



CJSM Defend

User Guide

History

Version	Date	Description
0.1	03/09/2024	First Draft
1.0	14/11/2024	Version 1.0

Confidentiality statement

This document contains information confidential and proprietary to Egress Software Technologies. It shall not be disclosed in whole or part by the recipient to any third party or to any employees other than those who have a need to know such information. It shall not be duplicated or used by the recipient for any purpose other than to evaluate Egress Software Technologies products and services.

No part of this document may be reproduced, distributed, stored in a database or retrieval system, or transmitted in any form or by any means, without the exclusive and written permission of Egress Software Technologies. No liability is assumed for damages resulting from the use of the information contained herein.

Copyright notice

Copyright © Egress Software Technologies. All rights reserved. Registered Address:
White Collar Factory, 1 Old Street Yard, London, EC1Y 8AF, United Kingdom.

Contents

Introduction	4
CJSM Defend Banners.....	5
Reporting an email.....	7
REPORT AS PHISH	7
REPORT AS NOT PHISH.....	7
Link Scanning.....	8
Security	9

Introduction

We are seeing an increase in email phishing attempts on users in the Justice community. Phishing is a cybercrime where attackers attempt to trick people into revealing sensitive information or clicking on malware. As a result, we have implemented additional security controls with the CJSM service, "CJSM Defend". This service will provide advice on incoming emails sent via CJSM, indicating whether the email is potentially harmful.

CJSM Defend is an anti-phishing and malware protection service that is integrated into the existing CJSM platform. CJSM Defend will provide you visible prompts and rewrite links to help you evaluate the context, relationships and message content of your inbound emails.

The "CJSM Defend" service is a dedicated and customised instance of a leading email security solution, specifically tailored for the CJSM service. It has been optimised to provide key benefits to the CJSM user community, ensuring the confidentiality and security of the CJSM platform is maintained at all times.

This solution incorporates the latest threat intelligence updates to protect against a range of sophisticated email security threats. All emails will be scanned automatically when traversing the CJSM service, with the introduction of clear banner alerts to notify users of potential threats.

CJSM Defend provides an **advisory notice** to users with additional information and guidance. It **does not** replace individuals and organisations existing processes and responsibilities for managing malicious emails.

Please remain vigilant and if you are in any doubt regarding the legitimacy of an email, inform your IT department and/or relevant parties within your organisation.

Rest assured that confidentiality is being maintained with all your emails and CJSM remains a secure communication method.

If you have any questions, please reach out to CJSM Support via cjsm.helpdesk@egress.com or 0207 604 5598 between 08:00 and 19:00 Monday to Friday.

CJSM Defend Banners

Incoming emails will have a coloured banner inserted to inform you how the email has been classified. The colour of the banner corresponds to the associated level of threat.

There are three colour classifications:

Blue

These banners are purely informative and not associated with a detected threat. In most cases, no action is required.

Amber

Email has suspicious elements that indicates phishing or impersonation. Exercise caution when responding or clicking on links and ensure you are responding to the real sender.

Red

Email has very strong signs of phishing. Extreme caution should be used if responding or clicking any links. Please refer to your internal policy for dealing with malicious emails.

The most common CJSM Defend banners can be seen below:

 First time sender >

 Contains topics of a financial nature >

 Discusses sensitive information >

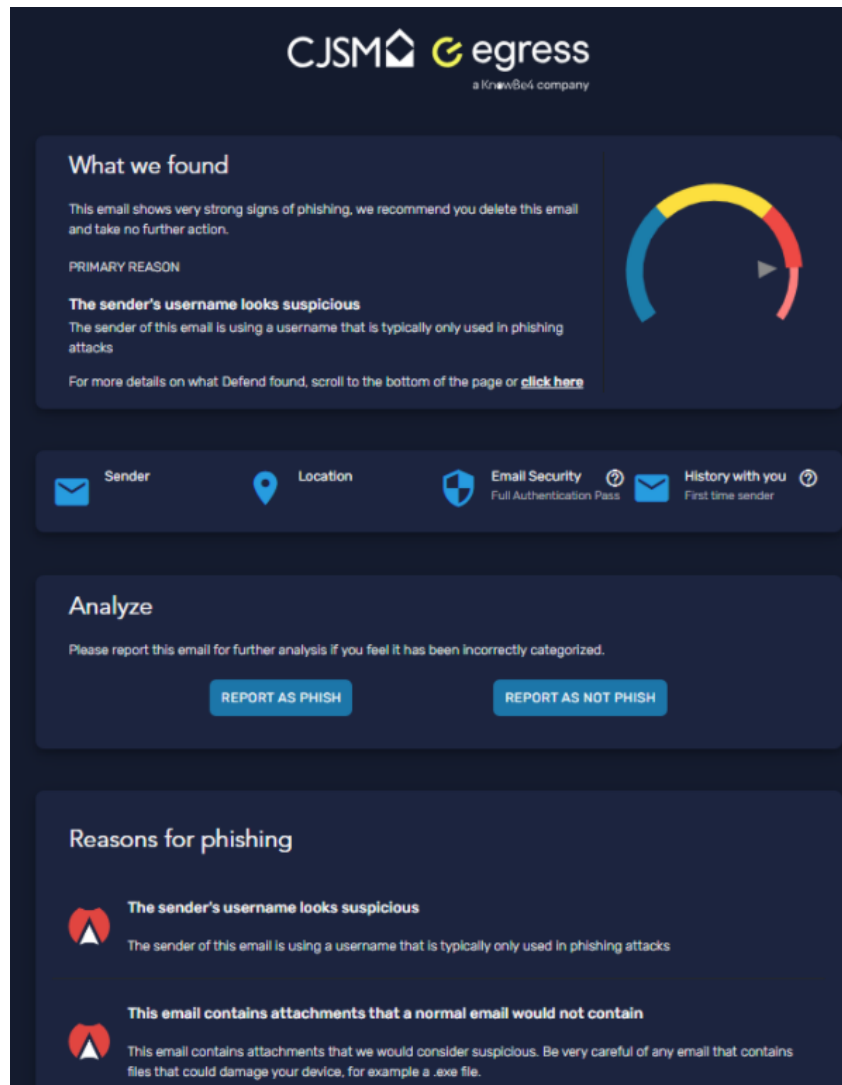
 This email shows signs of phishing >

 This email shows signs of impersonation >

 This email shows **strong** signs of phishing >

All banners applied by CJSJ Defend can be clicked on to find out more about what was detected in the email.

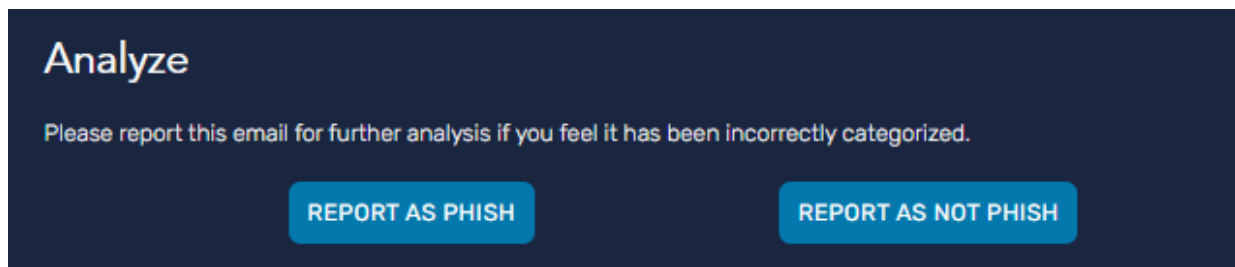
Here is an example of what will be presented when you click on a banner. This is known as the email summary section:



CJSJ Defend will provide information as to why your specific email has been flagged. Please note, there may be other reasons as to why the email has been classified a certain way that may not be visible in the email summary section.

Reporting an email

If you think an email has been categorised incorrectly, report it by selecting either **REPORT AS PHISH** or **REPORT AS NOT PHISH**, under the Analyze section of the email summary page.



