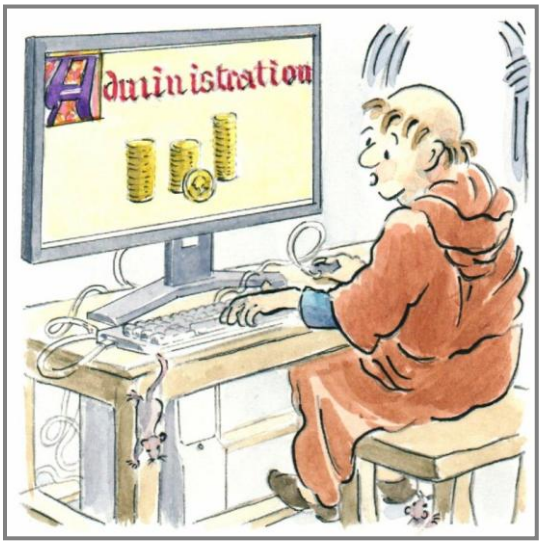
john truscott
church consultant and trainer



A beginner's guide to IT security

TN46 Training Notes series: Administration

We are almost all used to working with a PC/Mac or laptop, a tablet or smartphone, but many of us are only vaguely aware of the security dangers. Here is an easy-to-read, beginners' checklist of where you need protection.

The idea is not to give too much technical detail. The next stage on would be to visit a site such as https://www.getsafeonline.org and read its articles.

It is easy to forget that at the other end of your connection to that big world-wide web sit many nasty spiders that are only too happy to devour your church's data or your personal identity. Other dangers closer to home include fire, theft and your own stupidity. Here are ten actions to take to avoid a disaster.

1 Protect both hardware and files

If your computer contains sensitive information it needs to be both password and physically protected. If you leave the church computer switched on in an unattended office during a lunch-hour, what might a member of the congregation discover if they had a peek? What if there was a break-in? Or if you simply mislaid a back-up memory stick or hard drive?

So consider

- security passwords;
- switching the machine off when not in use;
- locking the office or study;
- all other issues of building and transportation security.

Laptops, memory sticks and DVDs are particularly vulnerable. Be aware too of the terms of the General Data Protection Regulation – GDPR) if you hold information that is covered by this. You may need to follow certain security requirements. Consider too the use of data encryption.

2 Always use a firewall

A 'firewall' is a piece of software that prevents unauthorised access to your computer by a hacker. While you are online it is easy for someone to gain access to your machine to steal personal information, to cause harm, or to use it as an intermediate stage in a wider trail of havoc. A firewall stands between your computer and the internet to block such attempts while allowing other messages that you have authorised to pass in and out. It is a first line of defence, though not enough on its own.

Your Operating System (eg. Windows 10 or 11) has a basic (or 'desktop') firewall (check it is switched on) but you will benefit from a more advanced one:

1 a 'commercial firewall' as part of an anti-virus or security package – see No. 3 below – or a stand-alone (such as is available free from ZoneAlarm);

2 a 'hardware firewall' in your router if you have several pieces of equipment all connected to the internet together.

Anti-virus packages or your 'ISP' (Internet Service Provider) may also offer 'parental control' settings for home computers so that your children can surf the internet safely.

3 Install anti-virus software

You will hear of terms such as 'viruses', 'worms', 'Trojans', 'ransomware'. These usually arrive in an email and any of them can cause havoc inside your computer.

Anti-virus software checks everything coming in (emails, files, etc.) and alerts you at once if it finds a nasty. It will then either sort the problem out or 'quarantine' the file (keeping it safely out of the way). It can also examine what goes out (in your emails) so you don't pass on a problem to others.

Check out some of the common packages available by entering Sophos, Norton (from Symantec), AVG and McAfee into a search engine. Some offer a free option to personal users, others offer a more sophisticated package, perhaps linked with internet security, for a price and an annual payment. But always buy from a trusted source: cheap internet offers may turn out to be anything but anti-virus.

It is essential that you update your protection daily (most packages do this automatically) – and you should set a whole computer scan for once a week too (usually done automatically too). But you still need to treat all emails with caution as your anti-virus package will usually be a few hours out-of-date and nothing is guaranteed to catch everything. See Nos. 7 & 8 below.

4 Back-up your files

A clergy couple I know had both their laptops stolen – and lost all their files that had taken them years to create. Your disaster may be fire, hardware failure, ransomware or simply deleting a key file in error. You may be able to reinstall software. But work files, photographs, address books, emails and internet bookmarks are your own work. You could lose them in an instant.

Hence the need for regular 'back-ups', that is copies kept on memory sticks, external hard drives (keep all in a separate location from your computer) or, increasingly common now, by an external agency in the cloud or as part of your anti-virus package. If your files are kept in the cloud anyway, still have a different back-up. Backing up files

is relatively straightforward, but backing-up emails needs a bit more skill unless you use a cloud-based system such as Office 365 or gmail when it is all done for you.

The danger of ransomware means that back-up is even more important now. If you get infected you are locked out of all your files unless you pay the criminal (never do this) and that can spread to any cloud-based storage too. Best to have a quality anti-virus program and never open suspicious attachments (often purporting to be invoices).

5 Update software and hardware

First, ensure you always have the latest versions of Windows if possible and of Internet Explorer, Firefox, Chrome or whatever browser you use. Then you need to have the latest security updates installed. It is wise to opt for automatic notification of updates. Try to ensure you always have the latest version of all apps. They are safer.

