Cartilha de Segurança para Internet

FASCÍCULO

DISPOSITIVOS MÓVEIS

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

O USO DE *TABLETS*, *SMARTPHONES* E CELULARES ESTÁ CADA VEZ MAIS COMUM E INSERIDO EM NOSSO COTIDIANO

Caso tenha um dispositivo móvel (*tablet*, *smartphone*, celular, etc.) muito provavelmente você:

- costuma levá-lo aos locais que frequenta, como sua residência, trabalho, escola, restaurante, cinema, ônibus, metrô, etc.
- mantém informações pessoais nele armazenadas, como compromissos, lista de contatos, chamadas realizadas e mensagens recebidas
- mantém informações de trabalho nele armazenadas e/ou por meio dele acessa seu *e-mail* profissional
- procura por novidades tecnológicas, como novos recursos, aplicativos, modelos ou opções de uso
- procura estar conectado, seja para manter-se informado sobre o que está ocorrendo ou para publicar informações
- frequenta locais onde sempre tem alguém usando um dispositivo móvel, seja para tirar fotos, acessar *e-mails*, ler notícias ou comentar sobre o que está fazendo.

Se você apresenta um ou mais destes comportamentos, é importante estar ciente dos riscos que o uso de dispositivos móveis podem representar para que, assim, possa tomar os devidos cuidados.

DISPOSITIVOS MÓVEIS: MOBILIDADE COM SEGURANÇA

RISCOS PRINCIPAIS

Os dispositivos móveis, além de funcionalidades similares aos dos computadores pessoais, também apresentam os mesmos riscos. Além disso, possuem características que podem torná-los ainda mais atraentes para pessoas mal-intencionadas. Alguns destes riscos são:

» Vazamento de informações

- informações armazenadas nos aparelhos, como mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, senhas e números de cartão de crédito, podem ser indevidamente coletadas
- os aparelhos costumam ser rapidamente substituídos por novos modelos, sem que sejam tomados cuidados para excluir as informações gravadas

» Maior possibilidade de perda e furto

- em virtude do tamanho reduzido, do alto valor financeiro e do *status* que representam, além de estarem em uso constante, podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes

» Invasão de privacidade

- como estão sempre à mão alguém pode tirar uma foto sua e publicá-la, sem seu conhecimento ou permissão. Isso pode expor mais informações do que realmente você gostaria

» Instalação de aplicativos maliciosos

- dentre a grande infinidade de aplicativos disponíveis, podem existir alguns com erros de implementação, não confiáveis ou especificamente desenvolvidos para execução de atividades maliciosas

» Propagação de códigos maliciosos

- você pode receber mensagens contendo códigos maliciosos e, caso não seja cuidadoso, ter seus equipamentos infectados, seus dados coletados, participar de ataques na Internet e contribuir para a disseminação de *spam*

CUIDADOS A SEREM TOMADOS

ANTES DE ADQUIRIR UM DISPOSITIVO MÓVEL

» Observe os mecanismos de segurança disponibilizados pelos diferentes modelos e fabricantes
  - escolha aquele que considerar mais seguro

» Não adquira um dispositivo ilegalmente desbloqueado (*jailbreak*) ou cujas permissões de acesso tenham sido alteradas
  - além de ilegal, isso pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho

» Restaure as configurações originais, ou "de fábrica", caso opte por um modelo usado

AO USAR SEU DISPOSITIVO MÓVEL

» Instale um programa antivírus, **antes de instalar qualquer tipo de aplicativo**

» Instale também outros mecanismos de segurança, como *antispam*, *antispyware* e *antimalware*
- não se esqueça de mantê-los atualizados

» Mantenha-o seguro
- com a versão mais recente de todos os programas instalados
- com todas as atualizações aplicadas

