



Ĩ		
		e e
		15
(553)		11

- 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,

/ Infrastructure & Operations / BTS Division /
Visit our pages at

Subject: FCA SENSITIVE:	Update - Update 5
The quarantine mailbox	created has now been converted to an

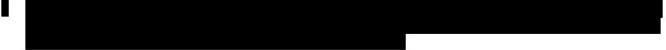
The quarantine mailbox created has now been converted to an Quarantine mailbox. Access will be limited to C&IR and Security Operations. No further emails have been captured as suspicious.

### 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.





• 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.



• 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,



_		

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



### **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.



• 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,

	Infrastructure & Operations / BTS Division /
Visit our	pages at .
Subject	: Action Update 13/10: Email - Spam Incident - Update 3
-	
()	
2	
	The quarantine mailbox created needs to be moved to an Quarantine mailbox and will require Security admin roles in Office365. Access will be limited to C&IR and Security Operations. The has agreed this.

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

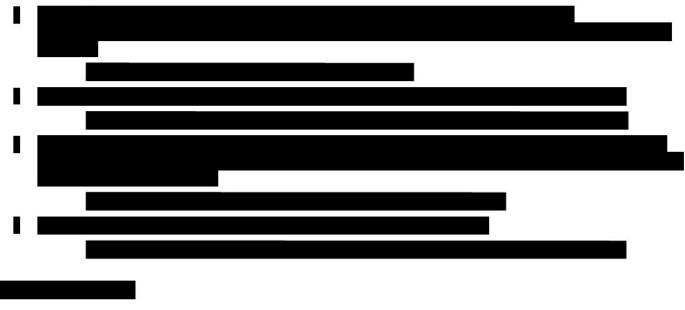
#### Remaining action updates are as follows:

Restrict Inbound mail sent to a large numbers of users.

Update: This continues to be investigated with EUC ( ) 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.





 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,



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

 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.

•		
	I	
	I	
I	-	

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

Regards, Infrastructure & Operations / BTS Division / Visit our pages at
Subject: Action update 13/10: Email - spam incident

# 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.



## 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.



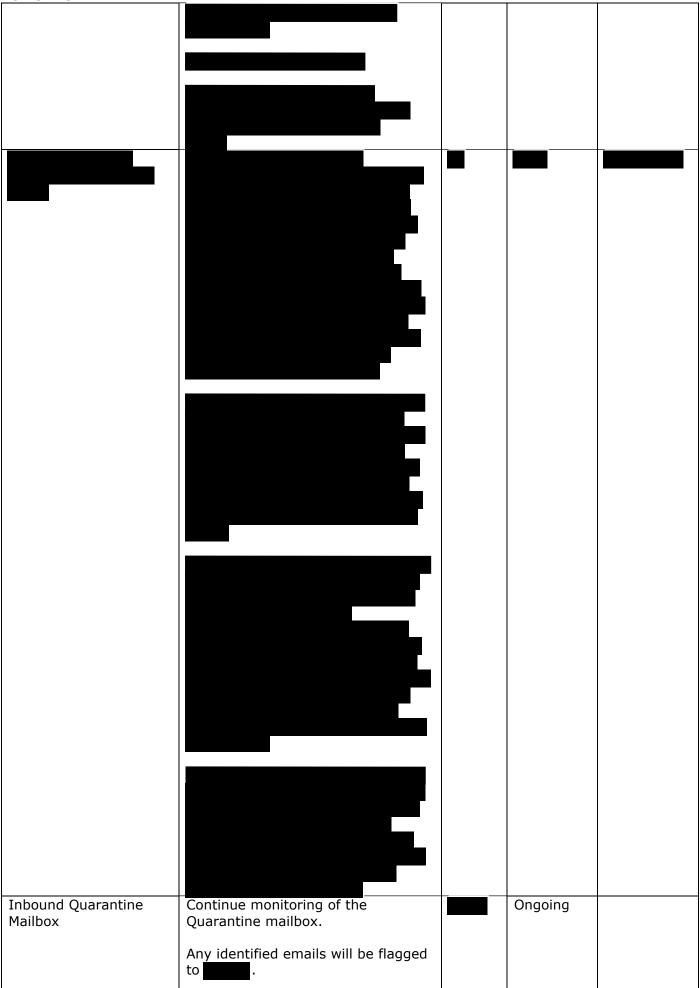
## Minutes of BTS Updates – No 7 21 October 2021

#### Attendees:



# **Apologies:**

# FCA SENSITIVE



## FCA SENSITIVE

FCA SENSITIVE			1
	<b>21/10 Update:</b> Some emails have been quarantined from UNITE. These have been released following approval from <b>Constant Sector</b> . Going forwards, emails that require confirmation of release should be sent to <b>Constant Sector</b> .		
	<b>20/10 Update:</b> Any identified emails will be flagged to		
	<b>19/10 Update:</b> Any identified emails will be flagged to <b>be and a set of the set of the</b>		
	<b>18/10 Update:</b> 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.		

# FCA SENSITIVE

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.	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	Closed	
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.	Closed	

Subject: Gold:	- Draft Decisions and Actions

4	13/10/2021	In response to the incident to mitigate the evoluting threat, incoming empile from addresses	
4	13/10/2021	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.	

