Publicação cert.br

Cartilha de Segurança para Internet

Fascículo Dispositivos Móveis

https://cartilha.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.

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

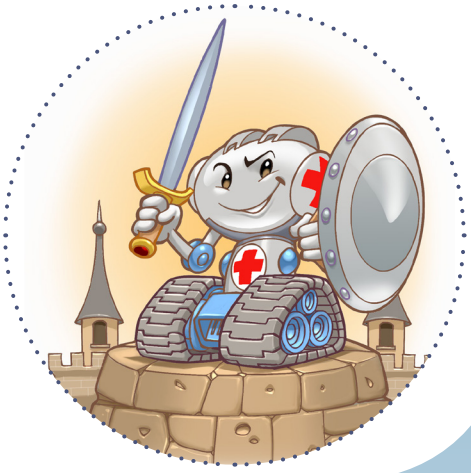
- ✓ Maior possibilidade de perda e furto
  - em virtude do tamanho reduzido, do alto valor financeiro e do *status* que representam, além de estarem em uso constante, podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes

- ✓ 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
- ✓ restaure as configurações originais, ou "de fábrica", caso opte por um modelo usado
- ✓ 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.

Ao usar seu dispositivo móvel:

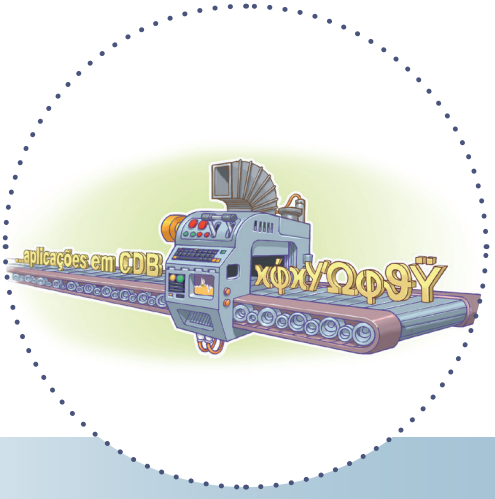
- ✓ instale um programa antivírus, **antes de instalar qualquer tipo de aplicativo**
- ✓ instale também outros mecanismos de segurança, como *antispam*, *antispyware* e *antimalware*
  - não se esqueça de mantê-los atualizados
- ✓ mantenha-o seguro
  - com a versão mais recente de todos os programas 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.

Consulte a **Cartilha de Segurança** para mais detalhes sobre os riscos e os cuidados a serem tomados para proteger seus dispositivos móveis:

https://cartilha.cert.br/dispositivos-moveis/

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/.

março / 2017