Maastricht University

12 March 2015

Safe use of Tablets and SmartPhones

This document helps you find out how to securely use your tablet or smartphone.
This document is intended to be a general advice to Maastricht University end-users.
If you (also) use your tablet or phone (private or UM-owned) for business purposes, processing confidential data like business e-mails, additional regulations may apply.
Contact your local IT-staff or Servicedesk-ICTS for specific information.

Mobile Device Technology

Mobile Device Technology delivers powerful and convenient tools for users for their communication with others, social networking, online shopping, information gathering and lots other activities. Mobile devices are becoming an increasingly important part of our daily lives, so we strongly encourage you to take some simple but important steps to keep your device safe and secure.

Securing Your Tablet or Smartphone

The first step is to set a passcode or some other screen locking mechanism. Tablets and phones are easy to take wherever you go, which also means they are easy to lose or have stolen. To help prevent your information from falling into the wrong hands, be sure you lock your devices screen with some type of hard-to-guess PIN, passcode or swiping motions. In newer devices, there may be some type of biometric authentication, such as a fingerprint reader. Use the strongest method your device supports, and be sure to set your device so that it locks automatically after a short idle time. If supported by your manufacturer, enable encryption on your devices.
Update your device so it has the latest version of its operating system. Bad guys are constantly finding new weaknesses in software, and vendors are constantly releasing new updates and patches to fix them. By running the latest operating system, you make it harder for anyone to hack into your device.

*Secure your mobile device by enabling some type of screen or passcode lock, enabling data-encryption and by running the latest version of the operating system and your apps.
Be aware of your privacy and Cloud options!*

What Next?

Pay attention when configuring your device for the first time. The most important configuration choices will be your privacy and Cloud options. Privacy is about protecting your personal information. One of your device's biggest privacy issues is its ability to know and track your location. We recommend that you go into the privacy features and disable location tracking for everything, then enable it on an app-by-app basis. For some apps, it is important to be able to track your location (such as mapping software or finding a local restaurant near you), but the majority of apps do not need real-time location information.

The other important option is Cloud storage. Cloud services such as Apple's iCloud, Microsoft's OneDrive, Dropbox or Google Drive allow you to store your data on servers through the Internet. Most devices have built-in options for automatically storing just about anything in the Cloud, including documents, pictures and videos. Think about the sensitivity of your data and decide whether it is appropriate (or even allowed) to store it in the Cloud. Make sure you understand how your data will be protected (such as by a password) and how you can control who will have access to it. The last thing you want is for the private pictures you just took to be posted on the Internet without your knowledge, complete with their geo-location information embedded.

Be aware that apps are increasingly synchronizing data with apps on other devices. This is common with many applications (including Google's Chrome), is pervasive in Windows 8 and is one of the most widely used features of iCloud. Synchronization can be a wonderful feature, but if you have it enabled, don't be surprised to see the sites you visited or the tabs you created on your personal browser (on Tablet or Smartphone) appear in your browser at work.

Finally, in most cases sensitive apps, like your mobile banking app, offer the possibility to secure the app itself with a PIN-code. If possible use this option and choose a different PIN then your initial access PIN.

Keeping Your Device Secure

Once you have your tablet or smartphone secured, you want to be sure it stays that way. Here are some simple steps for you to consider as you continue to use your device:

- Keep your operating system and apps current and running their latest version. Many devices now automatically update your apps, a feature we encourage you to enable.
- Do not jailbreak or hack into your own device. This will bypass a tremendous number of security controls, making your device far more vulnerable to attacks.
- Only download apps you need, and only download them from trusted sources. For iPads, simply download apps from Apple's iTunes App Store only. These apps are screened by Apple before they are made available. For Google, we recommend you to limit your apps to those found on Google Play. While you can download apps from other sites, they are usually not vetted and could be created with malicious intent. Finally, regardless of where you got your app, we recommend you to remove it from your device once you no longer need or actively use it.
- Free apps usually come with embedded advertising popups and reduced functionality. Advertisements often link to servers beyond your control. This imposes a risk of malware infections. Full function apps might also offer security features like PIN-code based access.
- Consider spending a small fee to reduce security risks and enjoy a better user experience.
- When installing a new app, make sure you review and set the privacy options, just like you did when initially configuring your new device. Be careful of what information you allow the app to access, or what you allow the app to do with that information. For example, does the app you just downloaded really need access to all of your contacts?
- Be sure to install or configure software that allows you to remotely track, lock or erase (wipe) your device in case it is ever lost or stolen.

Can I share my device?

Mobile devices are designed to be personal devices. You should not share them with anybody, because sharing your device often means sharing ALL your information on your device and possibly even information stored on servers accessible through your apps.
Some modern operating systems like Googles Android 5.0 Lollipop offer multi user functionality.
If you configure multi user access correctly, you can share your device with guests or co-users without putting your personal data at risk.

Before you Buy:

Put all necessary security functions like biometric authentication, device encryption and multi user support on top of your checklist!

More about information security at UM:
http://www.maastrichtuniversity.nl/informationsecurity

Special thanks to SANS Institute, Securing The Human
http://www.securingthehuman.org