Cyber @ ANZ Internship

Social Engineering Investigation

Submitted by: Valency Colaco, Masters of Information Technology, University of Sydney

Email 1:

Is this email Safe or Malicious?	My Analysis
Safe	The mail is in the inbox and not in spam, meaning it passed Gmail's SPF, DKIM and DMARC domain authentication checks (this indicates that the mail was sent from a gmail account and wasn't spoofed).

Email 2:

Is this email Safe or Malicious?	My Analysis
Malicious	OneDrive is owned by the Microsoft Corporation, USA. The email address used has a .ru extension that points to RUSSIA. Also, there are a ton of grammatical errors in the email – Mistakes that Microsoft would not make.

Email 3:

Is this email Safe or Malicious?	My Analysis
Malicious	The link in the email doesn't point to Facebook.com, it points to a faceβook.com.opt which is NOT the real Facebook.

Email 4:

Is this email Safe or Malicious?	My Analysis
Safe	The email passed Google's Strict Domain Authentication Checks as it is in the inbox and not in spam. The above tests also show that the email wasn't spoofed.

Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	Classic Scam from the 90s. Also, Government Officials don't call, text or email. They either show up at your doorstep or send a letter summoning you.

Email 6:

Is this email Safe or Malicious?	My Analysis
Safe	No Malicious Links, No request for sensitive information, Domain (@anz.com) looks genuine and not spoofed

Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	Even though the URL has been defanged, the link could point to a malicious site if the user manually copies the link and replaces the "hxxp" with "http"