RNP CAIS

sumário

Não há como falar sobre segurança da informação sem citarmos um dos temas mais preocupantes do momento: nossa privacidade. Nesta cartilha, você poderá saber um pouco mais sobre o cenário de privacidade no Brasil, além de conferir algumas dicas para preservar sua imagem e a de sua família na rede.

introdução

por que se preocupar com privacidade?

Novas tecnologias vêm trazendo avanços sem precedentes na vida das pessoas em termos de liberdade e acesso a informações. Entretanto, essas mesmas tecnologias permitem que indivíduos e organizações invadam a privacidade de uma maneira preocupante.

Suas buscas na Web sobre informações médicas, políticas ou qualquer outro assunto particular podem parecer um segredo entre você e seu site de buscas e computador, mas estão criando gradualmente uma enorme base de dados sobre você e seus hábitos.

Seu *smartphone* revolucionou seu contato com amigos, mas ele também passou a armazenar uma quantidade impressionante de dados pessoais como fotos, contatos, pessoas com quem

leis brasileiras e privacidade

A Constituição Federal estabelece a privacidade como direito básico da pessoa no artigo 5o., inciso X:

"Art. 5o – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X- são invioláveis a intimidade, a vida privada, a honra e imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

você se comunica e seus dados, mensagens (*e-mail*, SMS, *instant messaging*), sua localização (a partir das antenas de celular, GPS embutido ou aplicações de "*check in*" como FourSquare ou *check-in* do Facebook). O acesso não autorizado a essa riqueza de informações pessoais por pessoas ou organizações não é apenas indesejado como também um risco à sua privacidade e, consequentemente, intimidade.

A privacidade tem sido cada vez mais atacada e é fato que tolerar um certo nível de sua invasão, principalmente por empresas de serviços de Internet, infelizmente se tornou necessário para a vida em sociedade. Essa cartilha tem o objetivo de orientar o usuário sobre aspectos da privacidade que estão ao seu alcance na forma de práticas que favoreçam a privacidade.

Entretanto, com os avanços nas telecomunicações (Internet, telefonia celular) e dispositivos de processamento e armazenamento de dados (computadores, *smartphones*, *tablets*), ficou muito mais difícil saber quando exatamente esses direitos foram violados.

Atualmente o principal avanço na direção de um tratamento mais apropriado da proteção da privacidade e dos dados pessoais dos brasileiros na Internet é o chamado ***Marco Civil da Internet***. O ***Marco Civil*** está em debate desde 2009 e tramita na Câmara dos Deputados como projeto de lei (PL 2126/2011) desde 2011.

Outra lei que trata indiretamente da privacidade é a chamada "***Lei Carolina Dieckmann***" (12.737/2012), que pune o acesso não autorizado a dados pessoais.

Falar sobre a privacidade na Internet não é diferente de falar sobre o conceito geral de privacidade. Acreditamos que essa seja uma das principais mensagens desta cartilha.

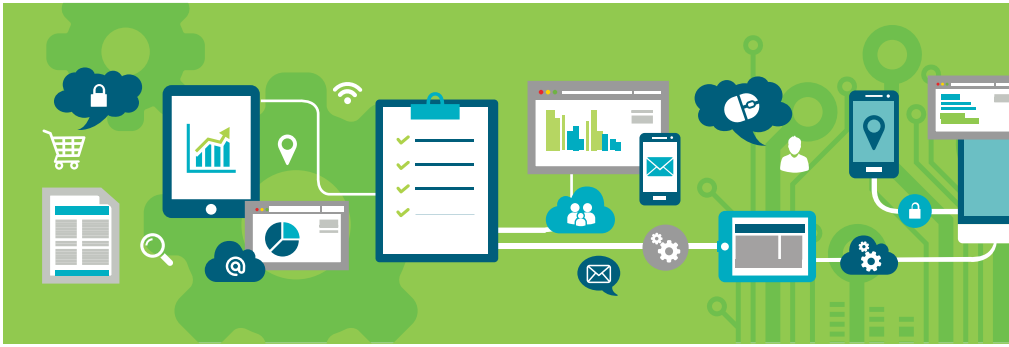
recomendações **gerais**

privacidade

O Brasil é um país em que as pessoas não estão acostumadas a cuidar de sua privacidade. Frequentemente somos obrigados a preencher longos formulários para uma simples compra em dinheiro ou cartão de crédito, sob o pretexto de relacionamento com o cliente.

A seguir daremos dicas de como proteger sua privacidade em pequenos atos no dia a dia.

