

as well as (actually, much better than) BlackBerry, BlackBerry devices have fallen out of vogue. However, BlackBerry is still around and there are still plenty of BlackBerry users out there. (Note that newer BlackBerry phones run Android rather than the old proprietary BlackBerry OS.)

## Considering Security for Mobile Devices

As a network administrator, one of your main responsibilities regarding mobile devices is to keep them secure. Unfortunately, that's a significant challenge. Here are some reasons why:

- » **Mobile devices connect to your network via other networks that are out of your control.** You can go to great lengths to set up firewalls, encryption, and a host of other security features, but mobile devices connect via public networks whose administrators may not be as conscientious as you.
- » **Mobile devices are easy to lose.** A user might leave her smartphone at a restaurant or hotel, or it might fall out of her pocket on the subway.
- » **Mobile devices run operating systems that aren't as security conscious as Windows.**
- » **Users who wouldn't dare install renegade software on their desktop computers think nothing of downloading free games or other applications to their handheld devices.** Who knows what kinds of viruses or Trojans these downloads carry?
- » **Inevitably, someone will buy his own handheld device and connect it to your network without your knowledge or permission.**

Here are some recommendations for beefing up security for your mobile devices:

- » Establish clear, consistent policies for mobile devices, and enforce them.
- » Make sure employees understand that they aren't allowed to bring their own devices into your network. Allow only company-owned devices to connect.
- » Train your users in the security risks associated with using mobile devices.
- » Implement antivirus protection for your mobile devices.