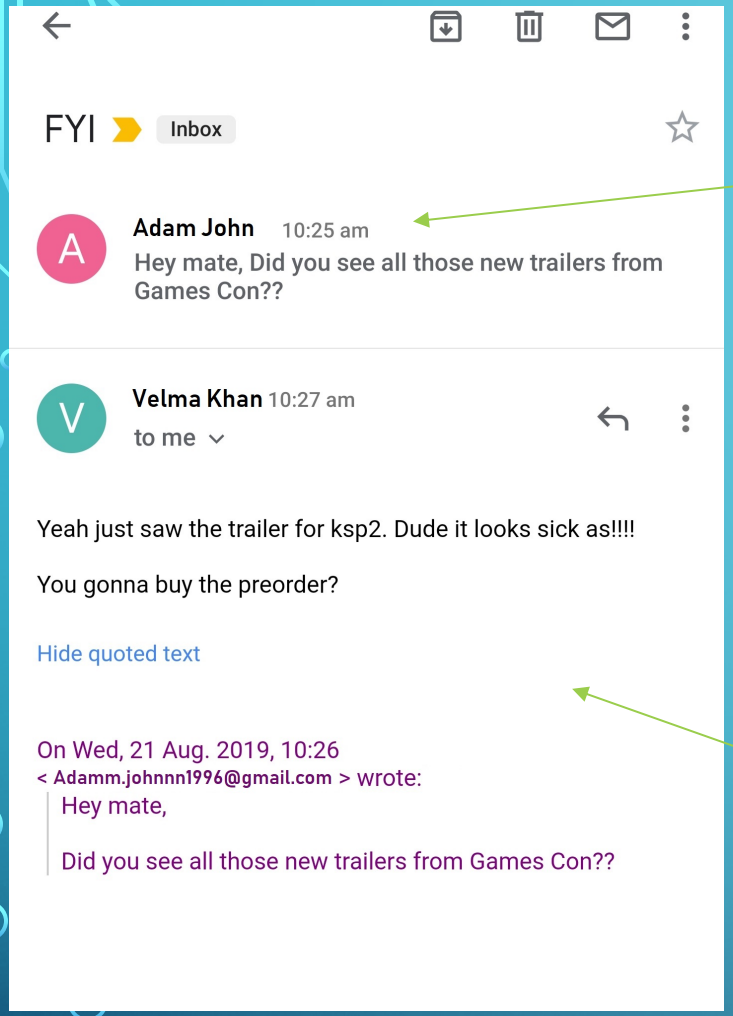
Email 1



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

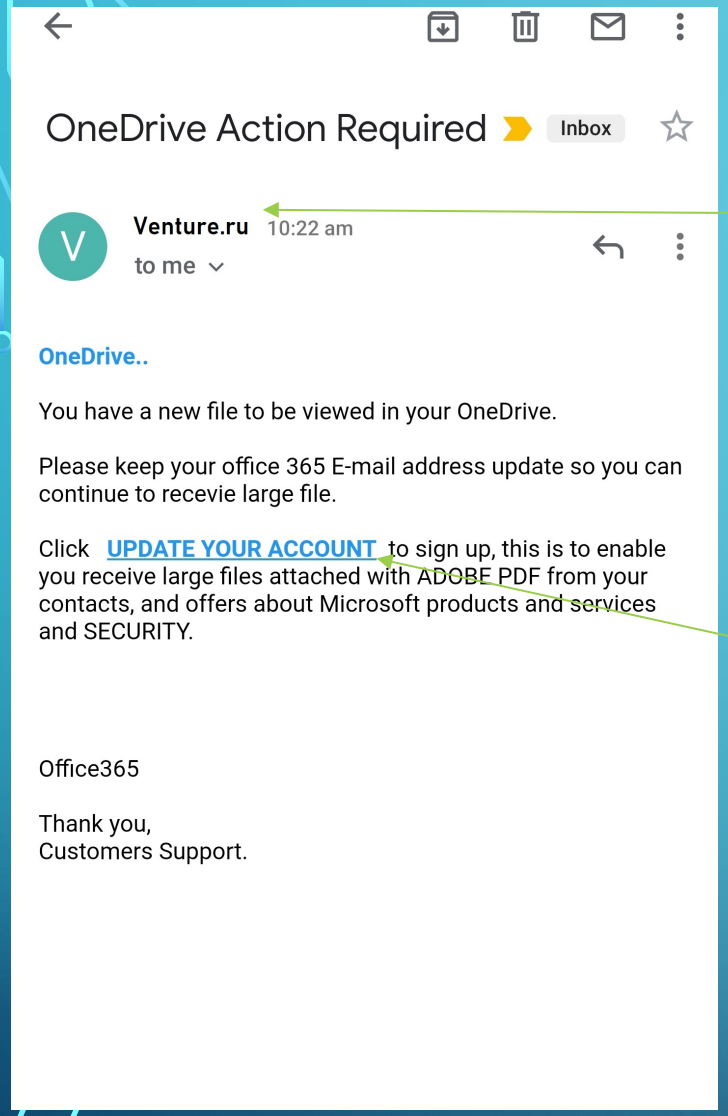
On Wed, 21 Aug. 2019, 10:26
< Adamm.johnnn1996@gmail.com > wrote:

