HOW TO IDENTIFY A SPEAR PHISHING EMAIL

A 5 STEP TIPSHEET

CHECK SENDER EMAIL ADDRESS

Often when people receive an email they will only look at the display name i.e. Bill Gates, and not probe further to look at the email address (Bill_Gates@M1cros0ft.com). This is especially true when the display is one that is recognised. If an email or request looks unusual, the first port of call is to check the email address is correct and matches the display name.

EVALUATE THE EMAIL FORMAT

Some attackers may use more sophisticated techniques and spoof not only the display name, but the email address itself too. In these cases, you should be wary of any indications that the format of the email looks unusual. Does the spacing look strange? Are logos displaying correctly in the sender's signature? Does the email contain typos or spelling mistakes?

EVALUATE THE CONTENT

If the email has come from a sender you communicate with frequently, does the tone match their usual emails? Is the request normal or out of the blue? If it's a communication from an organisation, are they requesting you to act immediately? Financial institutions or other organisations with PCI data will contact you via phone with urgent requests and communicate through email.

VALIDATE URLs

Sometimes attackers may use links in their emails to hijack web browsers or direct receivers to fraudulent websites attempting to gain credentials. By hovering over links in an email you are able to see the complete address. If the address looks suspicious then the link should not be clicked on.

PHONE THE SENDER

If the sender is known to you but their request looks unusual, phone them to confirm the email is legitimate. It is much better to be safe than sorry, and if the request is urgent and valid it's likely the sender will answer straight away.

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust