

Signaler les courriers indésirables, les messages mal classés et les messages viraux

Contenu

[Introduction](#)

[Types d'envoi de messages électroniques](#)

[Pourquoi envoyer des e-mails à Cisco ?](#)

[Portail d'état de la messagerie](#)

[Comment signaler des messages électroniques à Cisco](#)

[Complément d'envoi sécurisé d'e-mails Cisco](#)

[Plug-in de sécurité de la messagerie Cisco](#)

[Envoi direct par e-mail](#)

[Microsoft Outlook](#)

[Microsoft Outlook Web App, Microsoft Office 365](#)

[Microsoft Outlook 2011 et Microsoft Outlook 2016 pour Mac \(OS X, macOS\)](#)

[Courrier \(OS X, macOS\)](#)

[Thunderbird Mozilla](#)

[Plates-formes mobiles \(iPhone, Android ou autre\)](#)

[Comment vérifier les envois à Cisco](#)

[Envoi direct par e-mail](#)

[Portail d'état de la messagerie](#)

[Additional Information](#)

[Documentation relative à la passerelle de messagerie sécurisée Cisco](#)

[Documentation de la passerelle de messagerie sécurisée](#)

[Documentation relative à Cisco Secure Email and Web Manager](#)

[Documentation relative aux produits Cisco Secure](#)

Introduction

Ce document décrit les rapports de courrier indésirable, d'erreur de classification, de virus ou d'e-mails supplémentaires envoyés à Cisco pour assistance ou examen.

Types d'envoi de messages électroniques

Les courriels de spam, de spam et de marketing sont les suivants :

- *Courrier indésirable* : Message(s) électronique(s) non pertinent(s) ou inapproprié(s) à un destinataire.
- *Ham* : Message électronique qui n'est pas du spam. Ou « non-spam », « bon courrier ».
- *Marketing* : Commercialiser directement un message commercial.

Cisco accepte les envois pour tout e-mail mal classé :

- faux négatif (spam manqué)
- faux-positifs (ou « jambe »)
- messages marketing faux-négatifs
- messages marketing faux positifs
- messages suspectés de phishing, messages positifs de phish
- messages infectés par des virus

Pourquoi envoyer des e-mails à Cisco ?

Les e-mails manqués ou marqués de manière incorrecte ont été signalés à l'aide de Cisco en ce qui concerne la confirmation du contenu, l'efficacité globale et les règles et scores associés. Une fois que vous avez signalé un e-mail à Cisco, vous pouvez également afficher d'autres objets observables et pièces jointes intégrées via le portail d'état des e-mails.

Portail d'état de la messagerie

Avec un ID CCO valide, vous pouvez vous connecter à https://talosintelligence.com/tickets/email_submissions. Le portail d'état des e-mails est un outil permettant d'afficher l'état de vos e-mails envoyés à Cisco. Cisco encourage les envois de spam/hameçonnage qui ont contourné le contenu de détection actuel et de spam, e-mail souhaitable qui a été filtré de manière incorrecte, afin d'améliorer l'efficacité globale. Le portail d'état des e-mails permet de suivre l'état de ces envois. Vous pouvez surveiller vos envois et les administrateurs de domaine ou les visualiseurs de domaine peuvent surveiller tous les envois de votre ou vos domaines.

Remarque : l'ancien portail de suivi et de soumission des e-mails (ESTP) a été remplacé par le portail d'état des e-mails, hébergé sur Talosintelligence.com, à compter du 1er septembre 2020.

Comment signaler des messages électroniques à Cisco

Les méthodes prises en charge sont les suivantes :

1. Complément d'envoi sécurisé d'e-mails Cisco
Prise en charge d'Outlook (Windows, Mac et Web)
2. Plug-in de sécurité de la messagerie Cisco Prend en charge Outlook (Windows uniquement)
3. Envoi direct d'e-mails par l'utilisateur final

Complément d'envoi sécurisé d'e-mails Cisco

Le complément d'envoi sécurisé d'e-mails Cisco prend en charge Microsoft Outlook pour Windows, Mac et Web. Reportez-vous à Configuration prise en charge pour le complément Cisco Secure Email Encryption Service et le complément Cisco Secure Email Subvention » dans la [matrice de compatibilité pour Cisco Secure Email Encryption Service](#) pour garantir la compatibilité de votre version d'Outlook.

