Watch out for phish!

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal your details to sell or perhaps to access your organisation's information.

Reducing phishing emails needs to happen at different levels – we've got guidance for IT teams on our website - but all users should follow these guidelines:

- **'If in doubt, call it out'.** Always ask for advice if you're not sure if the link or email is legitimate.
- Don't feel silly if you think you have been caught out: it happens to all of us from time to time. But **do report this** to your Head Teacher or IT team so they can minimise any damage

Phishing flags

- **Some phishing emails are more sophisticated than others, but it helps to be aware of some of the more obvious clues. These include:**
- **Does it contain poor quality images of logos?**
- **Are there spelling or grammatical errors?**
- **Does it address you as 'dear friend' rather than by name?**
- **Is it asking you to act urgently?**
- **Does it refer to a previous message you don't remember seeing**