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

It's clearly not spam as the reply indicates a previous relationship and that the email was expected and welcome. The date and time could indicate that the conversation was anticipated, as there is next to no delay in a reply.

This email is non malicious. It's a typical conversation between friends and contains no potentially dangerous artefacts.

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 recevie 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.

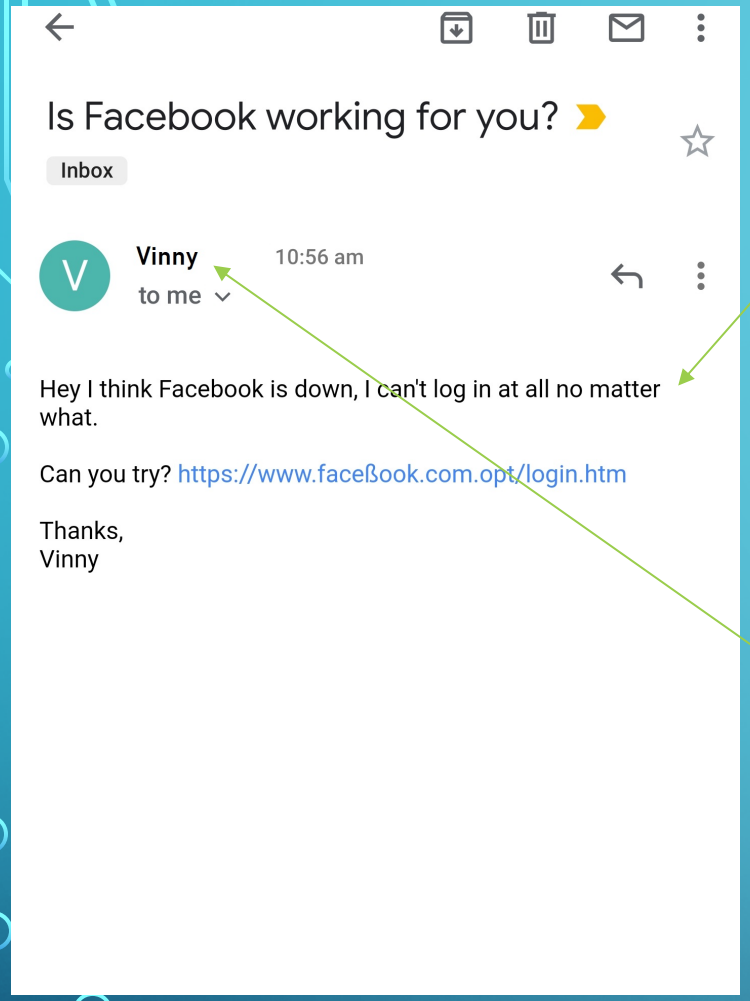
Office365

Thank you,
Customers Support.