Actions:

3	13/10/2021	Draft	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	

### Kind regards

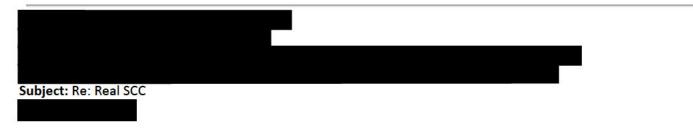
Central Secretariat / Corporate Governance Division

### This email is FCA Official unless marked otherwise

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

Ľ	
N 2	





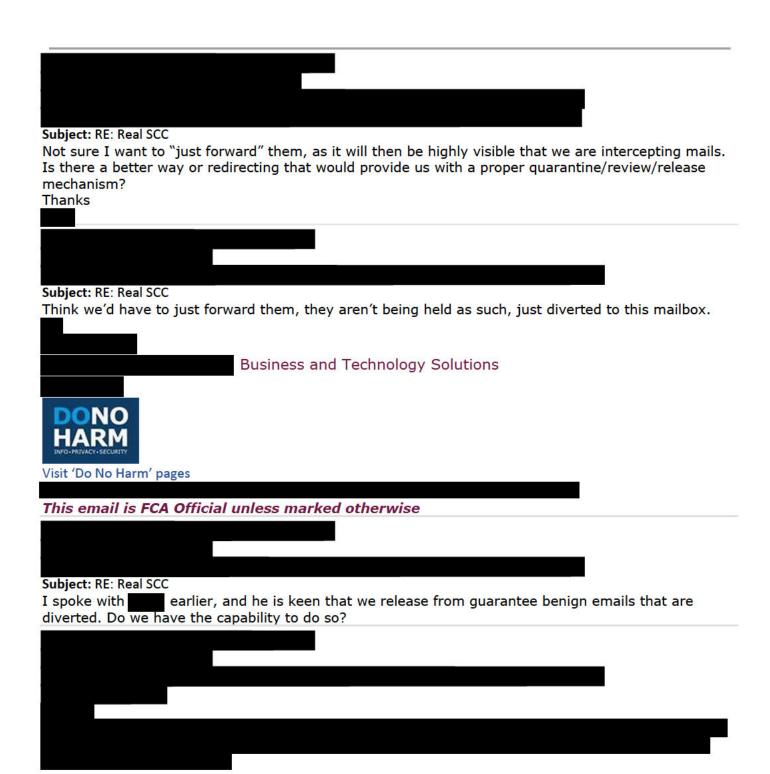
I've just asked the CC Messaging team via MIM. I've suggested the **exact set of the set** 

Business and Technology Solutions



Visit 'Do No Harm' pages

This email is FCA Official unless marked otherwise



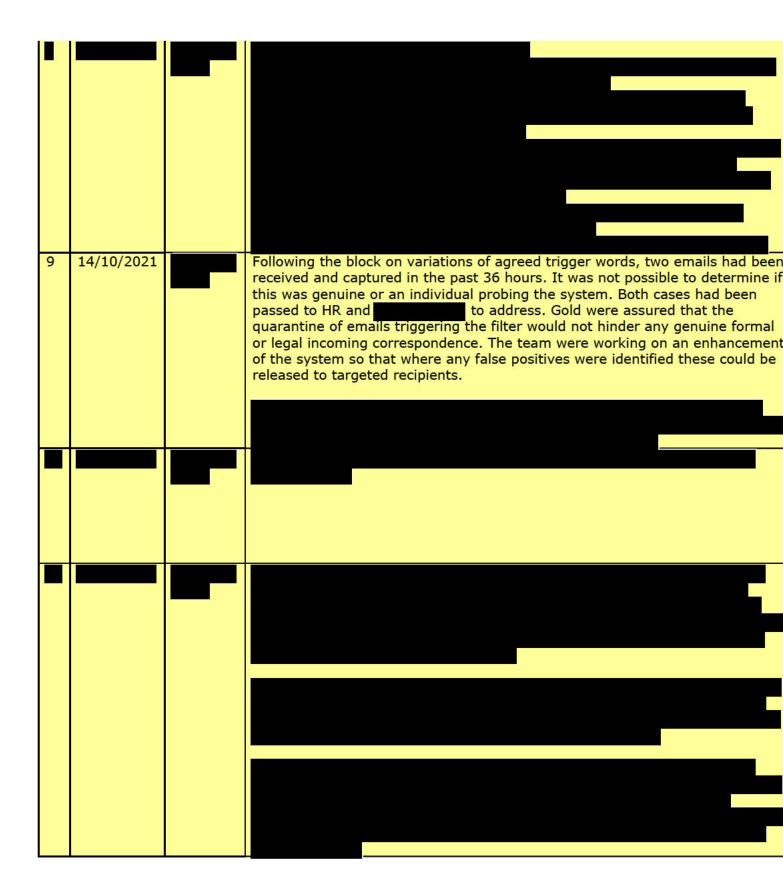
DONO
HARM
INFO-PRIVACY-SECURITY
Subject: RE: Real SCC
The current redirection rules already catch that scenario – please see attached for a test.
Visit our pages on This email is classified as FCA Official, unless marked otherwise.
This email is classified as FCA Official, unless marked otherwise.
Subject: EW/: Peol SCC
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 wh
actually goes somewhere else?
Our values
Deliver in the Act with Be Work Connect
public interest   integrity   ambitious   inclusively   and deliver

Subject: RE: Gold:	- Draft Decisions and Actions

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.



i .		
Subject: Gold:	- draft decisions and actions	



to - 62	144 - <sup>0</sup> 2f		



### This email is FCA Official unless marked otherwise

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