Respeite a privacidade das outras pessoas da mesma forma que você quer que a sua seja respeitada. Isso é mais aplicável no ambiente de redes sociais (fotos alheias, etiquetas em fotos, divulgações de informações alheias sem autorização prévia), mas pode ser aplicado a outros contextos, como por exemplo, enviar um *e-mail* para dezenas de pessoas com os endereços delas no campo TO/Para.



Formulários são uma das formas mais claras de obtenção de dados pessoais. Eles estão presentes tanto na Internet (cadastros, perfis em redes sociais) quanto fora dela, em papel. Nossa recomendação é que você sempre preencha o mínimo de dados possível (somente os obrigatórios) e questione, ou mesmo não preencha, formulários que exijam dados demais. Outra recomendação é utilizar um endereço de *e-mail* alternativo para cadastros menos importantes, como uma compra isolada ou formulários em papel. O endereço de *e-mail* ainda é um dos principais identificadores únicos de uma pessoa e pode ser usado no cruzamento com outros bancos de dados.

Evite fornecer seu celular pessoal em formulários. Está cada vez mais comum a prática de *spam* por meio de SMS, no qual as empresas enviam mensagens de texto mesmo sem autorização prévia. A maioria das pessoas não tem filtros de *spam* por SMS. Além disso, o celular é, assim como o *e-mail*, um dos principais identificadores únicos de uma pessoa na Internet.

***Cookies* do navegador são arquivos que armazenam alguns dados sobre a última sessão de visita a um determinado *website*.** Esses arquivos são lidos pelo *website* quando você volta a visitá-lo com o mesmo navegador. O risco desses arquivos está nos dados armazenados, que vão desde a data de sua última visita até dados sobre seu computador. Recomendamos que você limpe completamente o histórico de seu navegador periodicamente e que inclua apagar *cookies* nessa limpeza.

Atualmente, os principais navegadores possuem o recurso de navegação privativa. A vantagem desse modo de navegação é que histórico de navegação, *cookies* e outros rastros de navegação são automaticamente apagados ou omitidos, dificultando assim a identificação de uma nova visita sua. No Mozilla Firefox esse recurso se chama "***Navegação Privada***" e está disponível na opção ***Ferramentas › Iniciar Navegação Privada***. No Google Chrome, essa opção está disponível em ***Arquivo › Nova Janela Anônima*** (***Incognito*** na versão em inglês) ou através das teclas ***CTRL+N***.

Você já deve ter lido ou escutado alguém comentando que uma vez que uma informação esteja na Internet é difícil retirá-la. Considere isso verdade na maioria dos cenários, particularmente com fotos e vídeos íntimos e redes sociais mais abertas como Twitter e Facebook. Pense muito bem antes de divulgar informações e, se realmente quiser usar seu celular para registrar imagens comprometedoras, faça *backup* e remova-as do dispositivo móvel o mais cedo possível.

privacidade em seu **computador**

A dica pode parecer repetitiva, mas não custa lembrar: mantenha seu computador totalmente atualizado (sistema operacional, aplicativos, *plug-ins* de navegador e especialmente seu navegador de acesso à Internet) e tenha um antivírus. Essa simples medida previne algumas formas de vazamento de dados pessoais, como *phishing* (páginas falsas) e programas maliciosos (como os RAT – programas que permitem controle completo por um terceiro).

Defina uma senha para seu computador e, se possível, tenha usuários diferentes para pessoas diferentes que usam o mesmo computador.

Habilite criptografia total do disco rígido (*full disk encryption*), se disponível. Os principais sistemas operacionais possuem esse recurso em suas versões mais recentes. Essa prática é importante especialmente no caso de perda e roubo. No Windows Vista, Windows 7 e Windows 8 essa opção se chama ***BitLocker***. No Mac OS X essa opção se chama ***FileVault***. Em ambos os sistemas a ativação do recurso é muito simples. Guarde com cuidado a senha de emergência, preferencialmente impressa em papel.

Comunicação segura: Há poucas maneiras de se comunicar de maneira segura. A melhor delas é PGP (*Pretty Good Privacy*) que, embora não seja de utilização muito simples, é muito usada para cifrar mensagens de *e-mail* e arquivos de forma que somente os destinatários especificados possam ter acesso ao conteúdo. Há opções pagas e gratuitas, que implementam o padrão OpenPGP. A maneira mais simples de começar a usar PGP é usar o cliente de *e-mail* Thunderbird em conjunto com a extensão ***Enigmail***. Mais informações em *http://www.enigmail.net*, *http://www.gpg4win.org*, *https://gpgtools.org*

Na prática, PGP funciona da seguinte forma: você começa criando uma chave privada (que você nunca deve compartilhar) e uma pública. Ao se comunicar com alguém com PGP você deve primeiro fornecer sua chave pública ao destinatário. Você pode assinar a mensagem (permitir que o destinatário tenha certeza de que a mensagem foi criada por você), cifrar (somente remetente e destinatários podem ler) ou ambos. PGP também pode ser usado para cifrar arquivos isoladamente. Recomendamos que você use mensagens em formato somente texto, sem qualquer tipo de formatação.

Outras maneiras de comunicação segura: Uma das opções de chat seguro é OTR (*Off-the-Record Messaging*), um "*plugin*" para certos programas de mensagem instantânea que permite que você use Google Talk e Chat Facebook com criptografia. Outra opção é ***Cryptocat***, um *chat* temporário anônimo seguro por meio de navegador. Mais informações em *http://www.cypherpunks.ca/otr/software.php* e *https://crypto.cat*

Navegue sempre que possível usando TLS / SSL, um mecanismo de segurança que protege com criptografia os dados transmitidos entre seu computador e um servidor Web. Você já sabe, mas é bom lembrar: a presença de cadeado ou endereço não indicam que um *website* é seguro, mas sim que o protocolo de comunicação SSL (*Secure*

Socket Layer) está em uso. SSL por si só não é garantia de estar livre de golpes de *Phishing*. Para forçar o uso de SSL sugerimos a instalação da extensão ***HTTPS Everywhere***, disponível em *https://www.eff.org/https-everywhere*.

- Caso deseje visitar um *website* com anonimato recomendamos o uso da rede ***Tor***, que basicamente oculta a real origem (endereço IP) de seu computador no contexto da navegação Web. Para o uso mais simples de Tor use o ***Tor Browser Bundle***, um pacote que inclui um navegador novo pronto para Tor. É bom lembrar que Tor provê anonimato, não privacidade. O tráfego de sua navegação web pode ser capturado por terceiros em certos cenários. Mais informações em *https://www.torproject.org*.

- Tente sempre usar serviços que ofereçam a opção de autenticação por dois fatores – uma senha que você escolhe e outra temporária enviada por SMS ou *app* ***Google Authenticator***. O mecanismo é muito semelhante ao que muitos bancos adotam. Dessa forma o acesso não autorizado a sua senha não será suficiente para ter acesso a sua conta. Atualmente vários serviços possuem esse recurso: Google, Facebook, Dropbox, Apple ID e, mais recentemente, Microsoft. Na maioria desses serviços a melhor opção é usar SMS como meio de envio. Portanto, você deve fornecer seu número de celular.

privacidade em **redes sociais**

As redes sociais são provavelmente o ambiente no qual mais dados pessoais vazam para contatos indesejados ou mesmo para a Internet. A seguir daremos algumas dicas básicas sobre como proteger sua privacidade em redes sociais.

- **Logout:** Pode parecer uma dica sem importância, mas lembre-se de sair da rede social (*Logout*) sempre que não estiver mais usando. Isso impede que outros usuários da máquina tenham acesso a sua conta de *webmail* e redes sociais.

- **Senha:** Escolha uma senha forte e troque-a periodicamente. Certas redes sociais são tão importantes quanto seu *e-mail*, por isso você deve ter os mesmos cuidados.

- Adquira o hábito de revisar periodicamente as configurações de segurança e privacidade de seu perfil. As configurações mudam frequentemente.

- **Atualizações em redes sociais:** Esse é provavelmente o ato voluntário mais significativo que permite a invasão da privacidade. Atualizações no Twitter, Facebook, Instagram, LinkedIn e outras redes sociais devem ser feitas com cuidado. Recomendamos não revelar rotinas pessoais, local em que está (por texto), dados de amigos e parentes. Recomendamos também que a localização geográfica seja desabilitada em *smartphones* e navegadores do computador.

- **Perfis em redes sociais:** A dica é semelhante à dica relacionada com formulários de maneira geral: preencha somente os dados obrigatórios. Evite preencher local de residência exato, escolas em que estudou, onde trabalha, relacionar membros da família, telefone ou mesmo preencher o nome completo.