The email claims to be from one drive but the email sender is from a Russian domain which is well known for malicious emails.

The email tries to get the user to download a file, without providing information about the file's content, or the sender. The email's format is unprofessional and contains poor grammar & spelling. You would not expect an email from an official Microsoft service to be formatted and presented like this.

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.faceßook.com.opt/login.htm

Thanks,
Vinny

The email is presented as a question from a friend who cannot access Facebook, and asks the recipient to follow a link to see if Facebook is working for them. But the link provided is actually a phishing link make to look like facebook.com at first glance.

The senders account could be compromised, so a malicious email like this could still come from a trusted friends account.

Email 4

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 >
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 >

---------- Forwarded message ---------
From: **Drop (formerly Massdrop)** < 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 >

DROP

Step Your Game Up

★★★★☆ 23 Reviews

SEE MORE

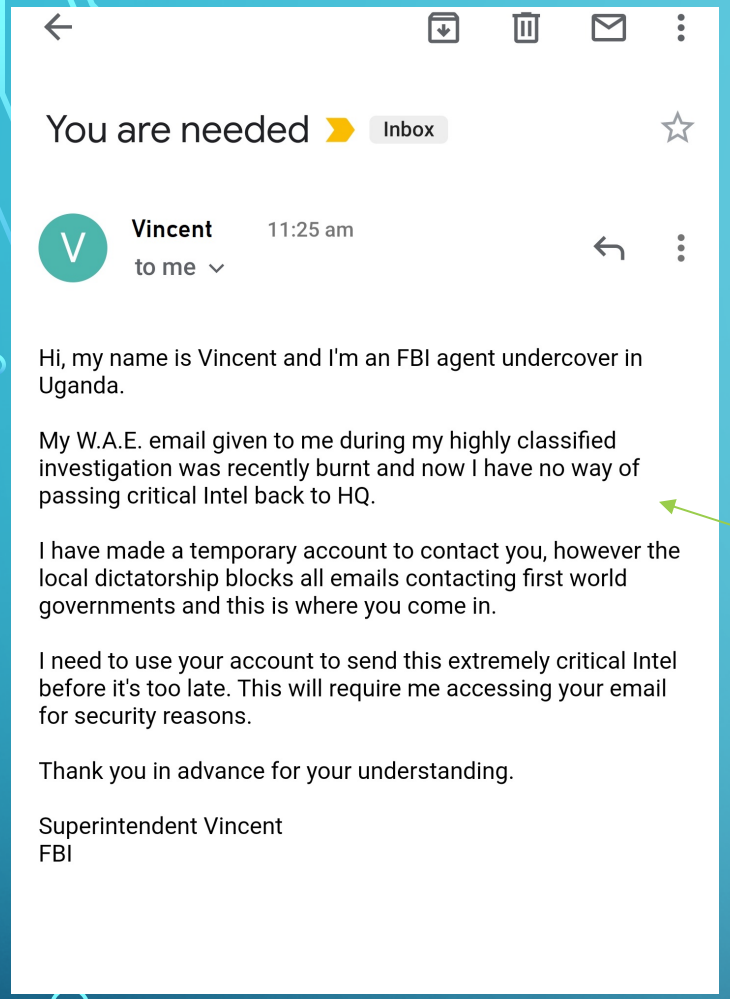
Pairing a closed-back design with custom-engineered acoustics, the Drop + Koss GMR-54X-ISO gaming headset offers truly immersive 3D sound—when gaming or listening to music. Crafted in a subtle midnight blue colorway, the headset features a lightweight headband for comfort during long sessions. It also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

This email is an example of generic marketing, it could be regarded as Spam (unwanted or unrequested marketing content). It's been forwarded twice, but the original sender is a mass mail service.

If googled, the site can be seen as a sales site that contains no malicious content.

The email contains no links or requests for information, just pure advertising.

