

Extract from ITsorted Newsletter – March 2009

Security issues and Backups

for ICT workers

It was in the 'Press' a lot last year ... lost and stolen data. What's reported is mostly government, local authorities and financial institutions. But it happens to small organisations too!

Don't become one of the statistics!

Each of you has a responsibility to ensure that the data you hold on people remains secure. Make sure that you have a procedure and guidelines in place for your organisation.

Here we only skim the surface, but we do provide links to where you can find out more.



contactLINK related Security issues

Access to contactLINK

Do you need to ensure that all users are using a password? They all start off blank. Users can change their password from the Tools menu.

What permissions do different users have? They often start off with full System Administrator rights! Change these from the Admin menu, System Users option.

Data security

Make sure that if any or all of the data from contactLINK is copied from your office server it is kept secure and staff are made aware of the importance of this.

E.g. off-site backups, copies on laptops, sending data via email

Consider password protecting laptops (i.e. they need a password entered on start up, similar to logging onto the office network)

Password protect files you send by email (we can provide instructions for this on request).

Backing up contactLINK

The only file that is crucial is **contactLINK DATA.mdb**. However you may prefer to and it may be easier to backup the entire contactLINK folder.

Some general Security issues

Data on laptops

If anyone takes a laptop off-site they should have a password set up on it (on the laptop itself and not just the data!).

Sending data outside of your office

Whether by post, on CD or USB key or as an email attachment – is it secure? Email us for instructions on how to password protect files that contain sensitive data **before** you send them out.

Backups

Very recently our server had a hard disk crash and 90% of what was on our server was unavailable!

Fortunately, we had a backup procedure and were able to recover nearly everything from our backups – and we're now up and running again.

“It's not how many times you fall that matters; it's how many times you get back up.”

Unfortunately, we had trouble with one of our backup arrangements and as a result we lost most of our emails - not critical, but very useful and there were a lot of them! On the bright side, it's been like a rather drastic spring clean!

But it could easily have been much worse if we had been less prepared, and we've shared this with you in the hope that it will inspire you all to have adequate and up to date backup systems in place.

Some questions to ask

Are you taking regular backups?!

Do you have one person responsible for taking backups?

What happens if they are on holiday or off sick?

How often do you review your backup procedure?

If you're doing server backups only, then what consequences are there if one or more staff PCs get hit?

Is your backup system designed for fire or theft (i.e. you lose **everything** from your offices)?

Where are your backups held? Are they secure?

How are the off-site copies transported? (you **are** taking some off-site aren't you?)

Do your backups get done when they should or is it too dependent upon people remembering?

Have you checked whether the system is actually working and that you can get data back from your backups?

How long would it realistically take to get staff back up and running if you lost everything? This includes reloading software as well as the data.

Do you have original CDs and/or registration/license numbers for software?

A definition of backup:

“The duplicate copy of crucial data that no one bothered to make.”

And have you considered **all** of the following types of data?

- Your main Word and Excel files (of course)
- Databases
- Financial systems/data
- Bank records
- Emails
- Your email address book (e.g. Outlook)
- Internet Explorer/Mozilla bookmarks
- Software downloaded from the internet (you'll need registration numbers and/or proof of purchase to reregister)

In the words of a famous song:

“Backing up is hard to do”

Further information

We can provide advice and support for you on backups. Give us a call to discuss what you might need. We may charge for this type of work, but we won't charge for an initial chat.

Here are some articles on backups (some relate specifically to the voluntary sector):

http://www.ictknowledgebase.org.uk/backupstrategy	Developing a Backup Strategy
http://www.ictknowledgebase.org.uk/backingupyourdata	What is the best device to use to back up your data?
www.microsoft.com/protect/yourself/data/storage.mspix	brief overview of types of backup
www.ictknowledgebase.org.uk/onlinebackup	a little out of date (so take any figures with a pinch of salt) but a good overview.
www.lasa.org.uk/circuitriders/crnewsdigest5.pdf	(pages 5 & 6) - more recent article reviewing 5 providers.
http://www.ictknowledgebase.org.uk/disasterpreparation	What would you do if all your computers were stolen, broke down – or were destroyed in a fire? In August 2001, one voluntary organisation in London faced just that when a blaze broke out in their building.

And lots more if you use the search facility (top right) at www.ictknowledgebase.org.uk/ and search for 'backup'

It's generally accepted that the best backup systems require the least user involvement.

Generally we'd advise that you use a combination or solutions that overlap. So perhaps backing up selected (or all) files locally (using CDs, spare PC, external hard drive, tape drives, USB key, etc), taking some off-site and having an automatic on-line backup for selected critical files that runs overnight.

I recently came across www.safedatastorage.co.uk which has a deal for charities (there may be a number that will do a deal for charities).

We use Jungle Disk www.jungledisk.com/ for some of our files.

And there are many things to consider, some of which may not be obvious. For example, while the UK has strict Data Protection laws this only covers data held in the UK. And some on-line data backup services store data across the globe, for example in the US. In this case your data is no longer covered by UK law but by US law (www.ictknowledgebase.org.uk/dataprotectionandweb).

Do call us if you have any questions.