- **Limite seus amigos nas redes sociais:** Seja bem mais seletivo ao autorizar amigos em suas redes sociais, autorizando, por exemplo, somente amigos próximos e família. Dessa forma, a distribuição de seu conteúdo (atualizações e fotos) será mais controlada, mesmo que você não seja muito cuidadoso nas configurações da rede social.

Desabilite a localização geográfica: Assim, suas atualizações e fotos não serão associadas a um ponto geográfico, o que pode revelar onde exatamente você está. Essa dica é mais aplicável a FourSquare, Facebook e Twitter.

Instale a extensão de navegador *Disconnect*: Ao visitar outros *sites* que tem botões ou outros elementos de *sites* e redes sociais (Facebook, Google, LinkedIn, Twitter, Yahoo) sua atividade é monitorada. Esse monitoramento permite que uma rede social saiba, por exemplo, que você esteve visitando um determinado *website* e passará a oferecer anúncios publicitários sobre aquele produto ou serviço. A extensão ***Disconnect*** bloqueia essa atividade. Mais informações em *https://disconnect.me*.

Crianças e redes sociais: Sabemos que é irresistível não compartilhar todos os passos de seu filho em redes sociais, bem como fotos e outras informações. Se você deseja realmente fazer isso recomendamos que tenha um conjunto bem limitado de amigos. Além disso, lembre-se sempre de que seu filho é uma pessoa que também tem direito à privacidade.

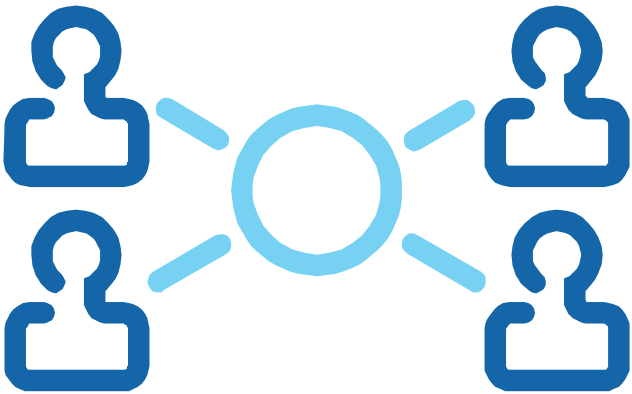
Se você não gosta da opção de ter poucos amigos em redes sociais então o recurso de listas do Facebook é uma maneira muito boa de controlar melhor o acesso a seus dados pessoais e mídia (fotos, vídeos). Crie, por exemplo, três listas: ***Família***, ***Amigos*** e ***Trabalho***, e filtre seus compartilhamentos através deste recurso.

Importante lembrar: mesmo adotando todas as melhores práticas de privacidade em redes sociais ainda assim há o

armazenamento de toda a sua atividade pela própria rede social e a possibilidade de vazamento de algum dado, especialmente atualizações e mídia (fotos, vídeos). Pare e reflita muito bem antes de compartilhar qualquer conteúdo.

Cuide de sua imagem profissional: Sugerimos mais uma vez que você limite a quantidade de amigos que tem em sua rede social pessoal, que normalmente é Facebook. Sugerimos que você use Facebook somente para assuntos pessoais, adicionando colegas de trabalho somente no caso dos mesmos serem também amigos próximos. Para uso profissional sugerimos outra rede social mais apropriada: LinkedIn.

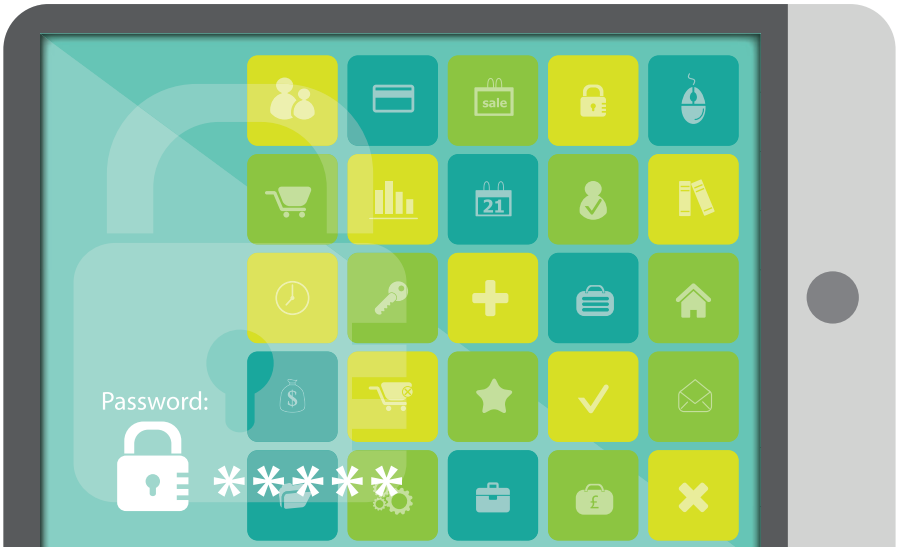
Avalie como deseja usar o Twitter: pessoal, profissional ou ambos. Diferente das demais redes sociais abordadas, é mais difícil controlar o destino do conteúdo compartilhado porque a rede foi concebida para ser simples. Se você pretende compartilhar conteúdo particular ou simplesmente deseja controlar melhor quem lê seus *tweets* sugerimos que ative a opção "***Proteger meus tweets***" (em ***Configurações***).



