Input TECNOLOGIA

www.input.com.vc

Dispositivos móveis:

Mobilidade com segurança

Segurança da Informação

Dispositivos móveis
Mobilidade com segurança

O uso de tablets, smartphones e celulares está cada vez mais comum e inserido em nosso cotidiano, por essa razão, é importante estar ciente dos riscos que o uso de dispositivos móveis podem representar para que, assim, se possa tomar os devidos cuidados.

Riscos principais

Os dispositivos móveis, além de funcionalidades similares aos dos computadores pessoais, também apresentam os mesmos riscos. E ainda 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.

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.

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.

Fonte: www.cert.br

Dispositivos móveis
Mobilidade com segurança

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 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.

Fonte: www.cert.br

Dispositivos móveis
Mobilidade com segurança

Cuidados a serem tomados

Ao usar o 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 clique em links recebidos por meio de mensagens eletrônicas:

- 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.

Proteja sua privacidade:

- seja cuidadoso ao publicar sua **geolocalização**;
- cuidado ao 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.

Fonte: www.cert.br

Dispositivos móveis
Mobilidade com segurança

Cuidados a serem tomados

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).

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

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.

Fonte: www.cert.br

VISITE O SITE

Input®
TECNOLOGIA

www.input.com.vc

+55 (11) 3976.8000

/input.com.vc