# Radio Days – 2009-12-12

## *Tip of the Week – Viruses Galore*

A client rang me to get his computer working again after a successful virus attack. A week later I had another call to clean his computer because it had again become infected by a virus. This new virus, and probably the previous one, had attacked his computer inside an infected download using a program called LimeWire. LimeWire is used by many people to download music, and is also often used to infect computers. The advice which I have received from an expert user is to ensure that you only download mp3 music with a bit-rate of at least 128 kbps.

This, according to my source, is the only way to ensure that you do not become infected when you are using LimeWire to download music. It will also help keep your computer safe from the annoyance of having a recently-cleaned computer slowing down with a new virus almost immediately.

Another way to ensure that you do not get a virus with your music is to use one of the music download sites where you have to pay for each song. The main advantage of this is that you can be sure that the song does not contain a virus. While this suggestion does go against the general trend of wanting everything for nothing it can be cheaper than repairing, every week or so, the damage caused by yet another virus attack.

## *Passwords Galore*

Many people have one or two passwords because that is all that they can remember. Others keep a password list written on sticky notes stuck to their screen or one a sheet of paper which is kept in an obvious place. These practices are becoming more unsafe as intruders can get a single password and use it to access all your supposedly secure places.

There is a better way to handle passwords, and it is both free and simple to use. This new and improved method is a free program called *KeePass*. The word *KeePass* is a contraction of *Keep* and *Passwords*. KeePass stores passwords which you generate or, for a better solution, passwords which it generates for you. You do not need to remember these passwords (they are stored by the program itself in a protected safe) so they will be longer and more complex than those which you would create yourself.

As many people will know, people who want to gain access to your usernames and passwords are often able to guess them using a *dictionary attack*. This involves getting a copy of an electronic English (or American) dictionary (and there are plenty around) then using this to guess both your username and password for any web site or program. Once this method has found one username and password combination it will be tried for all other sites and programs which you use.

The only requirement for the safe storage of all your passwords is a secure password to protect your KeePass safe. This password must not be too easy to guess. There are various techniques for creating secure passwords (and you only need one to lock your KeePass safe, remember!) which are available with a quick Google search. Create one good password for your KeePass safe and use it to generate and store all the other passwords which you need in today's multi-password mayhem which passes for a life.

## *Websites*

| | |
|---|---|
| KeePass | www.keepass.info |
| Google | www.google.com.au |