Veillez consulter le [complément d'envoi sécurisé de courrier électronique Cisco](#) pour obtenir de la documentation sur le téléchargement et l'installation.

Plug-in de sécurité de la messagerie Cisco

Le plug-in de sécurité de la messagerie Cisco prend uniquement en charge Microsoft Outlook sous Windows. Reportez-vous à la section « Configurations prises en charge pour le plug-in de signalement de courrier électronique Cisco » dans la [matrice de compatibilité pour le service de cryptage de courrier électronique sécurisé Cisco](#) afin d'assurer la compatibilité de votre version d'Outlook.

Note: Les anciennes versions du plug-in sont nommées « Plug-in de sécurité du courrier électronique IronPort » ou « Plug-in de chiffrement pour Outlook ». Cette version du plug-in contenait à la fois Reporting et Encryption. En 2017, Cisco a séparé les services et publié deux nouvelles versions du plug-in, « Email Reporting Plugin for Outlook » et « Email Encryption Plugin for Outlook ». Celles-ci étaient disponibles avec une version 1.0.0.x.

Envoi direct par e-mail

Suivez les instructions fournies pour votre client de messagerie afin de joindre l'e-mail en tant que pièce jointe codée [RFC 822](#) Multipurpose Internet Mail Extension (MIME). Si l'un des exemples ne reflète pas votre client de messagerie, reportez-vous directement au guide d'utilisation ou à l'assistance produit de votre client de messagerie et vérifiez que le client de messagerie prend en charge le transfert en tant que pièce jointe.

Veillez envoyer les envois par e-mail à l'adresse e-mail appropriée :

spam@access.ironport.com	L'utilisateur final considère que le courrier indésirable ou la ligne d'objet contient [SUSPECTED SPAM].
ham@access.ironport.com	L'utilisateur final NE considère PAS le message comme du spam. La ligne d'objet contient [SUSPECTED SPAM], ou la ligne d'objet inclut des balises supplémentaires.
ads@access.ironport.com	L'utilisateur final considère que le message électronique contient ou contient du contenu marketing ou des messages grisés, ou la ligne d'objet inclut [MARKETING], [RESEARCH], [SOCIAL] ou [BULK].
not_ads@access.ironport.com	L'utilisateur final NE CONSIDÈRE PAS le message électronique comme étant du contenu marketing ou de la messagerie grise, ou la ligne d'objet contient [MARKETING], [RESEARCH], [SOCIAL] ou [BULK].

