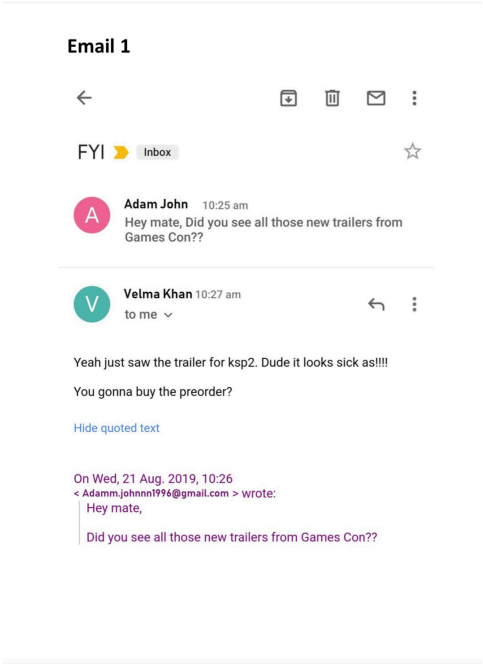
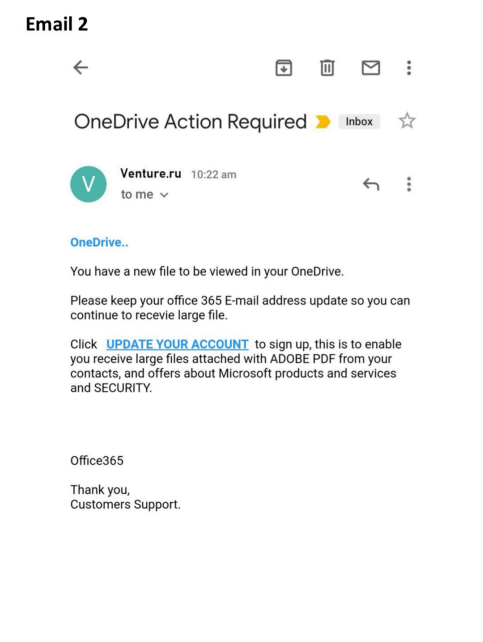


Email Analysis



- Safe

- Tone is casual and conversational
- No suspicious URLs
- No unusual or urgent requests
- No grammatical manipulation or false branding
- Message is typical of friendly tone between friends about gaming



-Malicious

- “Venture.ru” is not official Microsoft domain
- Official Microsoft emails come from domains like @microsoft.com or similar
- Also, there is some emergency to click on the link

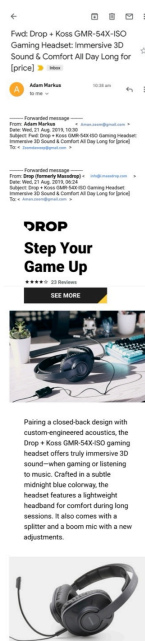
Email 3



-Malicious

- The link is fake because it appears to be Facebook URL but uses a fake domain name (special letter “b”)
- Also there is urgency to click on the link which could steal login credentials

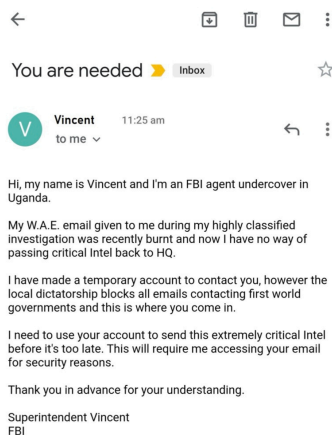
Email 4



-Safe

- It is a legitimate promotional email about headset
- The message if forwarded and consistent with normal marketing, referral communication
- Emails are also appears to be valid
- Also there is no request for personal information, suspicious links, or urgent action

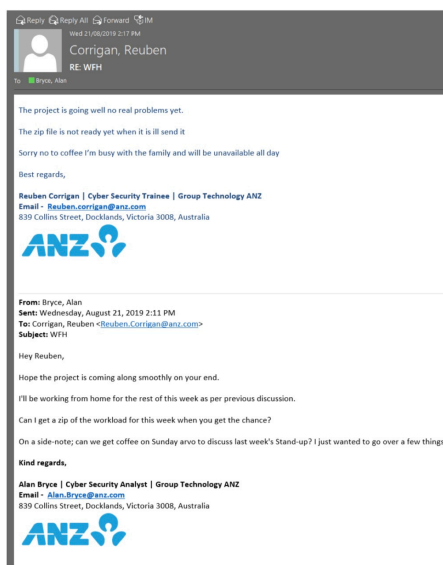
Email 5



-Malicious

- This is social engineering scam
- No real agency would request access to your personal account
- It uses a dramatic story to pressurise which is highly common in scams

Email 6



-Safe

- It appears to be genuine internal communication between two employees of ANZ

- Consistent formatting, no suspicious links or attachments
- There is also no urgency tactics
- This appears to be normal workplace conversation



-Malicious

- Highly suspicious sender name.
- Phishing-like subject to lure the reader.
- Link is suspicious because domain name is not affiliated with Geico and the path is suspicious and irrelevant to the message.
- No company branding
- No legal disclaimers