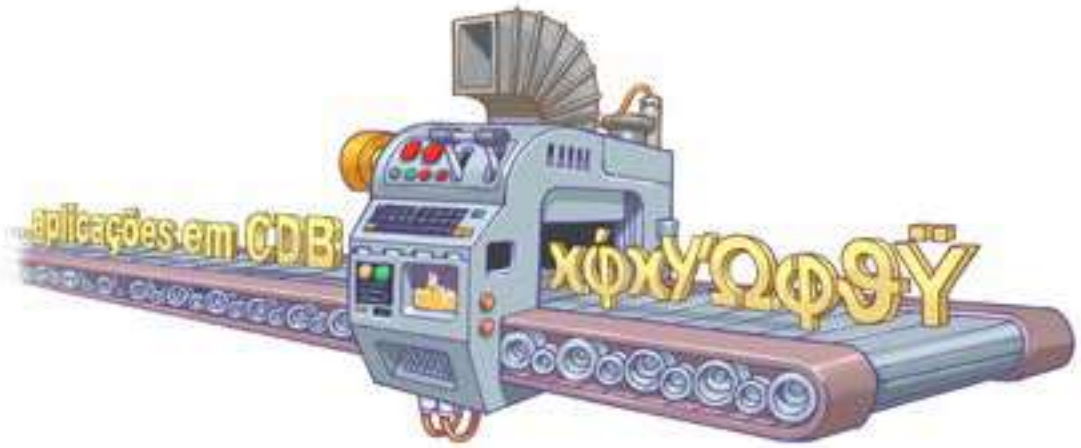
» Não siga *links* recebidos por meio de mensagens eletrônicas (SMS, *e-mails*, redes sociais, etc.)
- desconfie de mensagens recebidas, mesmo que enviadas por conhecidos

» Mantenha controle físico sobre o seu dispositivo
- principalmente quando estiver em locais considerados de risco
- procure não deixá-lo sobre a mesa e cuidado com bolsos/bolsas quando estiver em ambientes públicos

» Proteja suas senhas
- cadastre senhas de acesso bem elaboradas
- se possível, configure-o para aceitar senhas complexas (alfanuméricas)
- 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

» Proteja sua privacidade
- seja cuidadoso ao:
  - publicar sua geolocalização
  - permitir que aplicativos acessem seus dados pessoais

» Proteja seus dados
- configure:
  - uma senha de bloqueio na tela inicial
  - para que seja solicitado o código PIN
- faça *backups* periódicos
- mantenha as informações sensíveis em formato criptografado
- use conexão segura sempre que a comunicação envolver dados confidenciais



AO INSTALAR APLICATIVOS

» Procure obter aplicativos de fontes confiáveis, como lojas oficiais ou o *site* do fabricante

» Escolha aqueles que tenham sido bem avaliados e com grande quantidade de usuários

» Verifique com seu programa antivírus antes de instalar um aplicativo

» Observe se as permissões para a execução são coerentes com a finalidade do aplicativo

- um aplicativo de jogos, por exemplo, não necessariamente precisa ter acesso a sua lista de chamadas

AO ACESSAR REDES

» Seja cuidadoso ao usar redes Wi-Fi públicas

- desabilite a opção de conexão automática

» Mantenha interfaces de comunicação, como *bluetooth*, infravermelho e Wi-Fi, desativadas

- somente as habilite quando necessário

» Configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou "descoberto") por outros aparelhos

AO SE DESFAZER DO SEU DISPOSITIVO MÓVEL

» Apague todas as informações nele contidas

» Restaure as configurações de fábrica

EM CASO DE PERDA OU FURTO

» Configure-o previamente, se possível, para que:
  - seja localizado/rastreado e bloqueado remotamente, por meio de serviços de geolocalização
  - uma mensagem seja mostrada na tela (para aumentar as chances dele ser devolvido)
  - o volume seja aumentado ou que saia do modo silencioso (para facilitar a localização)
  - os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso
    - cuidado com essa configuração: principalmente se você tiver filhos e eles gostarem de brincar com o seu dispositivo

» Informe sua operadora e solicite o bloqueio do seu número (*chip*)

» Informe a empresa onde você trabalha, caso haja dados e senhas profissionais nele armazenadas

» Altere as senhas que possam estar nele armazenadas

» Bloqueie cartões de crédito cujos números estejam nele armazenados

» Ative a localização remota, caso você a tenha configurado
  - se achar necessário, apague remotamente todos os dados nele armazenados

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**.

creative commons

cartilha.cert.br/cc

outubro / 2020