The United Reformed Church

Help and Advice

Northern Synod Office, 4 College Lane, Newcastle upon Tyne NE1 8JJ (0191-232 1168)

Bulletin 41: INTERNET SECURITY

The Help & Advice Group was set up by Synod in 2009, to support local churches in being informed and effective in their life and mission. The group was disbanded in 2014, as part of a simplification of Synod committees, and its work continues through the Trust Officer, under the oversight of the Trust. We are willing to try to provide specific advice on particular topics. Please get in touch if you have questions or suggestions.

This article is part of a series giving an overview of particular subjects on interest for local churches. We also circulate general updates from time to time. Bulletins will also be posted on the members' area of the website with direct links to other websites.

Where readers are directed to web-based resources, the Synod Office is willing to respond to reasonable requests for printed out information for readers without web access, although they may find it more satisfactory to follow up their interest through their local library's web access.

This bulletin carries two warnings for churches using computers on the Internet.

Computer Security

Anyone using a computer on the Internet is strongly advised to install security software (such as a firewall, anti-virus and anti-malware programmes) to keep them safe online.

Two serious malware threats identified in June 2014 are GameOverZeus and CryptoLocker. **The National Crime Agency recommends all computer users take urgent action to ensure they are protected**.

The Churches Legislation Advisory Service has summarised advice for protecting your computer:

- Run all your Windows updates to make sure you are as up to date as possible: Start > All programs > Windows updates. If your operating system is still Windows XP, Microsoft is no longer issuing updates and your system is at particular risk.
- Ensure you have a recognised anti-virus package, such as Norton, McAfee, Avast or AVG on your system, *and that it is up to date and switched on at all times*.
- Run a full (not quick) virus scan on your machine. Or if you don't have anti-virus software or are not sure whether it is fully up to date, download the free tool from www.getsafeonline.org/nca to scan for GameOverZeus and CryptoLocker and remove them from your computer.
- Do not open suspicious email. GetSafeOnline has guidance on how to identify e-mails from spammers, scammers, phishers and hackers, but malware may be in an

attachment on an e-mail that looks like it is from someone you know or someone else who would plausibly be contacting you.

- *Never open email attachments or click on links in e-mails unless you are absolutely, totally, definitely certain they are authentic*.
- Delete phishing e-mails claiming that a bank account, tax return or anything else requiring a password is compromised and you need to re-enter your details to activate it again – dead obvious, but *someone* must fall for this one, otherwise no-one would bother to send them.
- Change your passwords. Original passwords may already have been compromised by GameOver Zeus. Never store passwords on your computer.
- Back up all your data. Copy everything onto a USB stick or external drive and keep it disconnected from your computer. This way, you have a complete copy of everything should the worst happen.
- Do not rely on Dropbox, SugarSync or other similar cloud-based file sharing solutions to protect your data. They may provide a backup solution, but you may have to e-mail and wait for them to restore your data which may take a few days to do.
- Set up an 'administrator' account on your computer with a strong password and:
    - use the administrator account for making changes to the machine, such as installing software or adding a printer:
    - use a standard account for everyday use.

  The head of the cybersecurity team at the Institution of Engineering and Technology says that by not using the administrator account for browsing the web or accessing emails, computer users can protect themselves from 90% of malware attacks.
- If you don't have an anti-malware program on your machine, install one *and use it regularly*. Malwarebytes is effective and you can get a decent free version: http://tinyurl.com/leela2x

Third Party Use of IT

Some churches may make available computer equipment, or more commonly wireless Internet facilities, to groups hiring their buildings. This can be a valuable added service in that it can enable a conference speaker to use the Internet as part of a presentation, and participants could use the Wi-Fi to check emails and social media in coffee breaks.

However, churches may have a problem if those using the facilities do so for an unlawful purpose, such as breach of copyright or performing rights, or downloading illegal material.

The Churches Legislation Advisory Service recommends adding a term to your hiring agreement if you provide these facilities, requiring hirers to indemnify the church against any claims made against it arising from use of the Internet.

andrew.atkinson@urc-northernsynod.org