Mobile and Portable Devices – How Safe and Secure is our Data?

(This document was written in 2013 by Mark Vening as an overview to how we as YWAMers can at least be aware of this subject. Things change fast in technology, so ensure you are regularly reviewing your safety and security solutions for your portable and mobile devices.)

Contents

Overview

Almost every YWAMer now uses a portable or mobile device as part of their regular daily routine – but how safe and secure is the data on them? If you were to lose your device – could you track it or recover the information you have stored on it? What about if it was stolen – could anyone hack sensitive or personal data from your device? These kinds of questions may seem low priority to many as we focus on our day to day missionary activities, but with so much information being able to be stored even on our phones, it is something we need to take seriously.

Also, did you know that there are legal requirements under the Data Protection Act that require you to have taken appropriate steps to both secure and encrypt any personal information you may have on your devices that relates to our YWAM activity? In short, that means if you store any personal details of anyone you do business with as a YWAMer, or have exchanged privileged information with them then you are legally required to have secured – and possibly encrypted – your device.

Further, there exists a number of extremely sophisticated hackers and writers of malware, spyware and virus software. Not just spam emails inviting us to 'click here' but clever people who can use our normal internet habits to surreptitiously gain access to our lives. We must not live in fear, but instead ensure we adopt a sensible attitude that protects us from these kinds of intrusions.

What follows are some options you can consider as you look towards responsibly addressing this aspect of your information management.

Backups

It goes without saying that you should be backing up your important data on a regular basis. Free solutions now exist that can back your data up literally as it changes and so there is really no excuse for not including regular backups as part of your normal routine.

Local Backup

This is where you backup your information to a portable storage solution. This would include CD/DVD, USB sticks, external hard drives and so on. I recommend this as part of your daily routine and would encourage you consider dynamic storage (eg external hard drive, USB stick) rather than static storage (write-once CD or DVD).

> ***Did you know…*** *the average shelf life of a home burned CD/DVD is between 5-10 years, and that is if you put it in a dark drawer and never use it! Leave it out in the sunlight or out of its case and CDs have been known to fail within a year.*

There are literally dozens of software solutions out there, and most operating systems have them built in. Both Windows and Mac users can take advantage of them and I know many do.

Free 3rd party solutions also exist for Local Backup:

Windows:	Inbuilt backup for Win XP, Vista, 7 and 8 are available. Google for more info. SyncBack Free (http://www.2brightsparks.com/freeware/freeware-hub.html) Allway Sync (http://allwaysync.com)
Mac:	Time Machine (included with the Operating System and hard to beat) Carbon Copy Cloner (http://www.bombich.com/download.html although only solutions for 10.4 and 10.5 are free).
Linux:	BackupPC (http://www.linuxlinks.com/article/20090106114938518/BackupPC.html) is just one of dozens of solutions. (This also works for **Mac** and **Windows** too.)

Online Storage

This is where you commit your backup data to a 3rd party online storage company in the event that you lose both your device and your local backup. Again, lots of companies offer this (we probably all have Dropbox accounts already) and you can Google for them at your leisure, but I do recommend the following for your consideration:

Sugarsync – www.sugarsync.com – initially a similar looking solution to Dropbox with 5GB for free that you can upgrade. What makes Sugarsync stand out to me is that it backs up your data in real time across all your devices. So if you have a laptop and a phone, for example, the data is backed up on both devices under the one account. Another significant benefit is that you do not have to drag and drop your files into a backup folder (like with Dropbox) but rather just select the folder where it normally resides on your drive and it will be backed up. You can of course share folders privately or publicly for cooperative working too. Sugarsync also works on Android mobile devices and tablets as well as the iPad and iPhone. Very handy!

Box – www.box.com – starts you off with a few GB for free, but if you signup under one of their deals, you can often get 50GB of free lifetime online storage, a benefit you can then invite anyone with the same email domain as you to share. In YWAM Wales, I registered my ywamwales.org address and then was able to offer the same 50GB deal to others with the same domain. You are then permitted to then change that email address to anything else you like – so that if you change email address you can take that account with you.

iDrive – www.idrive.com – very similar to Sugarsync, this allows you to backup on the fly and is Mac/Windows compatible too. It also allows you to choose specific folders on your drive rather than drag over those that you want backing up to another folder.