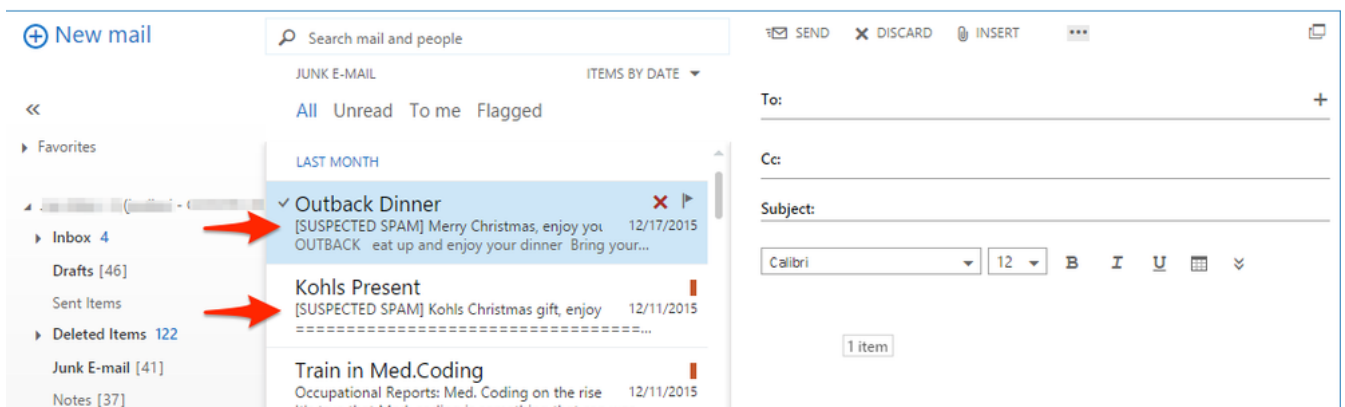
phish@access.ironport.com

virus@access.ironport.com

Le message électronique semble être un message de phishing (conçu pour acquérir plusieurs nom(s) d'utilisateur, mots de passe, informations de carte de crédit ou autres informations d'identification personnelle), ou le message électronique contient des pièces jointes de programmes malveillants (de même, conçu pour acquérir un ou plusieurs nom(s) d'utilisateur ou mots de passe). La ligne d'objet est précédée de [SPAM SOUPÇONNÉ], [Fraude \$menace_category possible] ou d'une ligne similaire. L'utilisateur final considère le message électronique ou une pièce jointe comme viral, la ligne d'objet contient [AVERTISSEMENT : VIRUS DÉTECTÉ].

Toutes les lignes d'objet ne contiennent pas de texte et de balises supplémentaires. Pour connaître vos paramètres, consultez la configuration de la passerelle de messagerie sécurisée Cisco ou de la passerelle cloud pour les filtres anti-spam, anti-virus, Graymail et contre les attaques, ou contactez votre administrateur de messagerie pour toute question.

Exemple de lignes d'objet marquées :



Avertissement : Ne transférez pas votre message électronique comme envoi. Cette action ne conserve pas l'ordre des en-têtes de routage de courrier et supprime les en-têtes de routage de courrier nécessaires pour attribuer l'origine de l'e-mail. Au lieu de cela, assurez-vous toujours d'envoyer l'e-mail en question via l'option « transfert en pièce jointe ».

Vous pouvez envoyer un e-mail directement à partir de :

- Microsoft Outlook
- Microsoft Outlook Web App, Microsoft Office 365
- Microsoft Outlook 2011 et Microsoft Outlook 2016 pour Mac (OS X, macOS)
- Courrier (OS X, macOS)
- Thunderbird Mozilla
- Plates-formes mobiles (iPhone, Android ou autre)

Microsoft Outlook

- La méthode d'envoi préférée de Microsoft Outlook est d'utiliser le complément d'envoi de courrier électronique sécurisé Cisco.
- Envoyez des messages à Cisco pour les courriels non sollicités et indésirables, tels que le spam, les virus et le phishing.
- Le bouton Not Spam permet de reclasser rapidement les messages électroniques légitimes marqués comme spam.

Note: Suivez les instructions suivantes si vous ne pouvez pas ou préférez ne pas installer le plug-in de sécurité de la messagerie Cisco.

Microsoft Outlook Web App, Microsoft Office 365

1. Ouvrez votre boîte aux lettres dans Microsoft Outlook Web App.
2. Sélectionnez le message à envoyer.
3. Cliquez sur « Nouveau courrier » en haut à gauche.
4. Faites glisser le message et déposez-le en tant que pièce jointe au nouveau message.
5. Envoyez le message électronique à l'adresse respective indiquée dans ce document.

Microsoft Outlook 2011 et Microsoft Outlook 2016 pour Mac (OS X, macOS)

1. Sélectionnez le message dans le volet des messages.
2. Cliquez sur le bouton Pièce jointe.
3. Transférez le message à l'adresse correspondante fournie dans ce document.

Courrier (OS X, macOS)

1. Cliquez avec le bouton droit de la souris sur le message électronique lui-même et choisissez **Transférer en tant que pièce jointe**.
2. Transférez le message électronique à l'adresse correspondante fournie dans ce document.