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

The email is requesting the recipient's credentials for unusual reasons. They've tried to make the issue seem urgent, which is a well-known persuasive technique often used for phishing. The email lacks professionalism which gives more reason to believe it's a fake. Legitimate users/services would not ask for account details. This is almost always a sign of malicious activity.

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

ANZ

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,

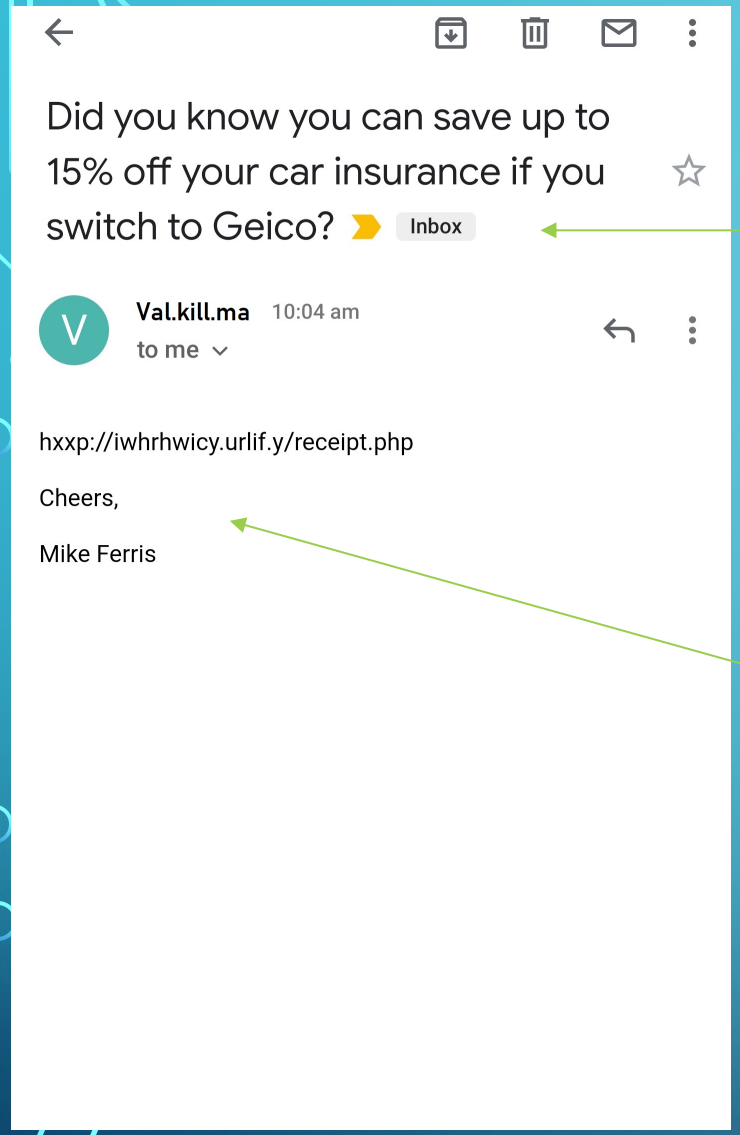
Alan Bryce | Cyber Security Analyst | Group Technology ANZ
Email - Alan.Bryce@anz.com
839 Collins Street, Docklands, Victoria 3008, Australia

ANZ

This email is non malicious. It is a typical workplace email. There are no files, links or suspicious requests within the emails, and for the most part internal work emails can be trusted to be safe.

The senders email address matches the name on the signature, and appears to be well formatted and professional.

Email 7



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

Cheers,

Mike Ferris

The email claims to be from Geico Insurance but the sender doesn't have an official Geico email address, and the URL provided is not linked to Geico in any way.

The email sender claims to be someone called "Mike Ferris", but the display name of the sender is Val.kill.ma.

Legitimate companies would use HTTPS for any financial transactions. The link provided is just http, which is another indicator that this is a fake. HTTPS is secured and encrypted where as HTTP is not.