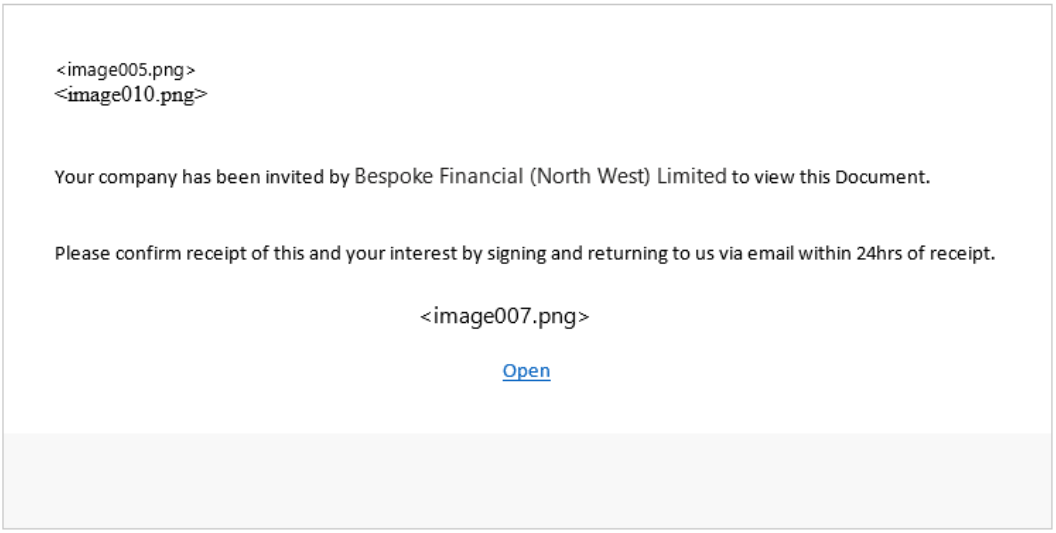
Information security: Phishing Alert

We have been made aware of a malicious e-mail going around claiming to be from Bespoke Financial (North West), a firm which has no links to PRIMIS, **this is a phishing e-mail and should be discarded**. Please **do not click** on any links within it etc.

An example of the email is below:



As with any form of phishing take some basic measures:

Secure your online Accounts
Two-factor authentication is one of the easiest and most effective ways to increase the security of your business. It's easier than it sounds - when you log in you'll type a code from your phone to get access to Office 365. This can prevent hackers from taking over if they know your password. Individuals can add Two-factor authentication to most accounts easily and without cost. This **guide for Office 365** explains how.

Don't click on links
Any link in any email is inherently dangerous. If a customer, vendor, supplier - or anyone, for that matter - sends you a link, do not click on it unless you were explicitly expecting it and it's from a known source. If the link is to a website, do not use the link to navigate to that website. Open up your browser and manually navigate to the website by typing its name into the address bar.

Don't give away your credentials
The only time you should enter your email address, password, account information or credit card number online is if you navigate directly to a website and login. NEVER email or message your information to someone. NEVER enter information on a website that you've linked to through an email.

Beware the "Urgent Action"
Look out for emails that convey a sense of urgency, fraudsters often rely on victims clicking before having thoroughly thought about the situation. Attackers will often try to drive an emotional reaction, using fear tactics, urgent language, and offers that seem too good to be true.

Educate employees
Whilst technical solutions can prevent significant amounts of spam and email-based threats, phishing attacks are becoming more sophisticated to try and circumvent perimeter controls. Employees remain a valuable last line of defence against data loss and cyber-crime. Ensure your employees are trained and aware of the risk that phishing poses. Consider using a simulated phishing service or exercise to gauge their response to a real attack.

If you believe that you may have been a victim of a phishing attack then report the incident immediately to your IT team/specialist.