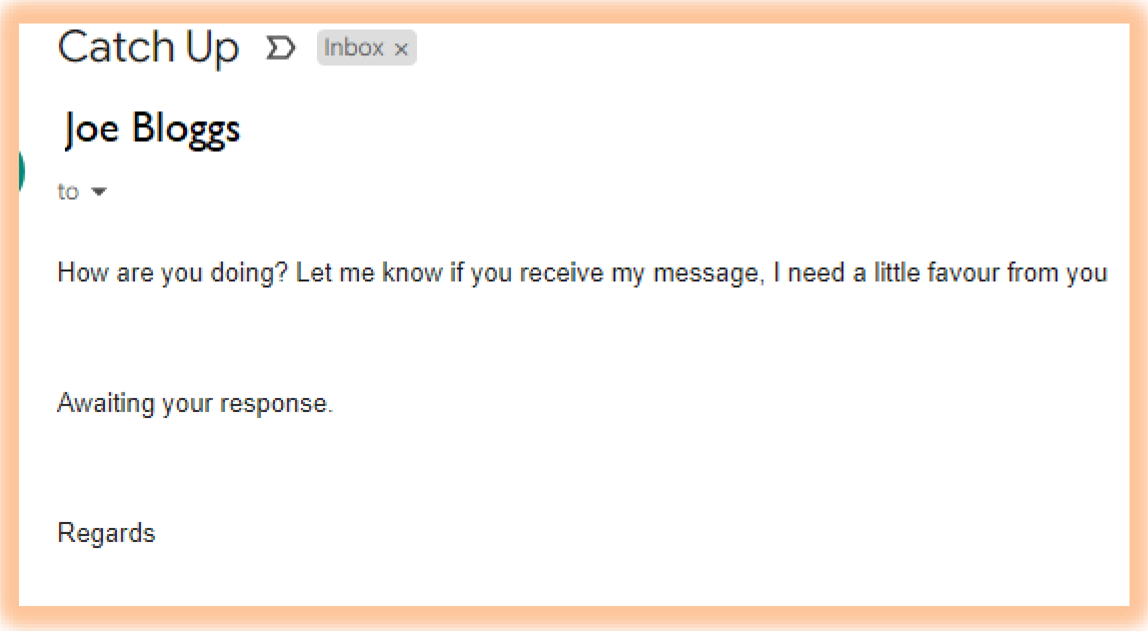
A guide to responsible email.

Version 1.0

30th March 2023

Several of our parishioners have recently received spam email, or had their email accounts compromised. Due to the ever-increasing amount of phishing, scamming and spamming these days, I thought it would be helpful to create a guide outlining how to be avoid being a victim of phishing, scamming and spamming.

This is an example of the spam currently doing the rounds:



Catch Up

Joe Bloggs

to

How are you doing? Let me know if you receive my message, I need a little favour from you

Awaiting your response.

Regards

Note that it does not address the recipient (Joe Bloggs) by name, and there is no name for the sender. This should alert you immediately to the fact that the person who sent the email does not know the identities of anyone in the account, and has just blind copied everyone in the address book with the same message.

Here are some tips that should help protect you.

1 – If possible, try and have 2 different email addresses.

Having 2 email addresses is good policy. You can then keep one email address just for banking and finance, and use a different email for online shopping, newsletters, social media etc.

2 – Never use the same password twice.

For example, if you subscribe to online food shopping, and you create an account with a supermarket, never re-use that password for a different account. Always use a different password when creating accounts.

3 – If an email wording looks strange, it is usually a scam.

If you notice a lot of grammatical mistakes, spelling mistakes, or strange requests for favours, then this is a sure sign of a spam or phishing email.

If the email reads something like the following:

“Help, I need a favour, please email me back”.

Without addressing you by name or adding a name of the sender, then this is a typical scam.

A typical scam going around was the request to purchase “gift cards” for someone in need:

The email starts off, looking like it has come from your friend by spoofing the ‘from’ field to make it look like your friend has sent it.

Contents of the emails will be something like:

“Do you have a few moments? I require your assistance with a minor task. I am available via email”.

There will be no names in the email content, however the “from” field will look like it has come from your friend. It is only after clicking on the “from” name to reveal the actual email address, will you notice that this is **not** the proper email address for your friend.

