HÁBITOS SAUDÁVEIS

Para mudar um comportamento vulnerável é importante mesclar soluções técnicas com uma postura preventiva. Confira as dicas do Cert.br:

- Manter o computador e os dispositivos móveis com a versão mais recente de todos os programas instalados e com atualizações aplicadas;
- Utilizar e manter atualizados mecanismos de segurança, como *antispam, antimalware* e *firewall*;
- Verificar a procedência de aplicativos de terceiros;
- Usar senhas longas, compostas de diferentes tipos de caracteres;
- Não utilizar dados pessoais, como nome, sobrenome e datas nas senhas, nem dados que possam ser facilmente obtidos;
- Avaliar com cuidado as informações divulgadas em páginas *web*, redes sociais ou *blogs*, pois não é possível voltar atrás;
- Divulgar a menor quantidade possível de informações;
- Verificar a política de privacidade dos *sites* utilizados e ficar atento às mudanças, principalmente aquelas relacionadas ao tratamento de dados pessoais, para não ser surpreendido com alterações que possam comprometer a privacidade;
- Usar as opções de privacidade oferecidas pelos *sites* e ser o mais restritivo possível;
- Manter o perfil e os dados privados;
- Ser seletivo ao aceitar contatos e ao se associar a grupos e comunidades.

NAVEGAÇÃO SEGURA

Os navegadores de internet têm recursos de privacidade em diversos níveis. Saiba como usar.

Chrome
www.google.com/chrome
Ao acionar CTRL+SHIFT+N o usuário entra em modo anônimo – as páginas visitadas não são armazenadas no histórico e os *cookies* são apagados assim que a aba é fechada. Outra possibilidade é configurar os níveis de privacidade. Clique em *Configurações*, depois em *Mostrar Configurações Avançadas*, e mais uma vez e *Configurações de Conteúdo*. Ali é possível permitir ou bloquear *Cookies, plugins, pop-ups*e aplicativos que rodam em JavaScript.

Firefox
www.mozilla.org/pt-BR/firefox
Clique em *Editar*, depois em *Preferências*, e escolha a aba *Privacidade*. Ali é possível mandar o Firefox dizer aos *sites* que o usuário não quer ser rastreado. Também é possível selecionar o nível de memorização de dados pessoais – entre tudo, nada, ou uma série de configurações, podendo definir a navegação privativa como padrão, e estabelecer que, ao ser fechado, o navegador deve apagar todos os dados daquela sessão.

IE9
No navegador, vá em *Ferramentas* e em *Opções de Internet*. Clique em *Privacidade*. É possível vetar ou aprovar o recebimento de *cookies*, em vários níveis. Clicando em *Sites*,

você pode criar uma lista de páginas a ser bloqueadas. Para não fornecer a terceiros a informação sobre onde está o computador no qual você está, selecione a opção *“Nunca permitir a Sites solicitar minha localização”.*

Android
Clique em *Ajustes* e vá em *Serviços de Localização* para desligar a identificação de local. É possível determinar se aplicativos poderão usar o recurso. Em *Codificação* ficam as opções de criptografia dos dados do telefone e do cartão SD. Ao acionar os recursos, o telefone passa um bom tempo convertendo os dados para um sistema mais seguro. O usuário deverá definir uma senha, a ser inserida sempre que o aparelho for ligado.

iOS
No iPhone, no iPad e no iPod Touch, vá em *Ajustes* e escolha *Privacidade*. Desabilite o serviço de localização para não ser rastreado. É possível escolher quais aplicativos poderão coletar esse tipo de informação. Quem autorizar a Câmera, vai revelar o local das imagens publicadas no Facebook, por exemplo. Em Facebook e Twitter há a lista dos *apps* com permissão para acessar a conta pessoal nesses *sites*.