Phishing Refresher - Red Flag Phishing Email Observations (Real Phishing Example from Today – "Think before you click")

Due to geopolitical issues & phishing being the highest security risk to the organisation, below is a recent real phishing example to assist staff identifying phishing "red flags" of a compromised email account and the different phishing webpage stages.

Please Note: Phishing comes in many different variations of the example below:

1. Phishing emails can start from a compromised email account (friend or associate) sending ad-hoc emails to gain trust and entice users to click on a link. Compromised email accounts regularly use file sharing applications via Dropbox, we-transfer, SharePoint, etc. Thanks to the CGD staff reporting the phishing email below this morning, phishing emails were removed from 20 email accounts. Reporting phishing emails early helps all staff in the organisation, you never know how many staff have been affected by the same email.
   Red Flags – Adhoc emails, irregular details with phishing links

   Phishing Email Greeting Example

   Good Morning,

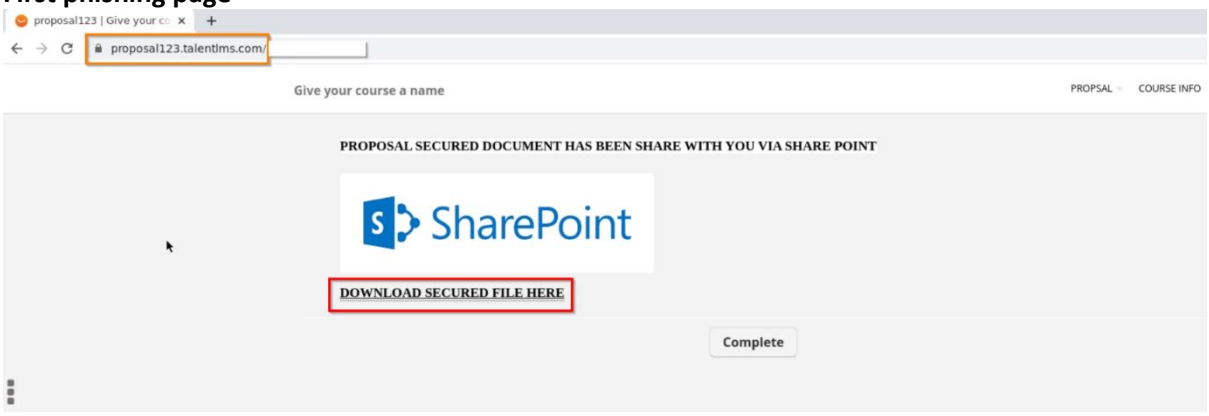
   Please finds the attached document below, If you have any questions, please email me.

   SharePoint

   2 - attachments
   View all attachments | Save to Drive

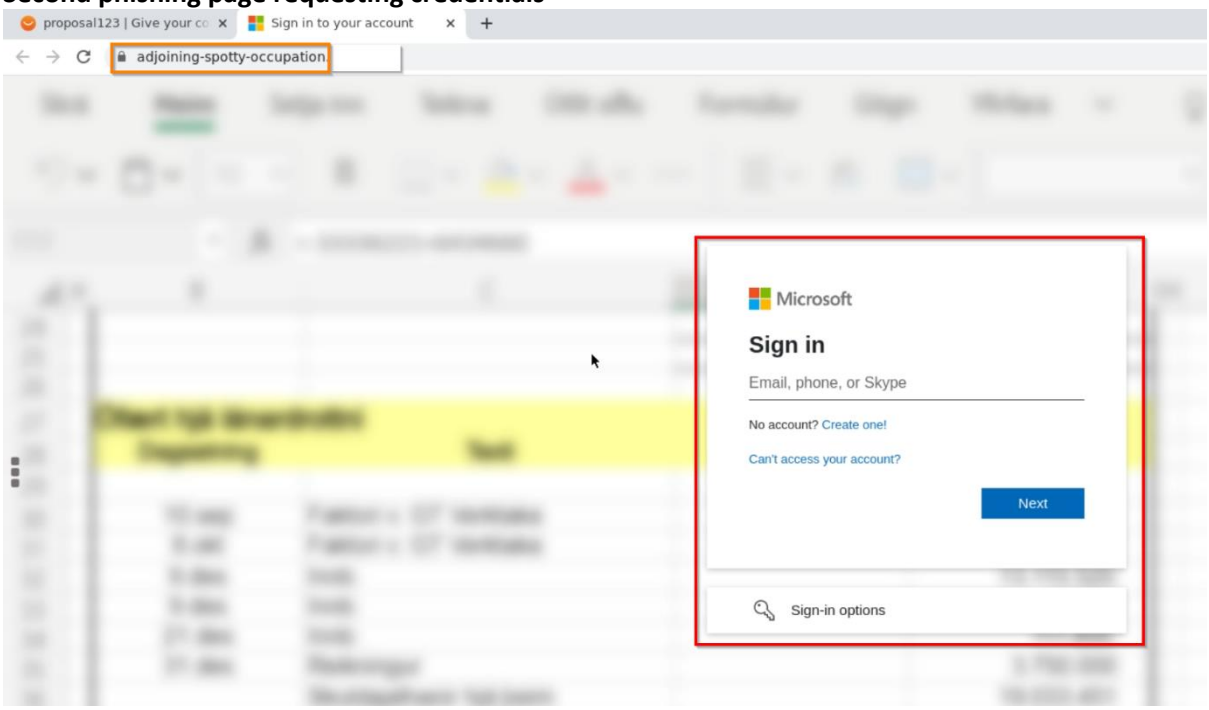
2. Once the link is clicked the user is taken to a fake webpage (please contact the IT servicedesk if you accidently click on the link).
   Red Flags – The web address has nothing to do with Sharepoint and contains the download link refers to a non Microsoft site (use the mouse hover to review website address).

First phishing page



3. When a user initiates the 'download' by clicking on the link in the previous step, the following prompt appears with a login prompt. Red Flags - the address in the address bar and that the **Background** image does not contain CGD logo.

Second phishing page requesting credentials



4. If login credentials are entered into the prompt the cyber criminals have access to your login and password. That will enable them to send you unprompted Multi Factor Authentication (MFA) requests to your phone**. Please report to CGD IT immediately and change password.** A common technique for malicious actors is to push hundreds of unauthorised MFA alerts to force the user to authorise due to the "MFA prompt frustration".

5. If you would like further phishing information, please refer to the source - https://thesource.greaterdandenong.vic.gov.au/information-technology-services-it/security-awareness and feel free to book a phishing training session refresher.