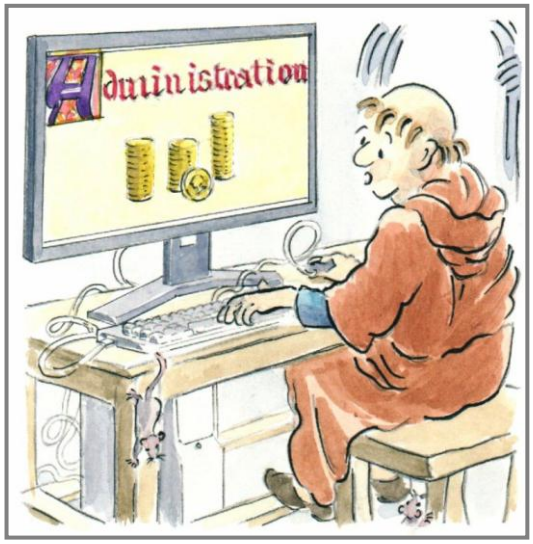
john truscott
church consultant and trainer



Protect your church from scams

TN143 Training Notes series: Administration

In recent months there have been several cases of scammers targeting churches to obtain bank account or personal data. On a wider front the Charity Commission report that one in eight charities experienced cybercrime in 2021.

Some scams are easy to spot but others are becoming more sophisticated. Even well-informed Ministers, staff and church officers can be fooled by a convincing email or telephone call. It may be even easier for well-meaning volunteers, assisting in the church office, keen to help people and unaware of the dangers, to follow fraudulent instructions from someone claiming to be from the church's bank. Anyone idly surfing the net may come across dubious or malicious sites that have been set up for fraudulent purposes.

These notes provide a checklist for church staff and officers to ensure they are aware of the dangers, and as a basis for training all church staff and volunteers who have access to your computer system or have copies of any aspect of it on their own laptops or phones.

1 Some common terms

Cyber security
The broader subject of which these notes form part. All churches with IT systems should have one Trustee with overall responsibility for training and operation within this subject area. Many charities now take this subject very seriously. Most churches have yet to catch up.

Denial of service
A cyber-attack which overloads your computer system to make it unusable.

Fraudulent cold call
An unexpected phone call from someone purporting to be your bank, tax office, internet service provider (ISP) or other agency, with criminal intentions.

Malware
This is short for 'malicious software' such as viruses, worms, keyloggers, trojans or code that can damage computer systems.

Phishing
A message by text, phone, social media but usually email presented to look as though it is coming from a well-known national body (such as a tax office, bank, building society, NHS, school, the government). The aim is to give the receiver a false sense of security so they then hand over personal or bank details.

Ransomware attack
Malware that blocks access to your data or systems until you pay the scammers a large fee – with no guarantee that they will then restore your files.

Scam
Any message you receive where the aim is to deceive you in some way whether in person, by phone or in any digital format.

Danger may come through any of these channels.

- Emails
- Landline or mobile calls
- Text messages
- Websites
- Pop-up windows on some websites
- Response forms on your church website
- Social media (eg. WhatsApp messages)

2 Scam topics

Be on your immediate guard if you receive a message covering any of the following topics.

- Tax or national insurance owed or rebates due for you or your church
- Government benefits available to certain people (eg. Covid related, energy costs)
- Sales of cheap deals for foreign holidays, energy, insurance, new phone, etc.
- Threats about parking fines you have apparently failed to pay
- Any calls from someone in authority such as a police officer or bank official
- Royal Mail or other delivery firms with items for you to collect for a fee
- Warnings of fraudulent activity on your bank accounts
- A need to take money out of a compromised account and hand it to a courier
- Suggestions that your computer is infected with malware
- The sender claims to have taken over your laptop or phone camera
- Dodgy investment opportunities with high returns
- Dating opportunities from new (fake) websites
- Sales of shopping vouchers requiring personal details
- WhatsApp access code requests

- Suspicious financial messages seemingly from your accountant, solicitor or IFA
- Anything where churches have been specially chosen for the offer
- Emotional stories of sick children in a Third World country
- Charity requests for a needy church or school abroad
- A (genuine) friend, son or daughter stuck abroad needing funds to get home
- Callers at the church selling shoddy goods ('Nottingham knockers')
- Anything designed to play on a Christian desire to be kind to those in need

Some of these may of course be genuine but most will be scams. Some will be so ludicrous that they give themselves away. But others may well come across as genuine unless checked out thoroughly. Scam messages aim to put you at ease so that you then give away your own or your church's financial or database details.

3 Clues for scam or fake messages

Here are nine clues to enable you to identify a message you receive as a scam.

1 **An attachment from an unfamiliar source**
Many scam emails may seem innocent enough but will often include an attachment which is where the real danger lies. Never, ever open an attachment from a source you are unfamiliar with, and always ensure a seemingly genuine attachment is checked by your anti-virus program before being opened. A typical example is an email from a finance department or credit control paying your apparent invoice with details attached.

2 **A sense of forced urgency with penalties**
There may be warnings in a text message or email that you only have 24 hours to reply, or an offer that expires tomorrow and needs immediate action. The message may threaten a fine or internet cut-off or even personal arrest if you fail to act on time. The scammer is trying to create a sense of mild panic.

3 **A generic greeting**
This means there is no mention of your name or the name of the church. The message starts, 'Hi' or 'Good afternoon'. There will also be no detail of your account number, or postcode or other specific information. They might mention 'your' ISP rather than name it. This email or text may well have been sent to millions.

