2TELA

Understanding Phishing

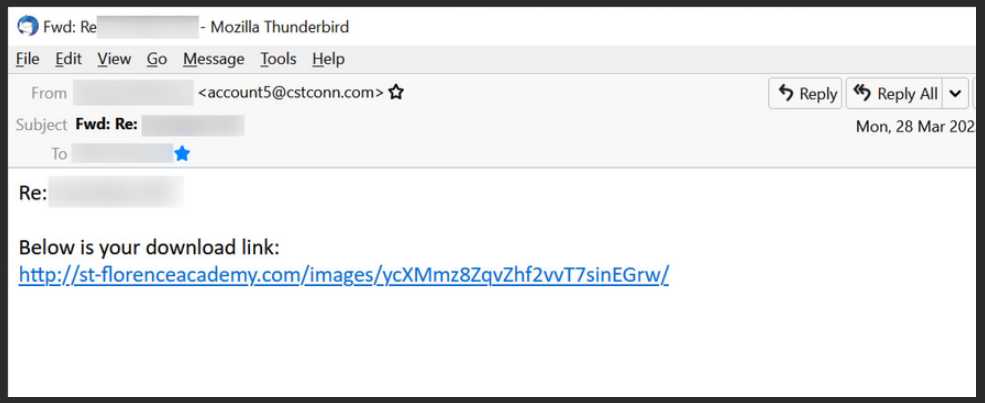
The three most common types of phishing emails targeting UK businesses and how to spot them

1. Phishing that contain malware that leads to ransomware attacks
2. Phishing that steals login details to attack your clients
3. Phishing that harvests banking information to steal your money

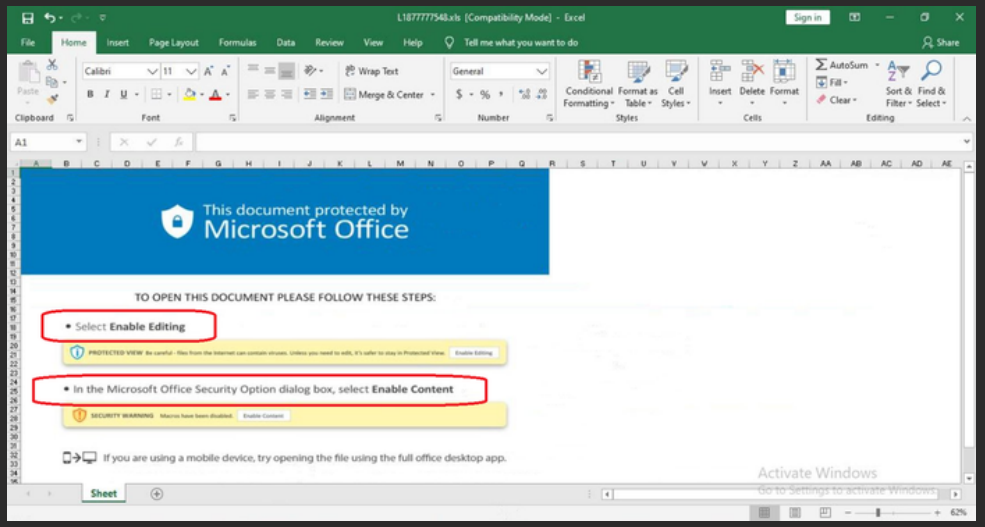
2TELA

1

Phishing email will be generic in nature sometimes financially themed or just bland content linking to an attachment & document



Document will often be Excel and will ask you to 'Enable Editing' and 'Enable Content' - highlighted here in red

