

# Parish Support

## Stay Alert!

*Email scammers are operating in our area. Our Diocesan IT Manager Alison Comlay says:*

It would appear that we are in 'silly season' with regards to potential threats directed at addresses within the [salisbury.anglican.org](http://salisbury.anglican.org) architecture. Myself and ABC Networking have dealt with a fair few this week and I would firstly like to thank those who been vigilant and alerted us to some 'dodgy' looking e-mails. Secondly, I would wish to reassure you that the system is secure and has not been infiltrated.

Our Sophos InterceptX detection software has been working overtime to deal with attempts before they make it to our server however, some particularly sophisticated items have snuck through. One such example purported to come from a couple of the Bishops; the example below shows how on first glance, the address can look genuine but if you take another look you will see that the address isn't quite right:

From: [bishop.salisbury.anglican.org](http://bishop.salisbury.anglican.org)  
To: [alison.comlay@salisbury.anglican.org](mailto:alison.comlay@salisbury.anglican.org)  
Subject: Urgent bank transfer required

The 'from' address is visually ok on first glance, but if you hover over you can see the true address of the sender is [rogueemail@hotmail.com](mailto:rogueemail@hotmail.com). In Outlook you would need to double click the address to see the true address.

These are phishing attempts, usually done to get a conversion going, then request an urgent same day payment!

Please remember that the majority of our e-mail addresses are present in the public domain either via the website or social media etc but may well be produced with a slight variance as per the above example.

Be wary too of clicking on a link within an e-mail which may redirect you to a rogue site.

I would urge you all to remain alert to potential threats and if it looks 'dodgy' then it probably is and should be deleted without any action.