Cyber Scams: What to watch out for

There are currently various scams circulating by email, text message or WhatsApp. We want to ensure our community is safe, informed, and able to protect itself. Below is a short guide we've put together to help keep you as safe as possible when dealing with potential online criminality.

The first point to make is that the Right Rev'd Mark Rylands, the Team Rector, or any of the Ashburton and Moorland ministry team or church officers, will NEVER ask you for financial assistance via email, WhatsApp or text message.

Approach with caution!
Please be very cautious when receiving unexpected emails, especially those requesting financial transactions or personal information. Check for grammar or spelling errors, verify sender email addresses (if you click on the name, the email address should appear. If it looks in any way unusual or unfamiliar be extra cautious).

Next, avoid clicking on unfamiliar links, and double-check requests for personal or financial information. If in doubt, contact the alleged sender through a trusted method (for example, by telephone) to confirm the legitimacy of the email.

But what if it looks legitimate?
Even if an email looks legitimate, be wary of urgent or unexpected requests for sensitive information. Verify such requests independently through official channels, like your Churchwarden or the Team Administrator, or, if it's a company, do it directly by checking your account on their official website rather than clicking on links in the email. Legitimate organisations usually won't ask for sensitive information via email.

Look for personalisation:
Legitimate emails often include personal details or information that only you and the sender would know. Be cautious if the email seems generic.

Why should I be suspicious of an email or text message asking for vouchers?
Requests for vouchers in emails, especially unexpected ones, are often a red flag for scams. Scammers use this tactic to trick individuals into providing codes that can be easily redeemed or sold. Legitimate entities typically don't request sensitive information or payments through vouchers via email. Always independently verify such requests before taking any action.

It feels urgent!
Beware of urgent or threatening language: Scammers often create a sense of urgency or use coerce and manipulate recipients. If an email conveys a pressing matter, independently verify it before taking any action.

To summarise:

- Always check the sender's email address – not just the name that appears.
- Watch for mistakes, spelling and grammar.
- Be cautious if the email seems generic.
- Don't click on a link unless you're 100% sure it's safe.
- Protect your information – don't share personal or financial details.
- No rush, no stress: scammers use urgency to trick people – it's okay to ask someone you trust if they think an email is genuine.

Remember, it's always better to be cautious than regretful. If you have doubts about an email or text message's legitimacy, take some time to verify its authenticity through reliable means. Stay safe online!

Further support
If you think you may have been a victim of a church-related scam email or message, please call Chloe Axford, one of our Licensed Lay Ministers: 07889 523776.

You can contact Devon and Cornwall Police Action Fraud team on 0300 123 2040.
There is also helpful guidance here about how to prevent personal fraud: https://www.devon-cornwall.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/prevent-personal-fraud/

If you would like to talk this advice through with someone in person, please call Cassie Long in the church office to arrange for a consultation. Phone number: tel:01364 654280