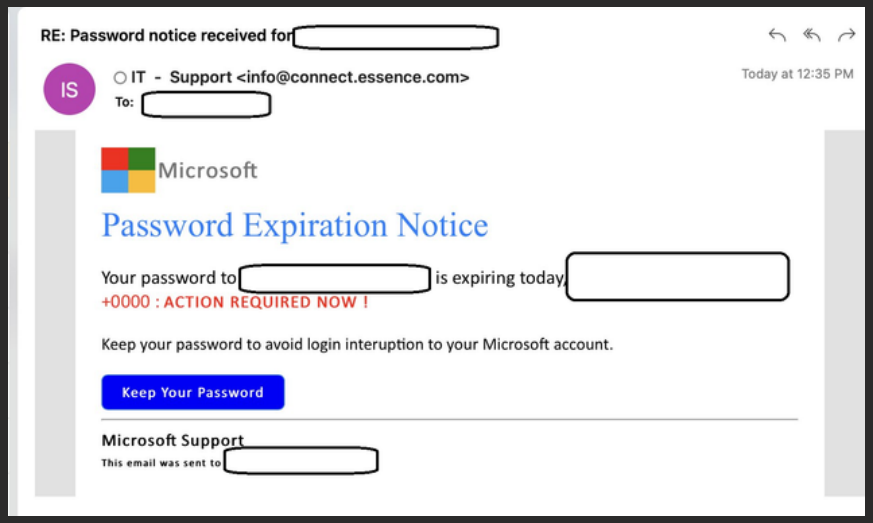


DO NOT 'ENABLE EDITING' OR 'ENABLE CONTENT' ON ANY MICROSOFT DOCUMENTS RECEIVED BY EMAIL

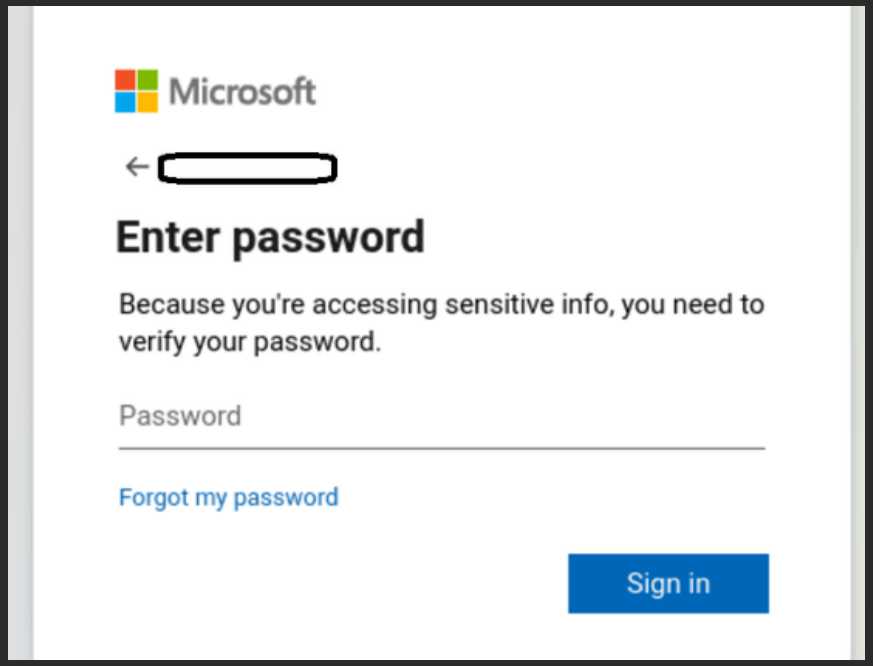
2TELA

2

Phishing email will be generic but require you to view a document or will be related to your Microsoft account such as updating a password



Once the link or document is opened it will open a genuine-looking but malicious Microsoft login portal