REPORT AS PHISH

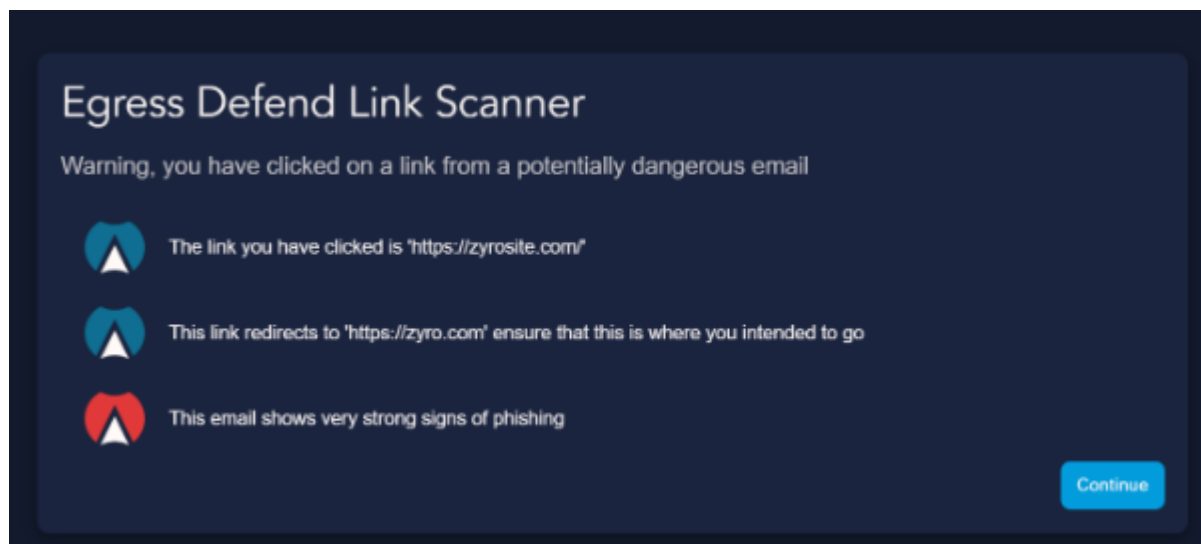
Your report will be reviewed by our threat intelligence team and dealt with on an individual basis. You will only be in contact if further information is required. If you are reporting a phish, please also inform your IT department and/or relevant parties within your organisation. If there is a confirmed compromise, please inform the CJSM Helpdesk via cjsm.helpdesk@egress.com.

REPORT AS NOT PHISH

If your email has been incorrectly categorised as Phishing, please ensure you report via the NOT PHISH button as this will feed the Defend algorithm and help improve the accuracy of the service going forward. However, please note that you may still receive warning notifications for similar emails in the future and we cannot tailor the email banners to individual needs.

Link Scanning

As a precaution, CJSM Defend automatically rewrites any links in emails you receive. This will check the website associated with the URL for security threats prior to you visiting it. Scanning is automated, maintaining the confidentiality of each link (URL) as well as any additional email content. If CJSM Defend flags a link you click on as potentially harmful, you will be redirected to a landing page while checks are carried out on the linked website. The landing page displays the link you have clicked, it also shows the true destination of the original link - and any results found in CJSM Defends analysis.



Important: The link scanning and rewriting functionality may have implications for organisations that send single-use links via CJSM. A single-use link is a custom web address (URL) that can ONLY be used ONCE, such as a link to reset a password.

If you are concerned that this may cause issues with your service, please reach out to the CJSM Helpdesk at your earliest convenience via 0207 604 5598 between 08:00 and 19:00 Monday to Friday, or raise a case with our Service Desk by emailing cjsm.helpdesk@egress.com.

Security

The CJSM Defend product has undergone rigorous assurance by the Ministry of Justice's cyber security team. The product has been assessed against the Ministry of Justice's security policy, HMG requirements and industry best practises, whilst ensuring it meets the user and security needs of the CJSM service.