Essential Mobile Security Tips Cheat Sheet

by David Pollack (Davidpol) via cheatography.com/2754/cs/8254/

Introduction

If your laptop (or other mobile device you work on) were lost today, what's the worst that could happen? That's the question everyone who works remotely should ask, especially before working on the road or using unprotected public networks.
Securing your portable devices—whether they're laptops, netbooks, BlackBerrys, USB memory sticks, etc.—and the data that's accessed by them from loss and cybercrime may be your most important responsibility as a mobile worker.

http://mobileoffice.about.com/od/mobilesecurity/tp/mobilesecuritytips.htm?utm_content=5471263&utm_medium=email&utm_source=cn_nl&utm_campaign=computersl&utm_term=

1. Carefully consider what sensitive information

Carefully consider what sensitive information is stored on your laptop/device.

Make sure any sensitive or confidential information stored on your laptop, cell phone, and other mobile devices really needs to be there. Sensitive data includes proprietary company or client information, as well as customers'—and your own—personally identifiable information (such as credit card numbers, Social Security numbers, or even just names and birthdays). Unless you truly need to directly access this info while you're mobile, consider removing the data completely or just remove the sensitive portions of it..

2. Take extra precautions to protect

Take extra precautions to protect any sensitive data you do need to access.

Storing the data on a server, if possible, and accessing it via secure methods (like VPN) would be safer than storing it locally. If that's not possible, use a program like the open-source and cross-platform disk encryption tool VeraCrypt to secure all local files and folders you wouldn't want anyone to access in the event of theft or loss.

3. Perform regular, essential maintenance.

Backups are like insurance—while you don't want to ever have to need it, you'd be glad to have it in an emergency. So, especially before taking your mobile devices on the road, it's vital to make a backup of your documents—or, better yet, a clone of your entire hard drive—and keep it in a safe, separate location from your main device. Also get the latest security updates and patches for your operating system, browser, firewall, and antivirus programs. These should all be part of your regular computer/device maintenance..

4. Protect your passwords and logins.

First, make your passwords are strong enough. The, make sure you're not storing your logins anywhere they could be easily discovered or stolen. For example, turn off your browser's automatic password-remembering functions, delete any saved login shortcuts (like cached VPN credentials), and shred any passwords you have written down. Instead, you can use password management software to help securely store and remember your username and password combinations.

5. Secure your Internet connection.

Connect to networks using the highest level of security available, such as WPA2 for wireless networks. Connecting to unknown, open wireless networks is very risky. If only unsecured networks are available (e.g., at public wireless hotspots), take extra care with these steps:
• Disable the "automatically connect to non-preferred networks" setting to make sure you connect only to approved wireless access points.
• Turn off file and printer sharing.
•Switch off your wireless card when not in use (how to do this will depend on your device; see the manufacturer's documentation).
•Use only VPN or other encrypted tunnels for business use (these instructions should be provided by your company's IT department).
•For safer, anonymous Web surfing, consider using a Web proxy or VPNs designed for consumer use. Here are 3 of the best VPN services you can subscribe to.

6. Take steps to prevent the physical theft

Keep an eye on your property when in public, use inconspicuous bags to carry your items (like a backpack holding your laptop in a protective sleeve), and, in general, try not to advertise that you have theft-worthy devices on hand. Hard-to-remove imprints or labels applied to cases, cable locks, and other security devices can also thwart would-be thieves.

7. Be proactive about protecting your data now.

If your laptop or other device does get stolen or lost, tracking services and recovery software products, as well as features such as remote wipe for BlackBerrys and other smartphones, can help you get it back--but you have to set up the software/service first (i.e., before your device disappears).

By **David Pollack** (Davidpol)
cheatography.com/davidpol/

Published 1st June, 2016.
Last updated 20th May, 2016.