Thunderbird Mozilla

1. Cliquez avec le bouton droit de la souris sur l'e-mail lui-même et choisissez **Forward As > Attachment**.
2. Transférez le message électronique à l'adresse correspondante fournie dans ce document.

Note: [MailSentry IronPort Spam Reporter](#) est un plug-in tiers pour Mozilla Thunderbird qui

effectue la même action que celle décrite mais fournit un bouton « Spam/Ham ». MailSentry IronPort Spam Reporter n'est pas un plug-in pris en charge par Cisco.

Plates-formes mobiles (iPhone, Android ou autre)

- Si votre plate-forme mobile ne dispose pas d'une méthode pour transférer l'e-mail d'origine en tant que pièce jointe, veuillez l'envoyer une fois que vous avez accès à l'une des autres méthodes fournies.

Comment vérifier les envois à Cisco

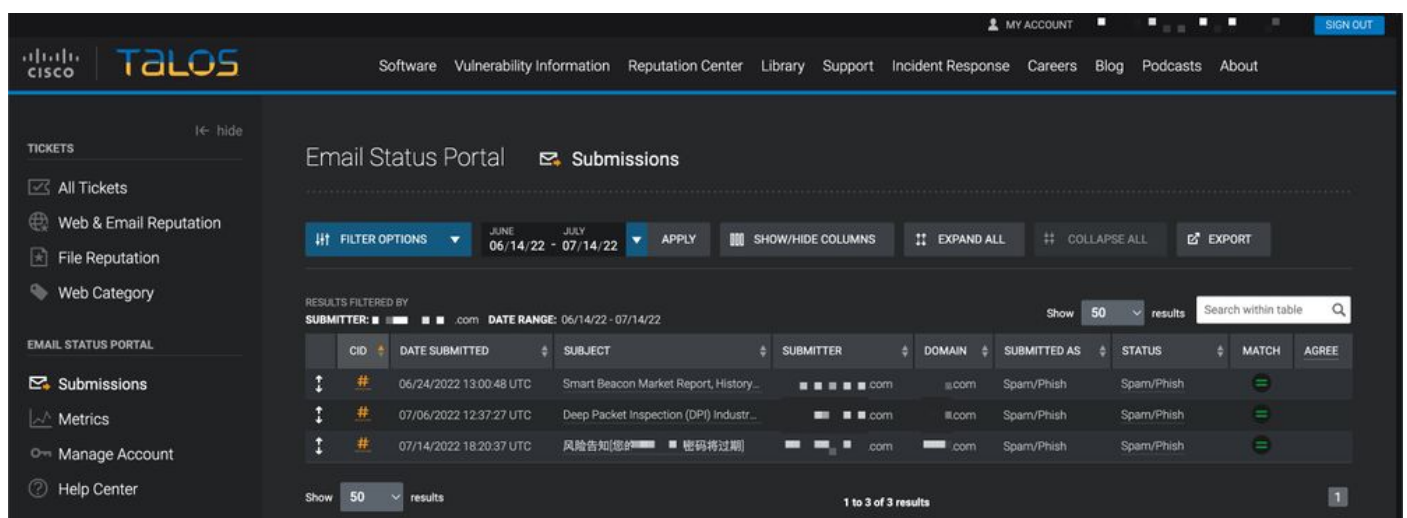
Envoi direct par e-mail

Cisco ne fournit pas d'e-mail de confirmation ni d'avis de réception pour les envois par e-mail. Au lieu de cela, consultez vos envois via le portail d'état des e-mails hébergé sur Talosintelligence.com.

Portail d'état de la messagerie

Veillez valider vos envois à partir du portail d'état des e-mails. Après vous être connecté, une liste de tous vos envois se trouve dans la plage de dates/heures spécifiée.

