22.02.2021

St James Church Taunton

Stay safe online

Online Meetings – The Zoom Phenomenon

During the pandemic period many of us have become increasingly accustomed to meeting on line, mainly through the medium of zoom, and we are becoming accustomed to mute button, breakout rooms and online protocols. With more people being involved here are some reminders especially for meeting hosts of general advice

- **Good practice advises not to advertise the meeting ID and Password- send these directly to the participants.**
- **Consider using the waiting room option.**
- **Consider locking the meeting when all participants have joined the meeting.**
- **Know who is in the meeting.**
- **Ensure you do not record the meeting- this is particularly so when meeting with Young people.**
- **If meeting with young people have another leader in the meeting**
- **When recording for online services consider the background and surroundings.**
- **Be mindful of others in the place you are recording**.

General Online safety

We are all using our computers a lot more during this period, to keep in touch, to send on cheery funny messages, to find information, to ensure we can access online services, etc.

This means that all of us are using apps (computer programs) and services with which we are unfamiliar; and more of us with limited technical knowledge are going online.

But the scammers are up to their usual tricks and are coming up with new threats aiming to exploit the current situation.

Keep your wits about you!

- **Always** make sure you have a good computer security system installed on your computer – and keep it updated so you are protected against newly-discovered threats.

- **Never** click on a link if you are unsure who sent it to you - even if you do know the *purported* sender. **STOP**! Take your hands off the mouse and keyboard! Make a cup of tea if you still feel the urge to do something!

  Then hover your mouse over the sender's name and/or the link they want you to click – on a PC a small box will appear showing the real address the link is pointing to. If it's a strange address, just delete the email.

- **Never** forward an email with a reported warning – many of these are hoaxes aimed at causing anxiety. **STOP!** Take your hands off the mouse and keyboard! Make a cup of tea if you still feel the urge to do something!

  Then copy the first few words of the text into a Google search and see what comes up. Ninety-nine times out of a hundred you will see the hoax debunked.

  And/or visit https://www.snopes.com/, which is a fact-checking and debunking service and search there for advice.

  Only if you find nothing from these searches should you consider forwarding the email to a responsible person. Whatever you do, don't broadcast it!

- **Never** give any details to some one purporting to be from your bank.

The same goes for telephone calls. No genuine company will call you wanting you to open up your computer to them. So disbelieve anyone claiming to be from Microsoft, Windows, HMRC, or whoever … and put the phone down – you are not being rude to cut off these criminals without the usual niceties.

Help and Advice

If you are worried by a message you have received call someone you trust, ideally someone with technical knowledge. If you are still in doubt, forward the email to the church office, info@stjamestaunton.co.uk making it clear you are asking for advice, not asking for it to be sent out widely!

Having said all that the internet is a fantastic tool and it is helping to keep us connected at what is a really difficult time – Don't be afraid of it, just **STAY SAFE**