The email that will be sent if you reply, will be the actual scam, which will be to ask you to purchase a gift card (gift cards cannot be traced, so it is difficult to recover any money lost to scammers this way).

The contents of the scam email will be something like this…

“Okay, sorry for bothering you with this mail, I need to get a Google play gift card for my friend who is down with cancer of the liver, it's her birthday today and I promised to make her happy with this but i can't do it now because I'm currently traveling and i tried purchasing online but unfortunately no luck with that.
Can you please get it from any store around you? I'll refund you upon my arrival. Kindly let me know if you can handle this.”

Never reply to this sort of email (See point 6 for how to check who the real sender is).

4 – Never click on a link in an email, unless you know who the email is from.

If you are unsure of an email, always, always, always double check on the sender’s email address.

It might come as a surprise, but scammers and phishers can spoof an email to make it look like it has come from your friend, but they cannot fake the actual email address.

If the email address of the sender is hidden (e.g. a name is shown, or a simple sentence such as “Congratulations, you’ve won” is shown) click on this name in the “sender” box to reveal the name.

This varies depending on whether you are using Gmail, Hotmail, BT internet, Yahoo etc as your provider and depending on whether you are using a Pc, mac, Android phone or iPhone.

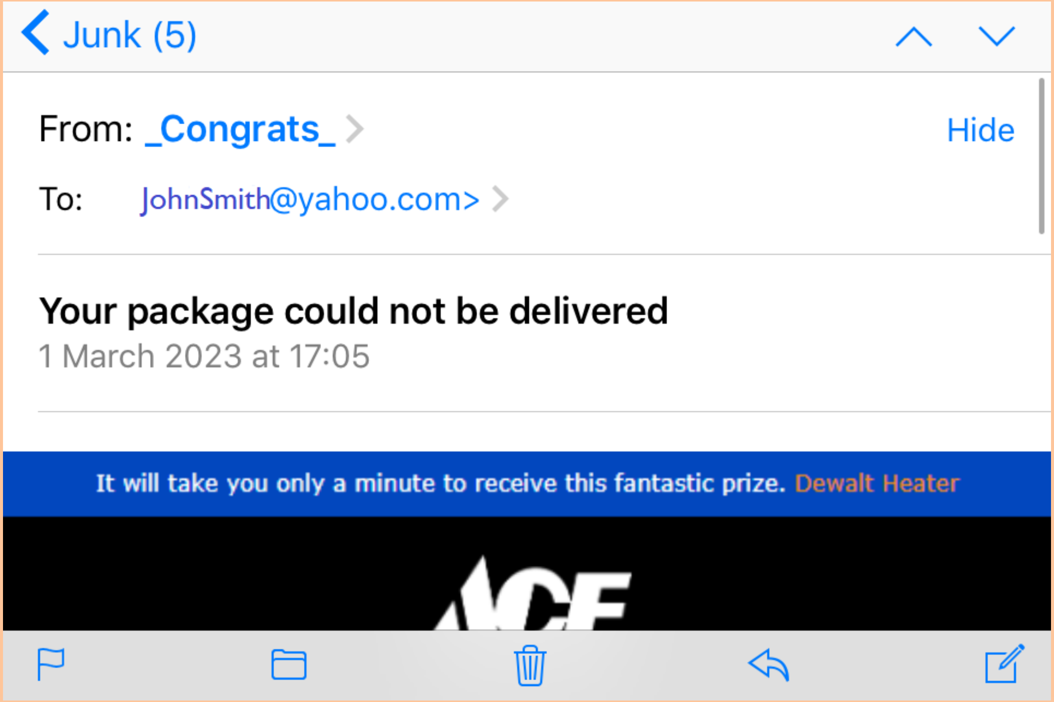
But irrespective of platform always check the actual email address of the sender (See point 6 to see how to reveal the identity of the sender).

5 – Never fall for the ‘undelivered parcel’ scam.

Royal Mail do not charge you to redeliver a parcel, so if you receive an email asking you to pay to have a parcel re-delivered, this is a scam.

If Royal Mail try to deliver a parcel, and you are not in, they either leave with a neighbour, or simply put a postcard through your door, asking you to nominate an alternative date for delivery, and giving you a reference should you wish to collect the parcel in person directly from the Royal Mail depot.

