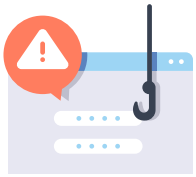
# Be safe, be fraud aware.

DIOCESE OF Hexham & Newcastle

Fraudsters are targeting the Diocese with a variety of Phishing emails. Please use the practical advice below to be fraud aware and protect yourself.

## Be aware of 'phishing' emails



**Phishing with a familiar name as bait:** Phishing emails may look like they're coming from a known person or service

**Do not give in to urgency:** Fraudsters often use a sense of urgency or authority cues that pressure a user to act.

**Be vigilant:** check a senders email address, is this the usual email that they would use to contact you? Or is it an impersonator?

**Hover before you click any links:** Please see the example overleaf on how to check for fraudulent links.

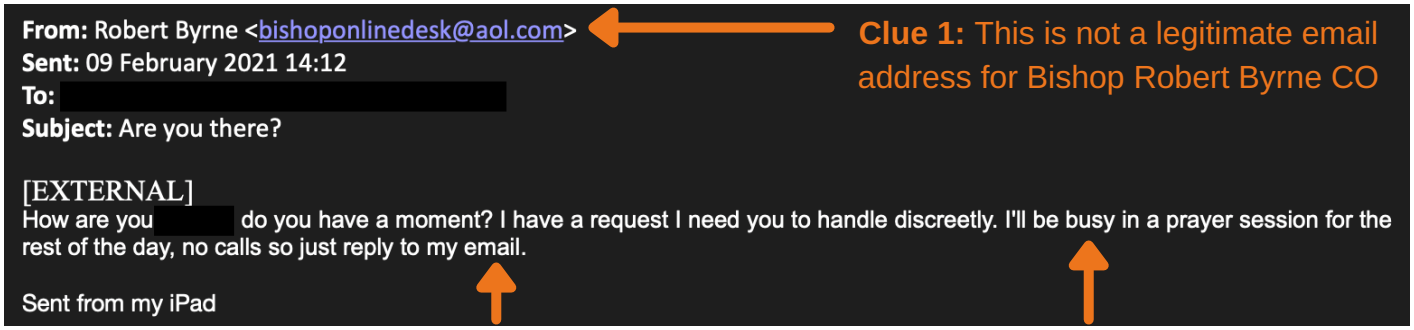
## Beware of 'vishing' phone calls or 'smishing' texts

**Vishing** is when fraudsters obtain personal details of a potential victim by phone. Fraudsters can go on to use this personal information to commit fraud.

**Smishing** is similar to phishing frauds but instead of an email it is via a SMS text message.

To protect yourself from **vishing** or **smishing**, use some of the same techniques you'd use to avoid phishing frauds. Don't give information to anybody unless you are certain you know who you're dealing with, and do not openly click links without knowing you are going to a legitimate source.

## **Example one:** How to avoid taking the bait




**Clue 1:** This is not a legitimate email address for Bishop Robert Byrne CO

**Clue 2:** the sender is using urgency to lure you into acting quickly and irrationally. Take the time to stop and think, and ask yourself, "Does this seem right?".

**Action:** If you receive an email like this then mark it as spam, or block the sender.

## **Example two:** What happens if I reply to an email like this?

If you reply to the first stage of an impersonation email then you will likely receive a follow up request to purchase a gift card or to transfer money. This is another clue as it is an unusual request. At this stage block the sender and report the incident to the Head of Communications who can assist you.

**From:** Robert Byrne <bishoponlinedesk@aol.com>
**Sent:** Tuesday, February 9, 2021 5:44 pm
**To:**
**Subject:** Re: Hi

[EXTERNAL]

Thank you for getting back to me! Here's what I want you to do for me because I'll be busy for the rest of the day. I've been working on incentive and I aimed at surprising some of our diligent staff and members with vouchers this week. I want to handle this personally and it should remain confidential until they all have the vouchers as it's a surprise.
I need you to get 10 qty of Amazon voucher £100 value on each ( total £1000 ). You should get them at any store around. After you get them, scratch the back to reveal the voucher codes and take a clear picture of each card and send each picture separately to me here, So I can easily assign them to the individual's email. Please keep the physical cards and receipt for reference. You will be duly reimbursed by the church for this.
Can you get this done?

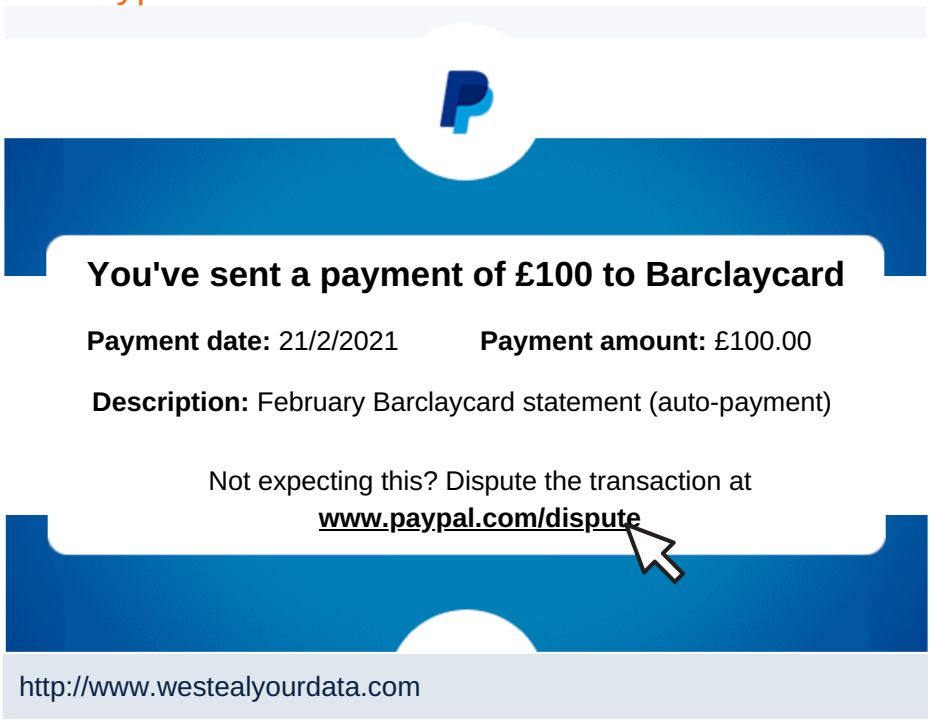
Blessings

Sent from my iPad

## **Example three:** How to spot fake hyperlinks

The example on the right illustrates how a hyperlink can be **masked** to look like it has come from a legitimate source.

The best practice before clicking any hyperlink is to **'link hover'** eg. hover your cursor over the link to show its true destination. For example the PayPal dispute link opposite is actually a fake website that could be used to capture your data. Why not try this out now by hovering your cursor over the link, and don't worry the website is not real!




## Are you still unsure? Let's talk

If you have received an email that you are unsure about then please do not hesitate to contact Iain Riddell, Head of Communications for further advice.

07508738296

head.communications@rcdhn.org.uk