



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??

Yeah, I will.

Yeah.

No, I didn't.

↩ Reply

↩↩ Reply all

➦ Forward

**Email 1:**

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



## 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.

↩ Reply

↩↩ Reply all

➦ Forward

**Email 2:**

| Is this email Safe or Malicious? | My Analysis   |
|----------------------------------|---|
| Malicious                        | <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• The opening of the email should be Hi, Hello, or Dear.</li><li>• The email has poor typos like Customers, and “products and services and Security”.</li><li>• Vendors would not update products and services via email.</li><li>• According to all evidence, this email is treated as malicious email.</li></ul> |



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

Ok, I'll check it out.

Yeah, I can.

No, I can't.

↩ Reply

↩↩ Reply all

➦ Forward


**Email 3:**

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

← 📁 🗑️ 📧 ⋮

Fwd: Drop + Koss GMR-54X-ISO Gaming Headset: Immersive 3D Sound & Comfort All Day Long for [price] ☆

📧 Inbox

 **Adam Markus** 10:38 am  
to me ▾

----- Forwarded message -----  
From: **Adam Markus** <[Aman.zoom@gmail.com](mailto: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: <[Zoomdawoop@gmail.com](mailto:Zoomdawoop@gmail.com)>

----- Forwarded message -----  
From: **Drop (formerly Massdrop)** <[info@i.massdrop.com](mailto:info@i.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](mailto:Aman.zoom@gmail.com)>

## **DROP**

# 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. |





You are needed >> **Inbox**



**Vincent**  
to me ▾

11:25 am



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

What's going  
on?

What is this  
about?

Acknowledged.





↩ Reply

↩↩ Reply all

➦ Forward

**Email 5:**

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


 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](mailto: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](mailto: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](mailto:Alan.Bryce@anz.com)**

839 Collins Street, Docklands, Victoria 3008, Australia



**Email 6:**

| Is this email Safe or Malicious? | My Analysis   |
|----------------------------------|---|
| Malicious                        | <p>The email signature's colour is inconsistent because it is written in blue by Reuben Corrigan, while the signature from Alan Bryce is black.</p> <p>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.</p> <p>The conversation between two colleagues is not professional and too generic, which can be considered a malicious email.</p> |



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



Inbox



**Val.kill.ma** 10:04 am  
to me ▾



[hxxp://iwhrhwicy.urlif.y/receipt.php](http://hxxp://iwhrhwicy.urlif.y/receipt.php)

Cheers,

Mike Ferris

↩ Reply

↩↩ Reply all

➦ Forward

**Email 7:**

| <b>Is this email Safe or Malicious?</b> | <b>My Analysis</b>   |
|---|--|
| Malicious                               | <p>This is spam email and phishing email.</p> <p>The link to the website should be started as HTTP/https, not hxxp. The URL is from Russia.</p> <p>The company's website must contain the company's name, Geico, to be considered a legitimate email.</p> <p>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.</p> <p>The root domain name must be .com for the commercial website, and the website must not have any root domain such as .php.</p> |