Here is a typical “undelivered parcel” email scam….



From: _Congrats_

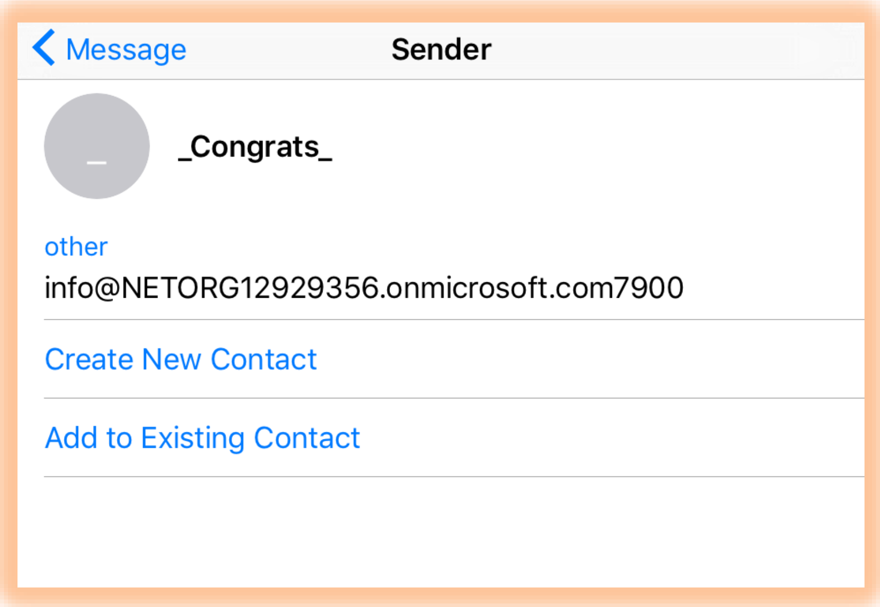
To: JohnSmith@yahoo.com>

Your package could not be delivered
1 March 2023 at 17:05

It will take you only a minute to receive this fantastic prize. Dewalt Heater

This looks strange from the start as this email sent to JohnSmith@yahoo.com shows the from field as someone called “_Congrats_”.

After tapping on this "_Congrats_" name to reveal the actual email address we see the following:



Message

Sender

Congrats

other

info@NETORG12929356.onmicrosoft.com7900

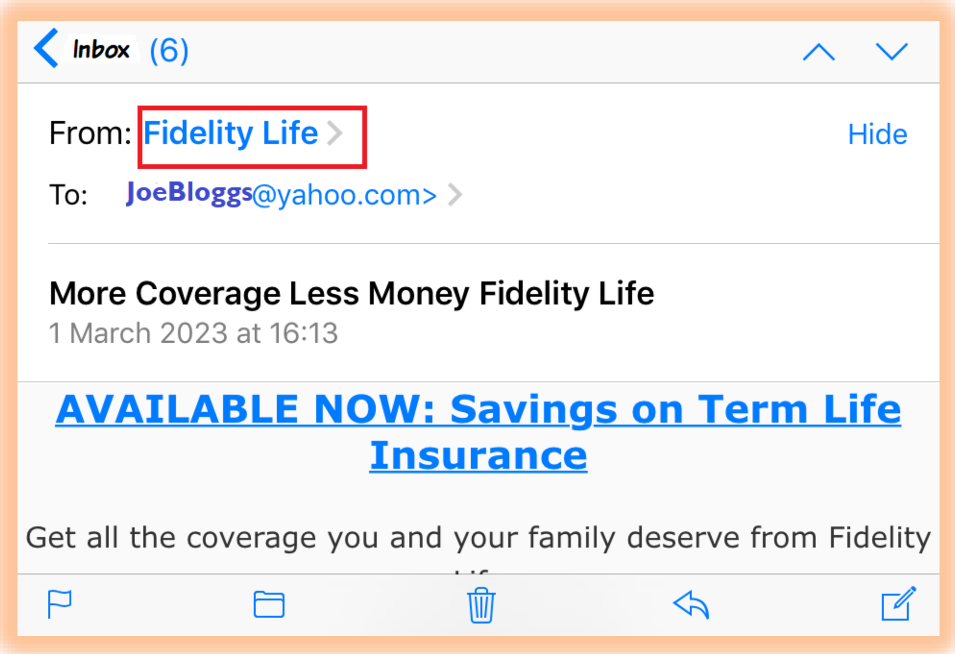
Create New Contact

Add to Existing Contact

Once again, this looks like a very strange email address, so you should mark this email as "spam" so that you do not receive any more emails from this spammer.