It can also help to use non-Microsoft software which tends to be more robust. For example, instead of Internet Explorer use Firefox from Mozilla or Chrome from Google for free. You do however need Internet Explorer to run some tools so keep it on the desktop. If you are using Mail, then Pegasus Mail or Eudora may be better.

6 Protect against spyware

Some files you download, or links you click, secretly drop the equivalent of a spy-camera into your computer. This then sends back information about the websites you are visiting and sometimes notes how you enter passwords and other confidential information (this is known as 'keystroke logging'). One warning sign is when your computer starts operating much more slowly than usual. Associated with this is 'adware' which displays pop-up advertisements and can change your browser settings.

There is a range of software available to scan your computer and get rid of such things. If you do not have an all-in security package (No. 3 above) try AdAware (from Lavasoft) and Spybot in a search engine. They operate in different ways so it is wise to run both. Another possibility which works in a different way is Prevx.

Run them regularly, perhaps as part of a weekly routine. Like anti-virus software they need regular updating too. But, first of all, avoid dodgy websites and cheap software downloads! A composite security package, such as Norton 360, automatically takes care of everything for you: spyware, anti-virus, identity protection, back-up, etc.

7 Expect fraudulent and hoax emails

Fraudulent emails may well come from people purporting to be Christians. Suspect *any* source you do not know and trust

If you receive an email from a known friend with just a strange weblink within it apart from the greeting, or an attachment purporting to be an invoice, delete it and then go to your Deleted box and delete it permanently. There may be nasties in these.

If you receive an email purporting to come from a bank or PayPal asking for security information such as passwords or memorable information, remember that NO bank will ever ask for this. This is a 'phishing' email designed to lull you into declaring your security information – a new form of identity theft. The latest internet browsers should warn you of dangers here – including spoof sites that look exactly like your own bank.

Be equally suspicious of a look-alike HMRC tax email telling you that you can claim a refund. Check out IBM Trusteer for some help with phishing sites https://www.ibm.com/security/fraud-protection/trusteer.

8 Deal with spam

Spam traffic has decreased in recent years, and most ISPs now remove most of it before it reaches you. But it is still a nuisance and some of it will contain viruses.

Never click on the link to be removed from the spam mailing list (tempting though this is) unless it is a named UK company with a UK address. This simply confirms to the spammer that you really do exist; you may then get more emails rather than less. Never, ever, open an email attachment from any source you do not recognise.

Many ISPs now offer sophisticated spam filters, your email program may sort your incoming mail and use a junk box, and your internet security software may do something similar. There is a wide range of options available for those for whom spam is a problem. Some of them are free. Try, for example, Mailwasher from Firetrust.

9 Understand website and PC security

If you are asked to choose a password, make it long rather than short, with a mixture of digits and letters and special characters (if the site lets you). You should *never* store the details on a file in your computer. Change it the moment you think it has been discovered. Try not to use the same password for multiple accounts on the church computer. You can always have the same basic keystrokes and then something specific for each site. You can use a Password Manager for safety.

Avoid words and numbers that could be guessed – hackers use dictionary attacks with well-known word combinations. Don't use personal names or dates others will know. Be especially wary if logging in to any 'secure' site (eg. one where you type in your credit card number) when you are in the church office or any public place. Disable any option to 'remember your password on this machine'. Make sure no one is watching you as you key in a password (to avoid what is known as 'shoulder surfing').

Always use any 'log off' option when leaving a financial website; never the usual cross in the top right hand corner. Then no-one else with access to your computer can trace your steps. Never leave your computer unattended if on a secure site.

Be very careful about how much personal information you reveal on social networking sites such as Facebook. Never add anything that identifies you, even if others do.

If you are using a secure site, check two things. First that the web-address at the top of your screen has its start labelled https:// (s for 'secure' – most sites now have this anyway), and secondly that there is a padlock symbol, usually to the left of the URL (depending on your browser). The padlock icon may convey additional information.

Take any warnings about site security certificates seriously and, if in doubt, do not accept them.

10 Secure your wireless network

Wi-Fi (or 'wireless') networks are highly vulnerable to eavesdroppers, hackers and freeloaders (who make unauthorised use of your internet connection, known as

'piggybacking'). Assuming you have wireless technology, read the instructions that come with the router. For encryption, always use WPA2. Change the router identifier from the default setting and change the default password (which may come as 'admin'). Ensure every computer on the network has a desktop firewall (see No. 2).

The problem for churches is that as technology gets more sophisticated, making it properly secure starts to become out of the reach of a typical computer user who has little interest in IT as such. Churches should appoint an IT adviser. Choose with care: it might be a member of the congregation who is happy to offer their time free, but it might need to be a commercial company.

Now check out the website listed in the introduction to these notes where you will find further advice and information. It's no bad idea to give yourself time for a check-up on all this once or twice a year. It could save a disaster….

These notes are available at https://www.john-truscott.co.uk/Resources/Training-Notes-index then TN46. See also Article A11, *Become a better emailer,* A14, *Create a quality website* and Training Notes TN99, *Social media+ guidelines.*

John's resources are marked for filing categories of Leadership, Management, Structures, Planning, Communication and Administration. File TN46 under Administration.

John Truscott, 24 High Grove, St Albans, AL3 5SU
Tel: 01727 568325 Email: john@john-truscott.co.uk Web: https://www.john-truscott.co.uk