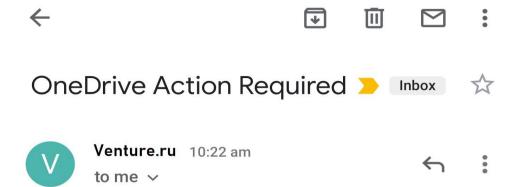


Email 1:

Is this email Safe or Malicious?	My Analysis
Safe	This is the normal email conversation between two
	friends.



OneDrive..

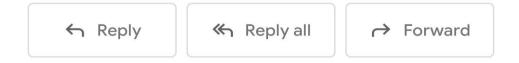
You have a new file to be viewed in your OneDrive.

Please keep your office 365 E-mail address update so you can continue to recevie large file.

Click <u>UPDATE YOUR ACCOUNT</u> to sign up, this is to enable you receive large files attached with ADOBE PDF from your contacts, and offers about Microsoft products and services and SECURITY.

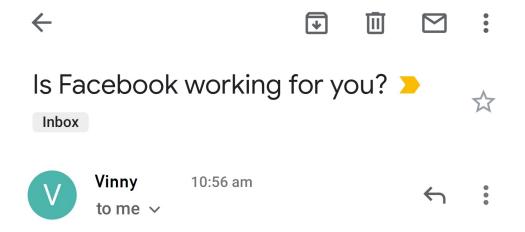
Office365

Thank you, Customers Support.



Email 2:

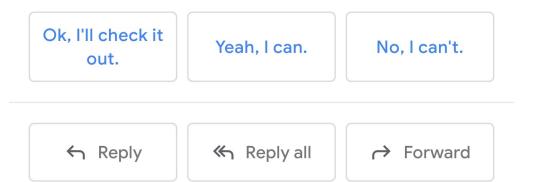
Is this email Safe or Malicious?	My Analysis
Malicious	 The sender's email address is considered malicious. Office 365 and OneDrive are both the products of Microsoft Company, so their email address must contain domain names and subdomain names such as micicrosoft.com, mail.support.microsoft.com, or microsoftsupport.com. However, the support email is from Venture .ru, which is not legitimate. OneDrive is personal cloud storage, and Office 365 does not contain Software to manage the Microsoft Email. Outlook is the software from Microsoft used to manage all Client emails, which is not mentioned in the Email body for updating. Therefore, the adversary tries masquerading as a legitimate email to gain TRUST from the victim. The opening of the email should be Hi, Hello, or Dear. The email has poor typos like Customers, and "products and services and Security". Vendors would not update products and services via email. According to all evidence, this email is treated as malicious email.



Hey I think Facebook is down, I can't log in at all no matter what.

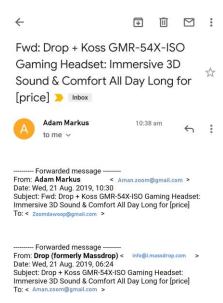
Can you try? https://www.faceßook.com.opt/login.htm

Thanks, Vinny



Email 3:

Is this email Safe or Malicious?	My Analysis
Malicious	The DN of Facebook must be www.facebook.com not hxxps[://]www[.]facebook[.]com[.]opt/login[.]htm. The adversary uses the familiarity for the attack to trick the user into clicking on the malicious link for harvesting credentials.



Step Your Game Up

★★★☆ 23 Reviews

SEE MORE

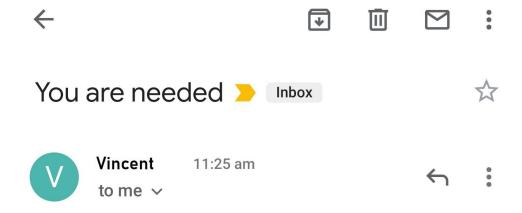


Pairing a closed-back design with custom-engineered acoustics, the Drop + Koss GMR-54X-ISO gaming headset offers truly immersive 3D sound—when gaming or listening to music. Crafted in a subtle midnight blue colorway, the headset features a lightweight headband for comfort during long sessions. It also comes with a splitter and a boom mic with a new adjustments.



Email 4:

Is this email Safe or Malicious?	My Analysis
Malicious	This is a malicious email because the legitimate email of
	Drop company must be drop.com which is not
	masdrop.com.



Hi, my name is Vincent and I'm an FBI agent undercover in Uganda.

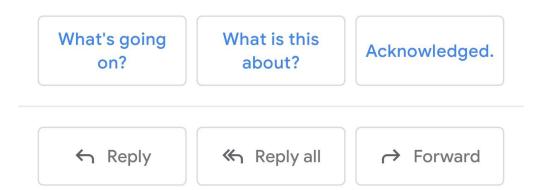
My W.A.E. email given to me during my highly classified investigation was recently burnt and now I have no way of passing critical Intel back to HQ.

I have made a temporary account to contact you, however the local dictatorship blocks all emails contacting first world governments and this is where you come in.

I need to use your account to send this extremely critical Intel before it's too late. This will require me accessing your email for security reasons.

Thank you in advance for your understanding.

Superintendent Vincent FBI



Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	The adversary tries to use Urgency and Intimation to access the victim's email account.



The project is going well no real problems yet.

The zip file is not ready yet when it is ill send it

Sorry no to coffee I'm busy with the family and will be unavailable all day

Best regards,

Reuben Corrigan | Cyber Security Trainee | Group Technology ANZ

Email - Reuben.corrigan@anz.com

839 Collins Street, Docklands, Victoria 3008, Australia



From: Bryce, Alan

Sent: Wednesday, August 21, 2019 2:11 PM
To: Corrigan, Reuben < Reuben.Corrigan@anz.com >

Subject: WFH

Hey Reuben,

Hope the project is coming along smoothly on your end.

I'll be working from home for the rest of this week as per previous discussion.

Can I get a zip of the workload for this week when you get the chance?

On a side-note; can we get coffee on Sunday arvo to discuss last week's Stand-up? I just wanted to go over a few things.

Kind regards,

Alan Bryce | Cyber Security Analyst | Group Technology ANZ

Email - Alan.Bryce@anz.com

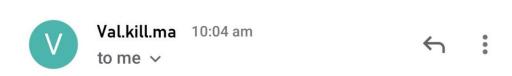
839 Collins Street, Docklands, Victoria 3008, Australia



Email 6:

Is this email Safe or Malicious?	My Analysis
Malicious	The email signature's colour is inconsistent because it is written in blue by Reuben Corrigan, while the signature from Alan Bryce is black. The adversary can masquerade as Bryce Alan because of asking for the zip file from the internal employee. The adversary tries to persuade the victim by using the familiarity of a colleague's email address.
	The conversation between two colleagues is not professional and too generic, which can be considered a malicious email.



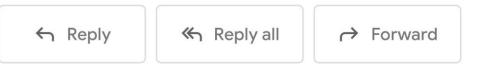


hxxp://iwhrhwicy.urlif.y/receipt.php

switch to Geico? > Inbox

Cheers,

Mike Ferris



Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	This is spam email and phishing email. The link to the website should be started as HTTP/https, not hxxp. The URL is from Russia. The company's website must contain the company's name, Geico, to be considered a legitimate email. The name of the sender and the "From" email address should be consistent, meaning they must indicate the legitimate name of the company or the sender, Mike. The root domain name must be .com for the commercial website, and the website must not have any root domain such as .php.