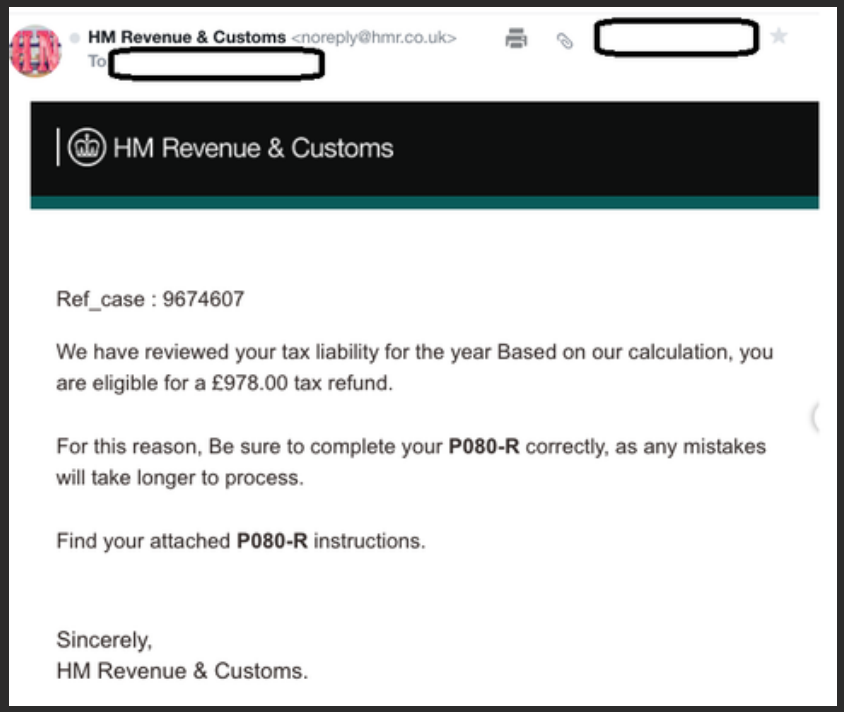


DO NOT ENTER YOUR MICROSOFT LOGIN DETAILS ON ANY PORTAL WHICH OPENS FROM A DOCUMENT OR LINK IN AN EMAIL

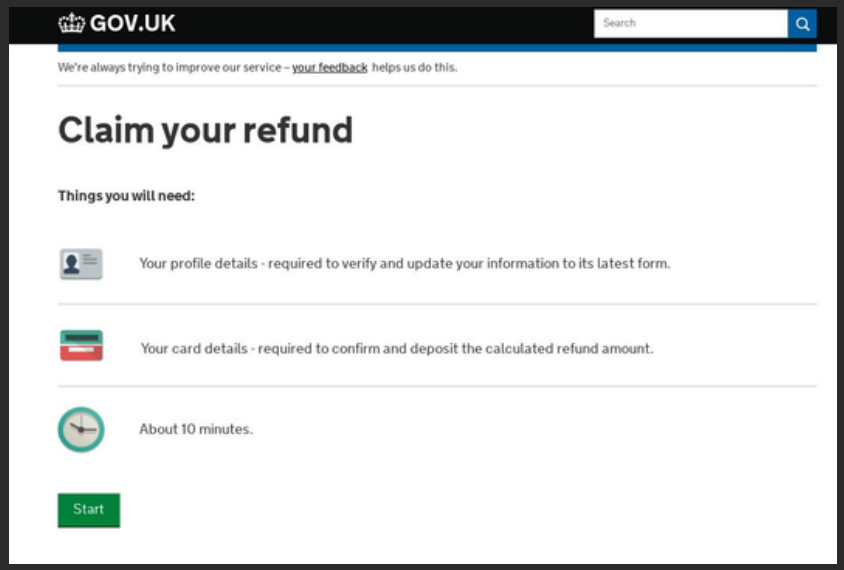
2TELA

3

Phishing email will be UK relevant - either HMRC or NHS or possibly a UK bank - & will be financially themed - offering money or requesting payment



Link or attachment in email will take you to a page where it will ask for banking details, often asking for personal details first



DO NOT ENTER ANY PERSONAL OR BANKING INFORMATION IN UNEXPECTED EMAILS FROM HMRC, NHS OR BANKS

2TELA

If you receive a suspected phishing email:

- Do not open the email or click on any links or attachments
- Do not Enable Editing or Enable Content on any documents
- Do not forward on the email
- Speak to your IT Helpdesk for further assistance OR
- Email hello@2tela.co.uk for further assistance

Credits:
Cryptolaemus (@Cryptolaemus1)
proxylife (@pr0xylife)
ps66uk (@ps66uk)
Craig Iskowitz (@craigiskowitz)
Ady Stokes (@A11y_Ady)
B3rt0 (@rpsanch)