

Email 1:

Email 1



FYI



Inbox



Adam John 10:25 am

Hey mate, Did you see all those new trailers from Games Con??



Velma Khan 10:27 am

to me ▾



Yeah just saw the trailer for ksp2. Dude it looks sick as!!!!

You gonna buy the preorder?

[Hide quoted text](#)

On Wed, 21 Aug. 2019, 10:26

< Adamm.johnnn1996@gmail.com > wrote:

Hey mate,

Did you see all those new trailers from Games Con??

Is this email Safe or Malicious?

Safe

My Analysis

- No attachments with the mail.
- No malicious conversation or asking for anything suspicious.
- Enough to guarantee the safety of mail.

Email 2:

Email 2



OneDrive Action Required



Inbox



Venture.ru 10:22 am
to me ▾



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 receive large file.

Click [UPDATE YOUR ACCOUNT](#) 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.

Is this email Safe or Malicious?

Malicious

My Analysis

- Sender information not mentioned in the e-mail header.
- URL is created using hyperlinking which generally does happens when the attacker is trying to get you click on the links without seeing its content.
- Spelling mistakes are there which shows the e-mail is not from a genuine vendor.
- URL may be a phishing link to steal the data of the user.
- In these cases the user should just visit the official site to check if there is a problem without clicking on these links.
- This much information confirms that this is a phishing link.

Email 3



Is Facebook working for you? ➤



Inbox



Vinny

10:56 am

to me ▾



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

Can you try? <https://www.faceBook.com.opt/login.htm>

Thanks,
Vinny

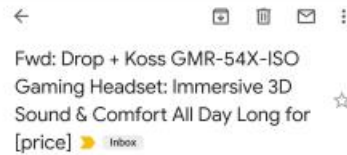
Is this email Safe or Malicious?

My Analysis

Malicious

- Firstly, the link provided in the e-mail appears to be fake as it has a trailer .htm which shows it is a fakely created link.
- This is an example of a phishing link which is attached in the mails to steal the information of the users.
- Also, if we closely observe the link it can be seen even by a non cyber professional that the link is fake as the "b" in facebook has a different format from the original spelling.
- This makes sure that the e-mail received by the user is fake and malicious.

Email 4



Adam Markus 10:38 am

----- Forwarded message -----
From: Adam Markus <Aman.zoom@gmail.com>
Date: Wed, 21 Aug. 2019, 10:30
Subject: Fwd: Drop + Koss GMR-54X-ISO Gaming Headset:
Immersive 3D Sound & Comfort All Day Long for [price]
To: <Zoomdewoop@gmail.com>

----- Forwarded message -----
From: **Drop (formerly Massdrop)** <info@massdrop.com>
Date: Wed, 21 Aug. 2019, 06:24
Subject: Drop + Koss GMR-54X-ISO Gaming Headset:
Immersive 3D Sound & Comfort All Day Long for [price]
To: <aman.zoom@gmail.com>



★★★★☆ 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




Is this email Safe or Malicious?	My Analysis
Safe	<ul style="list-style-type: none"> • No attachments of any kind. • A simple advertising mail by Adam Markus. • This confirms the E-mail is safe.

Email 5:

Email 5



You are needed  Inbox 

 **Vincent** 11:25 am
to me  

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

Is this email Safe or Malicious?	My Analysis
Malicious	<ul style="list-style-type: none">• Although, the mail looks professional and wants genuine help from the user• But, the person who sent the mail has claimed to be a government spy and a government spy would never reveal their identity to an unknown person.• And he is also requesting to a stranger's mail ID.• This is enough to deduce that this mail is a fake and malicious one.


Email 6:

Email 6

 Reply  Reply All  Forward  iM



Wed 21/08/2019 2:17 PM
Corrigan, Reuben
RE: WFH

To  Bryce, Alan


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



Is this email Safe or Malicious?

Safe

My Analysis

- Mails in this picture are in pprofessional format.
- Appears to be a conversation between two colleagues.
- No attachments or links
- This shows that the e-mails are safe.

Email 7:

Email 7

←

📄

🗑️

✉️

⋮

Did you know you can save up to 15% off your car insurance if you switch to Geico? 📧

Inbox

V

Val.kill.ma

10:04 am

to me ▾

↩️ ⋮

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

Cheers,

Mike Ferris

Is this email Safe or Malicious?	My Analysis
Malicious	<ul style="list-style-type: none">• Suspicious sender handle• No body in the mail• URL attached also appears to be a phishing link• This is enough proof to show that this mail is a malicious mail.