4 **A strange URL**
Check where an email has originated from. Watch out for strange groupings of letters or an additional letter added to a national brand name such as 'HSBCE' or 'govx.uk' and beware emails ending .ru or other suffixes you are not used to.

5 **Poor quality text/layout**
If you see misspellings, poor grammar or a strange use of words as if somewhat lost in translation, expect the worst. Be suspicious too of prices in dollars or mention of bitcoins. Many fraudulent messages (but far from all) give themselves away by poor design.

6 **A recorded message**
You receive a recorded announcement by phone, sometimes with an American accent, warning of an infected computer or other problem. They will say they are from your ISP or a major online retailer. This will often be combined with other clues listed here such as a penalty for lack of response.

7 **Any unexpected gain**
If you were not expecting this bank to call you, or a foreign telephone number (starting 00) or the lottery win announcement or investment returns that sound like a dream, or an amazing job offer, be very suspicious. For example, you receive a call, text or email referring to an expensive purchase from a major firm such as Amazon which you know nothing about, telling you to confirm or cancel the order. You of course assume it is a mistake and want to cancel it. But do NOT click the link. Another common example is a PayPal Request Money link to click.

8 **Any request to transfer funds**
This might look like a message from your bank or financial adviser and usually comes as a telephone message warning you that your present account details have been compromised in some way and you need to move everything to a new account without delay. The caller will sound refined and be very convincing, preying on your fears.

9 **Any offer of tech support**
There are fake websites that offer to remove viruses from your computer but are geared to taking personal financial information from you and may well charge you too. Such scams can also come from cold callers and intrusive pop-ups.

Be aware that the opposite of any of these points does not make the communication genuine. Some fraudulent messages have the logo and style of a national institution (bank, HMRC, insurance company, etc.) and look very professional. Others appear to come from a real UK landline number or a genuine firm's email account.

An email or text may describe a real situation for you (a mass mailout is bound to hit the jackpot for some). For example, you know there is likely to be a parcel waiting for you this week but had not appreciated that you had to fill in personal or church details. Or you do have a PayPal or Amazon account you rarely use so a message from them is quite possible.

But most scam or fake communications give themselves away on at least one of the nine points above.

4 What to do if you or your church is scammed

If you are not sure

- For banks and retailers, check your account/orders online (but never using the link just given to you) or contact Customer Services.
- Phone the company (or bank or adviser as appropriate) from your own listing and on a different phone (never on the same phone as the incoming call or using the number they give you) to check if this is genuine or not.

- Google the incoming phone number or email address to see if others have reported similar experiences.
- Call the Citizen's Advice Consumer Service on 0808 223 1133.
- Never trust an innocent-looking number in your caller ID – any scammer can spoof a genuine phone number.

If you suspect a scam

- Do NOT respond to the message or open any links offered.
- Do NOT open any attachment, however curious you are to know more.
- Report immediately to your manager, team leader or Treasurer as relevant.
- Report it within your church staff or equivalent team so others are aware in case the scam goes to them too.
- Report it or forward the email to the fraud department of the real institution if they want to know.
- Delete the email or text message. If this only puts it into a 'Deleted' box, delete it again so that it is no longer on your system.
- Forward scam texts to 7726 or call 0300 123 2040 for Action Fraud.

If you have been compromised

- Take professional advice without delay.
- Report a financial issue to your bank and block your account online.
- Change all relevant passwords: finance-related, retail-related, security-related.
- Report to https://www.actionfraud.police.uk/. Tel 0300 123 2040.
- Report any breach of data to the ICO.
- Run a full system scan of your computer to search for malware.
- Warn people on your contacts list who may have been sent an infected message from your church.

And in general

- Invest in a quality protection system to avoid malware entering your computers (or phones) and run a scan every day.
- Keep this antivirus software current with daily updates and checks on fixed and mobile hard drives.
- Ensure all your data is backed-up in at least two locations (eg. cloud and external hard drive) with strong passwords. One back-up should be disconnected from your system when not in use.
- Ensure staff and volunteers keep their smartphones and laptops safe and secure if they hold church data.

- When buying online ensure the website shows 'https' not just 'http', the padlock sign appears in the heading not the page, and the address bar turns green.
- Offer regular training on the topic of these notes to staff and office volunteers.
- Take part in training from https://www.friendsagainstscams.org.uk.
- See the 'Small charity guide' on the website of the National Cyber Security Centre https://www.ncsc.gov.uk.
- On the same website see how to set up an 'incident response plan'.
- Keep your personal data on online websites up-to-date. Churches may forget to do this when staff change.
- Ensure all your files are password protected with appropriate two-factor authentication systems and encryption.
- Change your router admin and WiFi passwords from the installation ones.
- Use a Password Manager or 'strong' passwords (as long as possible, with a range of symbols, upper and lower case, and no common words).
- Always install operating system updates and software updates so you use the latest versions.
- Install a VPN on your church system so online work is anonymous.
- Conduct an IT safety audit at least once a year with one Trustee and one staff member responsible for all cyber security.

These notes are available at https://www.john-truscott.co.uk/Resources/Training-Notes-index then TN143. See also Training Notes TN46, *A beginner's guide to IT security* and TN53, *A simple email filing system.*

John's resources are marked for filing categories of Leadership, Management, Structures, Planning, Communication and Administration. File TN143 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