6 – How to check email sender address:

Here is a typical scam email from someone pretending to be 'Fidelity Life assurance' sent to a person called JoeBloggs@yahoo.com



Inbox (6)

From: Fidelity Life

Hide

To: JoeBloggs@yahoo.com>

More Coverage Less Money Fidelity Life

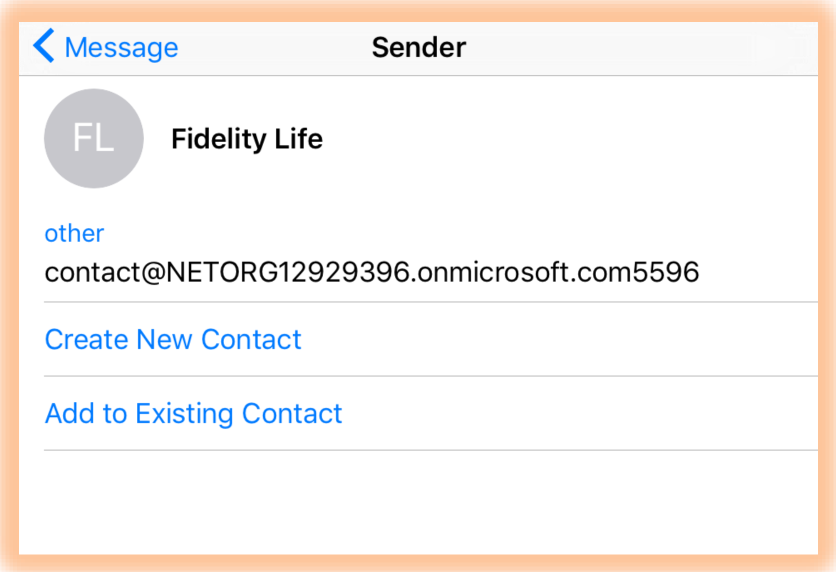
1 March 2023 at 16:13

AVAILABLE NOW: Savings on Term Life Insurance

Get all the coverage you and your family deserve from Fidelity

As you can see, the “From” field looks genuine. It shows “Fidelity Life”.

But when you tap on the “From” field (i.e. tap on the name “Fidelity Life” highlighted in a red box) it shows a very strange email address:



Fidelity Life

other
contact@NETORG12929396.onmicrosoft.com5596

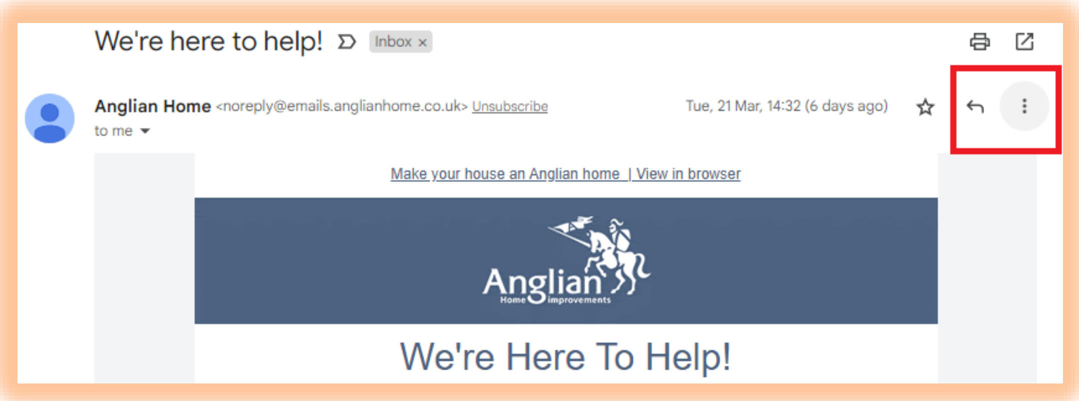
If this was genuine, you would expect it to have an email address from customersupport@fidelitylife.com or some similar email address. Certainly not from the email address in the screenshot above.

