[redacted]

[redacted]

Subject: FCA SENSITIVE: [redacted] Update - Update 6

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- Continue monitoring of the Quarantine mailbox.

  Update: 19/10 – No suspicious emails received.

- [redacted]
- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- Closed 13/10. Microsoft analysis of mail to see if it can be filtered using their services. – Update: MS have not presented any further options to that of which we are already pursuing.
- Closed 13/10. Emails with key words in sender address "SCC, Unite the Union, Collective Bargaining and Unitetheunion.org" to be added to email filtering

Regards,

[redacted] / Infrastructure & Operations / BTS Division / [redacted]
Visit our pages at [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]
Subject: FCA SENSITIVE: [redacted] Update - Update 5

[redacted]

- [redacted]
- [redacted]
- [redacted]
- The quarantine mailbox created has now been converted to an [redacted] Quarantine mailbox. Access will be limited to C&IR and Security Operations. No further emails have been captured as suspicious.

Remaining action updates are as follows:

- Continue monitoring of the Quarantine mailbox.

  Update: 2 emails received on the 13/10 and 1 on the 14/10, both have been reviewed and require no further action. No further emails received on the 15/10. 1 email received on the 18/10 however not suspicious and has been released. 19/10 – No malicous.

- [redacted]

[redacted]

- [redacted]

- Closed 15/10. Restrict Inbound mail sent to a large numbers of users. Update: Computacenter have confirmed following consultation with Microsoft that this is not technically possible.

- [redacted]

- Closed 13/10. Emails with key words in sender address "SCC, Unite the Union, Collective Bargaining and Unitetheunion.org" to be added to email filtering

Regards,

[redacted] / Infrastructure & Operations / BTS Division / [redacted]
Visit our pages at [redacted]

[redacted]
Subject: FCA SENSITIVE: [redacted] Update - Update 4

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- The quarantine mailbox created has now been converted to an [redacted] Quarantine mailbox. Access will be limited to C&IR and Security Operations. No further emails have been captured as suspicious.

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Completed Actions:

- Closed 15/10. Restrict Inbound mail sent to a large numbers of users. Update: Computacenter have confirmed following consultation with Microsoft that this is not technically possible.
- [redacted]
- [redacted]
- [redacted]
- Closed 13/10. Emails with key words in sender address "SCC, Unite the Union, Collective Bargaining and Unitetheunion.org" to be added to email filtering

Regards,

[redacted] Infrastructure & Operations / BTS Division / [redacted]
Visit our pages at [redacted]

[redacted]
Subject: Action Update 13/10: Email - Spam Incident - Update 3

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- The quarantine mailbox created needs to be moved to an [redacted] Quarantine mailbox and will require Security admin roles in Office365. Access will be limited to C&IR and Security Operations. [redacted] has agreed this.

  ACTION: [redacted] to take to Gold for approval on limited access for C&IR and Security Operations.

Remaining action updates are as follows:

- [redacted]
- Restrict Inbound mail sent to a large numbers of users.

  Update: This continues to be investigated with EUC ([redacted]) leading, along with options.
- Continue monitoring of the Quarantine mailbox.

  Update: 2 emails received on the 13/10 and 1 on the 14/10, both have been reviewed and require no further action.
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- Closed 13/10. Microsoft analysis of mail to see if it can be filtered using their services. – Update: MS have not presented any further options to that of which we are already pursuing.
- Closed 13/10. Emails with key words in sender address "SCC, Unite the Union, Collective Bargaining and Unitetheunion.org" to be added to email filtering

Regards,

[redacted]
[redacted] Infrastructure & Operations / BTS Division / [redacted]
Visit our pages at [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Subject: Action Update 13/10: Email - Spam Incident - Update 2

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- Key word filters have been enhanced to include "SCC, Unite the Union, Collective Bargaining and Unitetheunion.org" in the email address (as well as in content of email for unite the union, collective bargaining and unitetheunion.org), Computacenter will be capturing the different permutations of these words and including them in the filter. A redirect box has been created with access granted to Security Operations and CTU to review emails captured against these filters.
- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]

[redacted]

- [redacted]
- In Progress – Restrict Inbound mail to large numbers of users. Update: This continues to be investigated with [redacted] leading, along with options.
- Continue monitoring quarantine mailbox – ongoing. One email identified today relating to this incident (with CTU)
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

Regards,

[redacted] Infrastructure & Operations / BTS Division / [redacted]
Visit our pages at [redacted]

[redacted]

Subject: Action update 13/10: Email - spam incident

[redacted]

[redacted]

Option 2

Filtering of mails that contain the Unite URL and/or sender mail addresses and send to a quarantine

Benefit: Mails with links to Unite would be filtered and would not reach users

Risks: Legitimate mails would not get through. This would need to be maintained as new addresses and content to the mails are likely to be used by the senders. If this were to be used long term, resource would be needed to process quarantine mailbox.

Action 1: CC to look at if we could effectively filter emails in this way
Complete. A redirect mailbox has been created and access provided to SecOPS and CTU. The filters for the known sender mail addresses are in place. The filters for the Unite URL are in place.

[redacted]

Option 4

Microsoft analysis of mail to see if it can be filtered using their services

Benefit: Intelligent filtering could be done on Exchange prior to the mail arriving with a user
Risks: Some legitimate mails may also be filtered out. Resource would be needed to process quarantine mailbox

Action 1: FCA to send original mail samples to Microsoft
Complete. Microsoft have been engaged through a Severity A call to Premier Support. They have not provided any further options beyond that which we are doing in options 1-3. The mails are not technically spam as they carry no malware payload, or links to unsolicited products, services or known scams.

