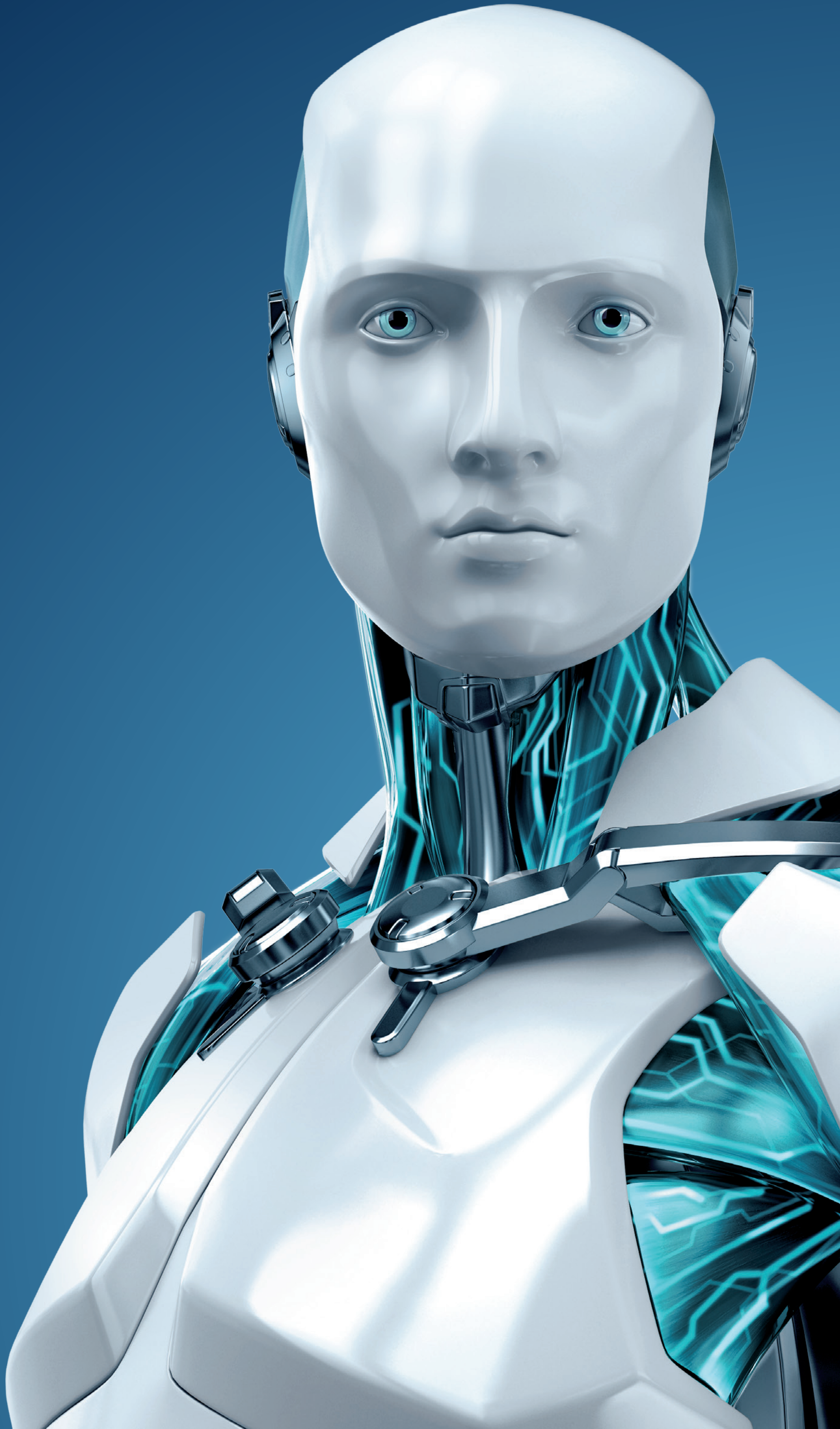
TECH BRIEF

5 physical security tips for protecting your digital devices



ESET®

ENJOY SAFER TECHNOLOGY™

5 PHYSICAL SECURITY TIPS FOR PROTECTING YOUR DIGITAL DEVICES

By Cameron Camp, ESET Security Researcher

As we read earlier this week, the chances that one or more of your digital devices may get stolen are uncomfortably high. So what would happen if your mobile device falls into the wrong hands? Here are a few tips that will help minimize the damage if it happens to you.

1. Password-protect your computing devices.

While it sounds obvious, if anyone steals your device they will have to defeat your password to get at your data and accounts, which will significantly slow attackers. Although it is not impossible to defeat password protection on a digital device, it adds a useful layer of protection, buying you time to locate and recover the device.

2. Always back up your files.

Even if you can't recover a stolen device, that does not mean you have to lose all your information and software. Regular backups are the ultimate defense against theft of your files. There are plenty of options for backup these days including online backup. My colleague David Harley has written about backup on a blog[1], and for more information see Aryeh Goretsky's white paper on the subject[2].

Taking the time to set up backup really pays off if a device is stolen, helping reduce the pain involved in re-creating the sensitive content.

3. Use tracking software to help get your stolen device back.

Getting your stolen device back is not impossible, particularly if the device itself can tell you where it is and you can communicate with it using a sort of "remote control" via SMS or other methods. You may even be able to communicate with the person who has it.

4. Don't tempt thieves with unattended mobile devices, particularly in public places.

Leaving your computer or mobile device unattended in a car, airport or restaurant is akin to asking for it to be stolen. In a recent survey[3] we found that one in five stolen devices were taken from a car, 12% from an airport, train, bus, or other means of public transportation, and 11% from a restaurant or coffee shop.

5. Encrypt sensitive data.

Storing sensitive data in encrypted files prevents anyone exploiting your data if your computer is stolen. Your computer may interact with sensitive data but it does not need to store all of it right there in one place. Consider using encrypted removable media for sensitive data and carrying that separate from the computer. Maybe leave sensitive work files on the company network and access remotely over a secure connection. This way, if "bad things" happen, you'll have a much lower likelihood that the bad actors get off with critical information.

[1] David Harley's Blog. http://www.welivesecurity.com/2011/08/25/backup-basics/

[2] Aryeh Goretsky White Papers. http://www.eset.com/fileadmin/Images/US/Docs/Home/Staying_Secure/2205_19_0_EsetWP-OptionsBackingUpComputer.pdf

[3] Survey. http://www.welivesecurity.com/2013/01/14/are-digital-device-theft-fears-justified-survey-says-yes/