privacidade em *smartphones* e *tablets*

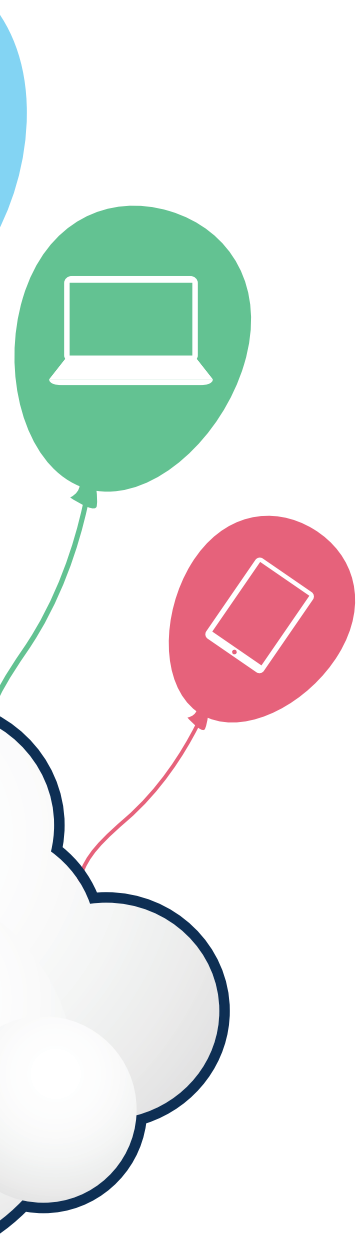
- Defina uma senha relativamente complexa de bloqueio do dispositivo. Se possível, defina o bloqueio automático em caso de inatividade depois de, no máximo, 3 minutos.

- Altere o PIN (senha) padrão de seu *chip* (também chamado de SIM) – cada operadora tem o seu. Esta senha, de quatro algarismos, normalmente é informada no cartão plástico no qual o *chip* é vendido. Depois, configure o chip de forma que ao ligar o aparelho o PIN seja solicitado antes de liberar o chip para uso. No iPhone, por exemplo, essa opção está em ***Ajustes › Telefone › SIM PIN › Alterar PIN***. Para forçar o uso do PIN sempre que o aparelho for desligado escolha a opção "PIN do SIM". Dessa forma no caso de um dispositivo roubado você não terá problemas de ligações feitas ou recebidas sem autorização.



- Faça *backup* (cópia de segurança) das fotos que estão em seu celular regularmente. Se possível, remova as fotos ao realizar o *backup*. Suas fotos, mesmo que não sejam íntimas ou comprometedoras, são particulares e podem cair em mãos erradas, facilitando vários cenários – roubo, acesso não autorizado, perda, sequestro.

- O uso de armazenamento de arquivos em



nuvem (Dropbox, iCloud, Google Drive, Microsoft OneDrive) é uma boa forma de *backup* automático de arquivos. Atualmente, consideramos Dropbox a melhor opção por oferecer suporte a vários dispositivos e um nível de segurança muito bom, que inclui autenticação por dois fatores (uma senha tradicional e uma senha temporária enviada por *e-mail* ou *app* Google Authenticator). Outro aspecto positivo de não concentrar serviços demais em uma mesma conta, o que é aplicável a Google Drive, iCloud e Microsoft OneDrive. Em casos de acesso indevido o atacante terá acesso a toda sua "vida digital".

- Desative o recurso de localização geográfica (GPS), particularmente em Redes Sociais, Fotos e *Apps* (aplicativos) que não tenham razão clara para esse acesso.

Confira as iniciativas e projetos de segurança da informação promovidos pela RNP em:
http://www.rnp.br/servicos/seguranca