FCA SENSITIVE

Minutes of [redacted] BTS Updates – No 7
21 October 2021

Attendees:

[redacted]

Apologies:

[redacted]

[redacted]

[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Inbound Quarantine Mailbox	Continue monitoring of the Quarantine mailbox. Any identified emails will be flagged to [redacted].	[redacted]	Ongoing	

	21/10 Update: Some emails have been quarantined from UNITE. These have been released following approval from [redacted]. Going forwards, emails that require confirmation of release should be sent to [redacted]. **20/10 Update:** Any identified emails will be flagged to [redacted] **19/10 Update:** Any identified emails will be flagged to [redacted]. **18/10 Update:** 18/10: 2 emails received on the 13/10 and 1 on the 14/10, both have been reviewed and require no further action. No further emails received on the 15/10. 1 email received on the 18/10 however not suspicious and has been released.			
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	

	[redacted]			
Inbound Email	Closed 13/10. Microsoft analysis of mail to see if it can be filtered using their services. – Update: MS have not presented any further options to that of which we are already pursuing.	[redacted]	Closed	
Inbound Email	Closed 13/10. Emails with key words in sender address "SCC, Unite the Union, Collective Bargaining and Unitetheunion.org" to be added to email filtering	[redacted]	Closed	
[redacted]	[redacted]	[redacted]	[redacted]	
Inbound Email	Closed 15/10. Restrict Inbound mail sent to a large numbers of users. Update: Computacenter have confirmed following consultation with Microsoft that this is not technically possible.	[redacted]	Closed	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Subject: Gold: [redacted] - Draft Decisions and Actions

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4	13/10/2021	[redacted]	In response to the incident to mitigate the evolving threat, incoming emails from addresses containing 'RealSCC' and 'Real SCC' and variants thereof (regardless of domain used) had been blocked and held in quarantine to be reviewed to verify the sender's identity and the validity of the email. Additional terms and variations were asked to be added to this list. It was also noted that some FCA staff had been sending emails from personal email addresses to their own FCA work email addresses containing links to the union petition. These had also been blocked and held in quarantine but was evidence that staff were probing IT rules to test which emails would come though, potentially in advance of sending to a wider audience. Gold clarified that staff were not allowed to use work emails for non-FCA business.	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Actions:

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3	13/10/2021	Draft	[redacted]	Add the following terms to the block list for incoming email addresses - 'RealSCC', 'RealFCA' (including underscore/hyphen/space variations), 'SCC', 'Unite the Union', 'Collective bargaining' and 'unitetheunion.org' and variants thereof	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Kind regards

[redacted]

[redacted]

Central Secretariat / Corporate Governance Division

[redacted]

This email is FCA Official unless marked otherwise

For more information on how the FCA is governed and decisions are made visit the Central Secretariat and Governance & Decision Making Faculty pages

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Subject: Re: Real SCC

[redacted]

I've just asked the CC Messaging team via MIM. I've suggested the [redacted] quarantine mailbox with the 3 of us having minimal permissions to get the emails released and ongoing monitoring.

[redacted]

[redacted]

[redacted] Business and Technology Solutions

Visit 'Do No Harm' pages

[redacted]

This email is FCA Official unless marked otherwise

[redacted]

Subject: RE: Real SCC

Not sure I want to "just forward" them, as it will then be highly visible that we are intercepting mails. Is there a better way or redirecting that would provide us with a proper quarantine/review/release mechanism?

Thanks

[redacted]

[redacted]

Subject: RE: Real SCC

Think we'd have to just forward them, they aren't being held as such, just diverted to this mailbox.

[redacted] Business and Technology Solutions

[redacted]

Visit 'Do No Harm' pages

[redacted]

This email is FCA Official unless marked otherwise

[redacted]

Subject: RE: Real SCC

I spoke with [redacted] earlier, and he is keen that we release from guarantee benign emails that are diverted. Do we have the capability to do so?

[redacted]

[redacted]

DONO HARM
INFO • PRIVACY • SECURITY

[redacted]

Subject: RE: Real SCC

[redacted]

The current redirection rules already catch that scenario – please see attached for a test.

[redacted]

Visit our pages on [redacted]
This email is classified as FCA Official, unless marked otherwise.

[redacted]

Subject: FW: Real SCC

I have a concern that a real attack may try to piggy back on the Unison petition. Is it technically possible to write a rule that looks for a phishing weblink disguised to look like the Union link, but which actually goes somewhere else?

[redacted]

Our values

Deliver in the public interest | Act with integrity | Be ambitious | Work inclusively | Connect and deliver

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]
Subject: RE: Gold: [redacted] - Draft Decisions and Actions

[redacted]

There was an additional action agreed in the side bar to add: SCC, Unite the Union, collective bargaining and unitetheunion.org in the filter terms (from external senders) so any containing these words in the sender field will be sent to the quarantine mailbox for monitoring too.

[redacted]

[redacted]

[redacted]

[redacted]

Subject: Gold: [redacted] - draft decisions and actions

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
9	14/10/2021	[redacted]	Following the block on variations of agreed trigger words, two emails had been received and captured in the past 36 hours. It was not possible to determine if this was genuine or an individual probing the system. Both cases had been passed to HR and [redacted] to address. Gold were assured that the quarantine of emails triggering the filter would not hinder any genuine formal or legal incoming correspondence. The team were working on an enhancement of the system so that where any false positives were identified these could be released to targeted recipients. [redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Kind regards
[redacted]

[redacted]
[redacted]
Central Secretariat / Corporate Governance Division
[redacted]
[redacted]

This email is FCA Official unless marked otherwise

For more information on how the FCA is governed and decisions are made visit the Central Secretariat and Governance & Decision Making Faculty pages