



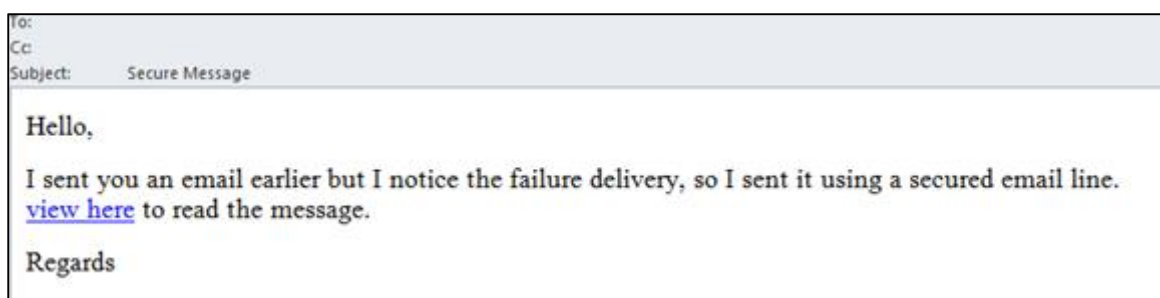
Spearphishing campaign targeting multiple government departments

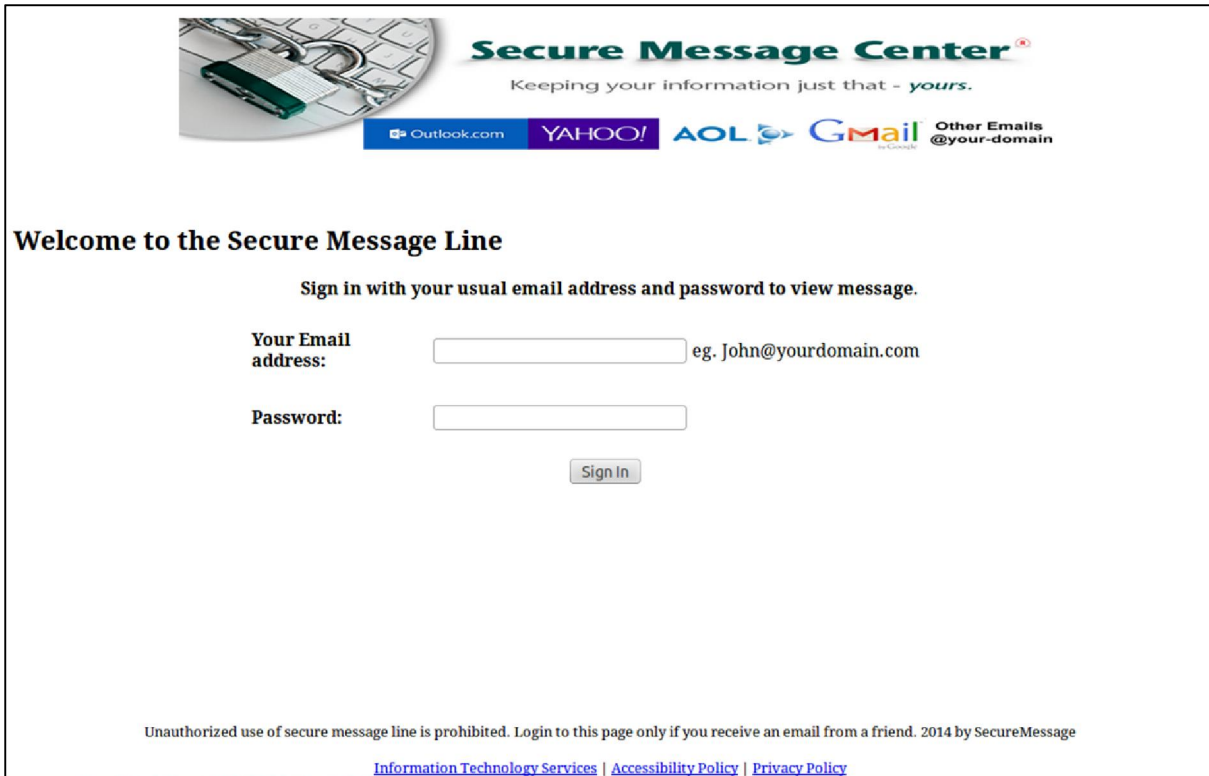
Outline

The NCSC is aware of a current spearphishing campaign targeting a wide number of government sector employees. To the recipient, the spearphishing email appears to be sent from a legitimate but spoofed (i.e. using a forged sender address) email address. The NCSC recommends all government IT Security Managers advise employees not to follow the hyperlink contained in the body of the spearphishing email.

The spearphishing email explains that a (fictitious) earlier email was sent to the recipient, but that the delivery had failed. The email requests that the recipient follow a hyperlink to view the email. If the recipient clicks on the link, they will be taken to a webpage that requests the recipient enter their email address and password. If the details are entered, the malicious actor responsible for the spearphishing campaign will gain full access to the recipients email account.

An example of the spearphishing email and the corresponding webpage that a recipient will be diverted to is attached below.





The image shows a screenshot of the Secure Message Center login page. At the top left is a graphic of a keyboard with a padlock. To its right is the text "Secure Message Center" with a registered trademark symbol, followed by the tagline "Keeping your information just that - yours." Below this are logos for Outlook.com, YAHOO!, AOL, Gmail, and "Other Emails @your-domain". The main heading is "Welcome to the Secure Message Line". Below it is the instruction "Sign in with your usual email address and password to view message." There are two input fields: "Your Email address:" with a text box and the example "eg. John@yourdomain.com", and "Password:" with a text box. A "Sign In" button is centered below the password field. At the bottom, there is a disclaimer: "Unauthorized use of secure message line is prohibited. Login to this page only if you receive an email from a friend. 2014 by SecureMessage" and three links: "Information Technology Services", "Accessibility Policy", and "Privacy Policy".

Mitigations

Please advise all employees not to reply to the email, not to follow the link and/or enter any details in the corresponding webpage. If an employee has previously entered their details then they are advised to contact their IT Security Team immediately. We would appreciate the IT Security Teams reporting any suspected activity related to the spearphishing campaign to the NCSC via phone, +64 4 498 7654, or our incidents email address, incidents@ncsc.govt.nz.