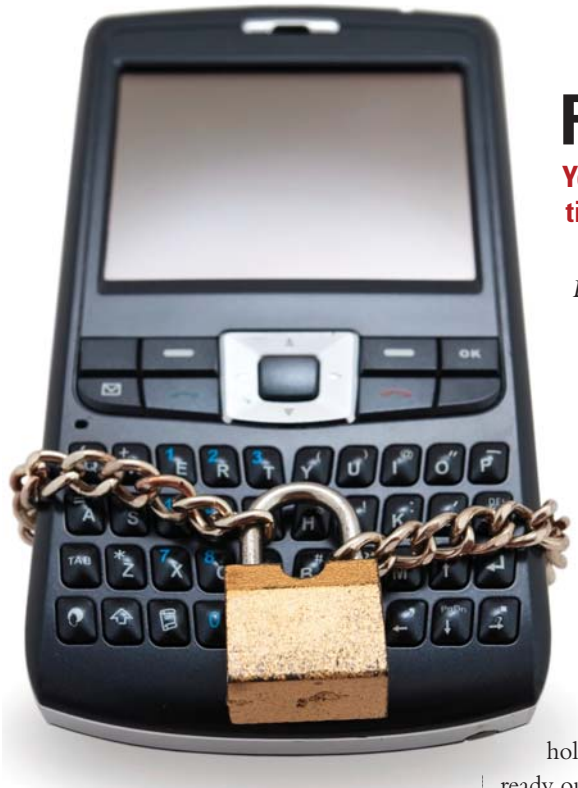

Feeling insecure?

You should be. Here are 12 smart security tips for your smartphone.

By Luigi Benetton

Question: Where's your BlackBerry?

More than 106,000 mobile phones went missing in 2009, according to the FBI's National Crime Information Centre.

If yours was one of them, you probably scrambled to find it as quickly as possible because it's a nuisance to replace a mobile phone. But did you ever consider what you stood to lose?

Tech-savvy lawyers who use the devices for billing, practice management, knowledge management and dictation, as well as contacts, e-mail, and calendars can suddenly find themselves missing some valuable information. And instead of being worried about replacement costs, they're suddenly worried about data breaches — and potential breaches of confidentiality and lawsuits.

That's why it's so important to get smart about smartphone security.

Choose a secure smartphone

Many lawyers use Research in Motion (RIM) Limited's BlackBerry. From a security perspective, that's a great choice.

"The Blackberry is well over 10 years old, and its roots are with enterprise and government customers," says Michael Brown, RIM's director, security product management. "When it was first marketed, RIM was told that if the BlackBerry puts customer information at risk in any way, it would be a non-starter."

"RIM's security approach is holistic. All the security tools are ready out of the box. You don't need bolt-on stuff."

Although Dan Pinnington thinks BlackBerry's security features are basically sound, he says there's more you can do to protect data on smartphones. "Out of the box, other smartphones aren't as secure," says the director, practicePRO for the Lawyers' Professional Indemnity Company (LAWPRO), "but you can take steps to make them secure."

Having to "bolt-on" security hasn't discouraged many enterprises from trying other smartphones, like Apple's iPhone, Google Android and Windows Mobile. RIM's competitors covet RIM's market, so expect them to substantially pick up their security game.

Talk to your IT department…

Many businesses have security policies in place governing every type of electronic communication employees may use.

… and ask for further education

A simple lunch-and-learn led by the firm's mobile device experts can set the record straight on everything from the choice of device to the reasoning behind policies.

"Not everybody is a security expert," Brown notes, adding, "It's a mindset shift for people to view their phones as computers."

Enable the passcode

Smartphones can be set to automatically lock themselves after a period of inactivity. To unlock them, the user needs to enter a code.

Prevent excessive attempts at the code

Thieves can be foiled by passcode-protected smartphones set to erase all data after a certain number of failed passcode attempts.

Encrypt the device

Devices are also useless to data thieves if they can't read the information on them. That's why many phones can encrypt all the data they hold. Specific applications may also encrypt their data.

Control access to applications

RIM's Brown notes that the BlackBerry's Application Control lets administrators or users control what specific applications can do on the device. This feature helps defend the device against malware and third-party applications which could cause data breaches.

Use VPN

Like computers, today's smartphones let people access corporate applications, so it's only natural that virtual private networks (VPN) should also make the jump to smartphones. VPNs enhance the security of a connection between a server and a device

ISTOCKPHOTO

outside the organization's firewall.

Beware unsecured Wi-Fi connections

Budget-conscious owners may prefer to use free Wi-Fi connections in places like coffee shops to keep cell charges to a minimum.

Pinnington recommends people think twice. "You could be connecting to a wireless access point that is illegitimate," he says, "one that is set up to look legitimate but captures your ID and passwords as you log in."

> **"You could be connecting to a wireless access point that is illegitimate…"**
>
> **Dan Pinnington, LAWPRO**

Back up your smartphone

Smartphones are made to be connected to computers and synchronized with both computer- and Internet-based systems. While synchronizing regularly won't prevent a data breach from a lost or stolen handset, it will enable the owner to recover data from that phone — appointments, tasks, contacts, documents and so forth — and in some cases put it on a new phone.

Tell your IT department about lost phones

And don't wait. The sooner IT staff know, the faster they can react.

Act remotely

A lost smartphone does not automatically lead to a data breach. Most smartphones let IT staff (or savvy smartphone owners) make some of the following evasive manoeuvres via the Internet:

- "wipe" the data off a phone;
- set a passcode (useful for people who did not set it prior to losing the phone);
- locate the phone;
- flash a message (e.g. reward if found, call 123-456-7890) when the phone is powered on;
- make the ringer sound, even if the phone is set to silent mode. ■

Luigi Benetton is a freelance writer in Toronto.