Security and Encryption

Securing and even **Encrypting** your device should now be considered routine if that device is used for any kind of YWAM business. Technology now exists for you to do this easily – and safely! – built right into modern operating systems. If your computer is lost or stolen, then your drive is as safe from hackers as is realistically possible for users like us – providing you **use** the encryption.

Further, every device you own should have a password, passcode or security option enabled for each time you switch the device on or wake it from standby. This may be a pain – particularly for our mobile phones – but if you lose your phone, and there is no passcode, then a hacker can easily get access to any accounts you have registered with the phone. Enable robust security right now!

Password Management

Remember – if you rely on a passcode or password for your security – make it a strong one. This means that you ensure that each password you use is different, has upper and lower case letters plus at least one number and one symbol. For your mobile device consider a passcode longer than just 4 digits or add a pattern unlock feature to supplement the normal digit unlock.

> ***Did you know…****an eight letter lower case only password can be brute force attacked by a couple of hackers in about a half an hour. Add an upper case letter, a number and a symbol and that becomes over 2 years.*

Managing your passwords can be a thankless task. If you have a few email accounts, a facebook account, a Google account, an online bank account – you get the picture – it can all add up. At my last audit, I have a total of 605 online passwords – which include forums, online shopping and so on. How many do you have – and do they all have the same password?

In my opinion, there is really only one solution – **LastPass**. For $1 a month – about 65p – you can manage ALL your online passwords, identities and form filling and have them integrate with Windows, Mac, Mobiles, iDevices and Linux. If you don't have an account – get one now. If you want a free month – use my referral link: https://lastpass.com/f?1556236

Encryption

As has been mentioned – consider encrypting your devices. This not just because we don't want to embarrass anyone by inadvertently disclosing their personal information sent to us in good faith, but also because the Data Protection Act specifically recommends this in their guidance. You do not want to be in the position where you are held responsible for a breach in data security – even if it was unintentional – through having your device stolen, for example.

Windows

BitLocker – if you have Windows 8 then you can simply use BitLocker. It is also available built in for the high end versions of Windows 7 (Ultimate and Enterprise). Simply enable it and you are done.

TrueCrypt - http://www.truecrypt.org/ - if you have Windows XP, Vista or Windows 7 Home or Professional, then the free Truecrypt will do the same job as BitLocker just as well. This excellent software is well supported and easy to use and can be configured to encrypt your USB stick, user data or even your whole drive. It is fully reversible and has a negligible impact on speed.

Mac

FileVault – use this inbuilt software to encrypt sensitive files and data. The very recent versions of Max OSX now include FileVault2, which has even more options.

Truecrypt – the same software as described for Windows is available for the Mac

Linux

Inbuilt – many distros now include encryption. See the support pages for your particular one.

Truecrypt – the same software as described for Windows is available for many distros.

Mobile Devices/Tablets

Phones and Tablets are most easily stolen and therefore are a non-negotiable for security and encryption. Do not forget to ensure to encrypt removable storage such as SD cards – and use strong passwords for your accounts.

Windows and Android

Encryption – this is built into both operating systems. Normally accessible through Settings, you can Google this for more information specific to your device. In addition, you can check the Windows Market or Play Store for more 3rd party solutions.

iPad and iPhone

Passcode – you can enable your iDevice to require passcode entry that will then erase the iDevice after a certain number of failed attempts. Do an iTunes backup on your laptop/desktop and then enable this function on your portable device. In addition there are 3rd party apps that allow you to do the same that you can check out in the App Store.

Security Software

Having appropriate security software on your device allows you interact with the internet with at least a measure of confidence. Spyware, malware and virus software makes the internet a place to be respected from a security perspective and different devices are exposed in different ways. Make sure you have a solution that is appropriate, and remember, the internet is a fast moving place, so ensure you update your solutions regularly.

Safe Internet Practice

No software will protect you entirely, so it is worthwhile becoming familiar with safe internet practices to minimise your risk of infection. Here are a few suggestions:

1. Never surf the internet without some kind of antivirus solution appropriate to your device. (The risk is much lower on an iDevice or Android/Linux device, but not entirely zero. Check out this article from The Telegraph about Macs - http://j.mp/15B0LlR)
2. Avoid opening email attachments or clicking on links from people you don't know
3. Do not install security programs that promise protection unless:
    a. You are technically savvy and can assess them – they may be masquerade software
    b. You have had a personal recommendation from someone you trust
4. Avoid browsing dodgy websites. You all know what I mean – 'free' music or video download sites (for 'free' read 'pirate') or crack/warez sites. If you visit these sites expect trouble!
5. Regularly update your solution and run full scans at least weekly

Windows Laptops: There are an extraordinary number of free solutions, but I recommend the free Windows product 'Microsoft Security Essentials'. In Windows 8 it is built in, but for other editions visit http://www.microsoft.com/security/default.aspx for more information.

