

ALERT: Email Phishing

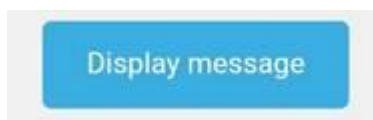
We have received reports that some of our parents have received suspicious emails from what appears to be a Helsby High School email addresses. We are investigating this; however, we believe these emails may appear to be about legitimate topics that we would contact you about. However, the emails may ask for password details or contain links or a 'button' to click on'.

We are sending this email out to inform you of this as soon as we can - and to urge you to be extremely vigilant about any emails you may receive from Helsby High School. If you are in any doubt about its legitimacy, please do not follow those instructions and report it to us as soon as possible (ictsupport@helsbyhigh.org.uk).

For avoidance of doubt we will never send you an email asking you for your password details or to provide personal information, or to click on links to take action, receive or display information.

What could the phishing email look like?

The email could be unique to the recipient, with different senders each time, and its title may relate to something like a report, school qualifications and subject, GCSE/A Level, or anything else related. There is generally no other text in the email, other than a blue link button, saying 'Display message' or something similar.



Do not click on any links or open any unexpected attachments. If you think you have received this email or another suspected phishing email, or if you are concerned you have clicked on a suspicious link, please report it to us immediately.

We will continue to keep you updated on this as we learn more information. As you know phishing and cyber crime is a real and present issue in our lives today and we all need to be aware and vigilant.

Top tips for spotting a phishing email:

- The email contains strange attachments or links
- The email contains links to unrecognised sites or URLs that misspell a familiar domain name
- A sense of urgency in the subject line or message
- The email contains poor spelling and grammar
- Personal information, urgent payment or a change to payment details is requested
- The email is addressed generically, as opposed to you personally
- Altered email address (i.e. sally@paypal.com > sally@paypal23.com)