7 – How to mark/report emails as Spam or Phishing.

If you do receive an email that you suspect is spam, it is certainly a good idea to “report as spam”, so that your internet provider can trace these emails to the source, and block the sender.

If you are concerned that the email looks like it is dangerous and could affect people financially and is asking for sensitive financial information (something that a genuine bank or building society will never do), then it is a good idea to ‘report as phishing’, so your internet provider can trace this back to the sender.

To do this, usually there will be a mechanism provided by your email account provider to report scams and phishing. For Gmail, you simply click on the 3 dots in the top right hand corner of the email :

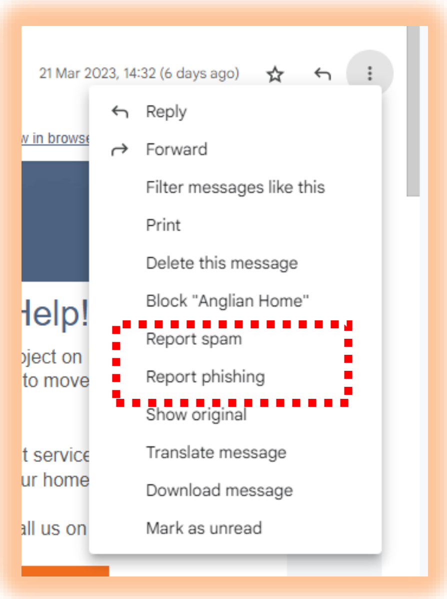

We're here to help!

Anglian Home <noreply@emails.anglianhome.co.uk> Unsubscribe
to me
Tue, 21 Mar, 14:32 (6 days ago)

Make your house an Anglian home | View in browser

We're Here To Help!

This will then pop up a menu with the “report as scam” and “report as phishing” options:



Be careful however to only report emails that you are sure are spam or phishing. You would not want to report a genuine email from your bank or friend as spam or phishing.

8 – Make sure you know the passwords to your accounts.

I have known people who have been using email for so long that they have forgotten their passwords, then have trouble getting back into their account when the password reminder is sent to an old email address or phone, they do not have access to. It is good practise to make sure you can remember all your passwords and have them written down and stored very safely and securely.

If you do forget your passwords, you can always click on the ‘forgotten password’ and the company will usually email you a link to create a new password. However if you have forgotten your main email account password, you won’t be able to log into your email account to receive the password reminder. This is why these days, email accounts usually ask for your other email address, and a phone number so they can send the password reminder that way.

9 – Always use strong passwords.

Most password fields these days only accept strong passwords, so it should come as no surprise that all passwords must contain both Capital and lower-case letters, numbers and some symbols. Never divulge your email passwords to anyone over the phone. Banks will never phone you to ask for your passwords.

10 – Ignore phone calls from people claiming to be customer support department of BT or Microsoft and wanting to “fix” or “improve the speed” of your internet connection.

Although BT genuinely do phone from time to time to offer broadband deals, they will never ask you to turn your computer on and type commands on your computer. Always Ignore requests from people phoning you and claiming to help “speed up your internet connection” or “fix viruses” remotely (I.e. where the person takes control of your PC).

There are lots of phone calls these days from scammers (usually based in India) claiming to be from either BT or Microsoft, and wanting to either “improve the speed of your internet connection” or “fix a virus that they have spotted remotely on their server”.

You should never allow anyone to take control of your PC remotely or type anything on your PC that a stranger tells you to type over the phone. (There are rare exceptions to this rule, where you might be in an office environment and the company has authorised remote access to your computer, but apart from this, do not let a stranger take remote control of your PC over the phone).

This is usually a scam where the person will tell you to navigate to a website, where they can gain control of your PC remotely, and copying the entire contents of your computer onto a remote server thus gaining full access to all your financial documents.

11 Blind Carbon Copy

When emailing long lists of people, it is generally good practise to add the names to a BCC list instead of a CC list. Unless it is vital that everyone should know the names and email addresses of everyone on a copy list a BCC list reduces the risk of spam and phishing. When you place email addresses in the BCC field, those addresses are invisible to the recipients of the email. Thus, if someone on the list is unfortunate enough to have their email account compromised, the other people on the copy list will be safe, as their addresses will be hidden.

[Stephen Hutchinson]