Mac: a large number of solutions exist, but for OSX a recommended solution is from Sophos software. Free and compatible with all versions you can get it from here: http://j.mp/YHZJiE

Linux: amongst the enormous amount of free software out there, I again recommend the solution from Sophos. Read about it here: http://j.mp/YhmRoi

iPad/iPhone/Android: much debate rages as to whether security software is needed. Should you want something robust and free, then the software from LookOut is likely to suit – and it works on all mobile platforms. You can read about it here: https://www.lookout.com/features
(Note: only the security option is free, the other features of the software require a subscription)

> ***Did you know…****do not be tempted to run two kinds of solutions at the same time. Security software works by checking changes and monitoring access to running files. Therefore, if one type of Security Software checks a set of files, the other will note the access and then proceed to check the same files. This can set off a loop which slows the computer as the two 'fight' to confirm the files are not infected. Pick one good solution and stick to that.*

Lost Devices

If the worst happens and you leave your laptop on the plane or have your device stolen your capability to manage your device may not yet be over. Many solutions exist that allow you locate your device, gain access to it, wipe sensitive data and even activate the on-board camera to see what it sees.

Whatever solution you have applied towards securing and encrypting your device, do not leave it too long before contacting your financial institutions and changing other important passwords. If you find your device the next day, it is going to be far easier to update it with the new passwords rather than enter into a lengthy process trying to regain access to those accounts that are now under the control of a hacker or thief because you thought you should 'give it 24 hours to see if it turns up'.

Prey Project

Below are some device-specific ideas that you might wish to consider when considering this kind of software. For an interesting free solution, you might want to consider the **Prey** software that runs on all devices. This open-source software allows you to manage all your devices independent of operating system or architecture. The free plan lets you cover up to 3 devices and they have a growing reputation amongst users and reviewers. I strongly recommend you consider this option as part of your security review. http://www.preyproject.com

Other Software

Windows Laptop: if you are using encryption technology such as BitLocker or Truecrypt, you have a good chance that your data is secure until such time as you can contact your financial institutions and change other important passwords. Should you want a solution for remote tracing and wiping, a competitively priced options such as Computrace or LoJack are available from **Absolute**. http://www.absolute.com .

Windows Mobile: use the **MyPhone** service. Full information can be found here. http://www.windowsphone.com/en-GB/how-to/wp8/basics/find-a-lost-phone

Android Phone/Tablet: for a free solution, I highly recommend **AndroidLost** (along with Prey, my own personal choice). http://www.androidlost.com/

Mac and iDevices: use the **iCloud** solution provided free by Apple.
https://www.icloud.com
(be sure to visit this on your laptop or desktop device to set it up first)

Honourable Mention: the previously mentioned **LookOut** software has a comprehensive solution for all mobile devices – but at the cost of a small monthly premium. Lots of functionality with professional help to go with it. Check it out here: https://www.lookout.com/features

If you own anther kind mobile device, you may find this article useful:
http://mobileoffice.about.com/od/mobilesecurity/qt/smartphone-remote-wipe.htm

What the Law Says

There are lots of rumours out there about just what exactly is the 'Data Protection Act' and how it applies to movements like YWAM. The Information Commissioner's Office (ICO) is the government department responsible and they have a great online guide to aid with understanding the Act.

The document you are reading is primarily concerned with **Principle 7** of the Act (there are 8 in total) which states:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

The full details of this principle are available here:
http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7

It is worth having a quick read of this page (takes about 5 minutes) to see whether or not your personal data protection is robust enough when considered in light of the above link. I definitely found one significant hole in my personal system which I am now closing.

For those that prefer a YouTube to help you understand, you can watch the ICO video on this page: http://ico.org.uk/for_organisations/data_protection which also links you to the rest of the 8 principles and lots more information.

Ignorance is no protection if you find yourself in breach of the Act. So please ensure that you have reviewed your personal data protection plan – especially if you hold sensitive or personal information on your mobile devices.