Phishing advice to schools

Over and above the safeguarding measures in place on the ENNI network within your school users also have their part to play in helping protect against a phishing attack from spam, spoofed and ransom emails.

Steps to protect yourself at home and at school:

- Be sensible and smart whilst browsing online and checking your emails
- NEVER click on links in an email to a website unless you are 100% certain it is authentic
- Be wary of emails asking for confidential information especially if it requests banking details or personal information. Legitimate companies and banks will NEVER request personal/sensitive information via email.
- Be cautious of shortened links both on websites and emails. As a way of checking place your mouse over the web link to ensure where the link is directing you to is what is referenced in the email.
- Phishing emails will generally have an impersonal greeting like “Dear Customer” and have lots of typos, exclamation marks and words typed in capital letters. Treat any email like this with caution.
- Be suspicious of emails containing threats and urgent deadlines. If you are concerned contact the company/person separately via your own contact details listed for them preferably via a phone number you have listed for them.
- Be wary opening any MHT (MIME HTML web Archive) attachments within emails
- Never use unsecured Wi-Fi for shopping, banking or entering personal information.
- Have different passwords for all accounts and ensure they are STRONG UNIQUE passwords changed at regular intervals.
- If accessing school work/emails on a home device ensure there is some form of Anti-Virus and end point security on the device and that all relevant security patches for the operating systems are up to date.