



## Fact Sheet

### Privacy on the Go: **10 Tips for Individuals** on Protecting Personal Information on Mobile Devices

*Mobile devices such as smart phones, laptops, tablets and USB keys have rapidly become part of daily life. These tools offer tremendous convenience; however, they also raise important new risks for privacy and the protection of personal information.*

*Mobile devices are increasingly powerful and can hold massive amounts of personal data. They are also small, which means they are easy to lose – or steal. Like personal computers, they are also vulnerable to threats such as viruses and spyware.*

*Once your personal information is compromised, you can never really get it back and it can be used in ways that could cause you significant personal and financial harm.*

*There are steps that individuals can take to mitigate the risks. Here are some of the basics:*

#### **10 Tips for Protecting Privacy**

1. Educate yourself about your mobile devices and how to enable or add privacy and security tools.
2. Limit the personal information that is stored on mobile devices to that which is absolutely necessary.
3. Ensure that mobile devices are protected with hard-to-guess passwords. Never rely on factory setting passwords.
4. Use an automatic lock feature so that a password is required to access information on mobile devices.
5. Consider using an up-to-date encryption technology to provide added protection for personal information on mobile devices. Without encryption, personal information is vulnerable to unauthorized access. Encryption involves using an algorithm to transform information into text that is unreadable without a “key” to read the code.
6. Install and run anti-virus; anti-spyware and firewall programs on your mobile device – and keep those programs up-to-date. Attacks against mobile devices – from spam, viruses, spyware and theft – are on the rise. For example, downloading an infected program could infect a mobile device.
7. Don’t send personal data over public wireless networks – at cafés, for example – unless you have added security such as a Virtual Private Network (VPN). Public wireless networks may or may not be secure and there is a risk that others may be able to capture data sent over these networks.

8. Never leave your mobile device unattended in a public place or a vehicle. Across North America, hundreds of thousands of mobile devices are lost or stolen every year. One survey by an information security and privacy research centre suggest that a laptop has a 5 to 10 per cent chance of going missing over a three-year period.
9. Ensure that data stored on mobile devices that are no longer needed is purged prior to disposal.
10. These tips are intended only as an introduction to protecting personal information in a mobile workplace. Check the user manuals for your mobile device for further information.