Exemple :



The screenshot shows the Talos Email Status Portal interface. The main content area displays a table of email submissions with the following columns: CID, DATE SUBMITTED, SUBJECT, SUBMITTER, DOMAIN, SUBMITTED AS, STATUS, MATCH, and AGREE. The table is filtered by date range (06/14/22 - 07/14/22) and shows 3 results. The first row has a unique CID starting with '#'. The interface also includes a sidebar with navigation options like 'All Tickets', 'Web & Email Reputation', and 'File Reputation', and a top navigation bar with links to 'Software', 'Vulnerability Information', etc.

CID	DATE SUBMITTED	SUBJECT	SUBMITTER	DOMAIN	SUBMITTED AS	STATUS	MATCH	AGREE
#	06/24/2022 13:00:48 UTC	Smart Beacon Market Report, History...	com	com	Spam/Phish	Spam/Phish		
#	07/06/2022 12:37:27 UTC	Deep Packet Inspection (DPI) Industr...	com	com	Spam/Phish	Spam/Phish		
#	07/14/2022 18:20:37 UTC	风险告知(您的密码将过期)	com	com	Spam/Phish	Spam/Phish		

Si vous cliquez sur l'unique CID "#« , vous pouvez voir d'autres détails associés à l'e-mail signalé.

The screenshot displays the Cisco Talos Email Status Portal interface. At the top, there is a navigation bar with the Talos logo and various menu items like 'Software', 'Vulnerability Information', 'Reputation Center', etc. The main content area is divided into several sections:

- TICKETS:** A sidebar on the left with options like 'All Tickets', 'Web & Email Reputation', 'File Reputation', and 'Web Category'.
- Email Status Portal:** The main header area with 'Submissions Information' and a unique ID: #cidG50062dHbf1nKacdo64RoaxbMFmpTopF.
- Submission Details:** A table showing 'Date Submitted' (Jul 14, 2022 7:04 PM), 'Subject' (风险告知[您的] = '密码将过期'), 'Submitted As' (Spam), 'Status' (Spam), and 'Match' (green bar).
- Observables:** A section with a button 'INVESTIGATE OBSERVABLES IN SECUREX'. It contains two tables:

Sender Domain				Sender IP	
DOMAIN	REPUTATION	CONTENT CATS	THREAT CATS	IP ADDRESS	EMAIL REPUTATION
huateng.com	Neutral			2603:10b6:408f6:15	Unknown
- Embedded URLs:** A table with columns for 'URLS', 'REPUTATION', 'CONTENT CATEGORIES', and 'THREAT CATEGORIES'. It shows one entry: 'http://adarx.com.cn/page.php' with a 'Questionable' reputation.
- Embedded Attachments:** A table with columns for 'FILE NAME', 'SHA256', 'REPUTATION', and 'FILE SIZE'. It displays the message 'No attachments were found in this submission'.

Le domaine de l'expéditeur, l'adresse IP de l'expéditeur, les URL intégrées et les pièces jointes intégrées sont associés à l'e-mail signalé. Vous pouvez prendre d'autres mesures avec **Réputation Web des litiges**, **Réputation par e-mail des litiges** et **Réputation des fichiers de litiges**.

Chaque ligne d'informations imbriquées affiche un maximum de 5 observables d'URL incorporées et de pièces jointes incorporées. Si un envoi par e-mail comporte plus d'observables, un utilisateur peut cliquer sur 'Accéder à la page Détails de l'envoi par e-mail' pour voir la liste complète des observables extraits.

Vous pouvez rechercher d'autres détails de réputation d'un seul observable avec l'observable désiré, puis cliquez sur le bouton 'Centre de réputation'.

Vous pouvez également étudier plusieurs observables via [SecureX](#). Ce tableau de bord combine les données de réputation de la suite complète de produits Cisco Secure en fonction de votre gamme de produits Cisco. Vous pouvez sélectionner jusqu'à 20 observables dans une seule soumission pour une enquête dans SecureX à la fois avec le bouton 'Investigate observables in SecureX'.

Les utilisateurs peuvent déposer un seul litige de réputation (Web, e-mail ou fichier) ou appliquer des litiges en bloc pour un ou plusieurs de ces litiges sur une soumission. Les URL et les domaines peuvent également faire l'objet de litiges de catégorisation Web.

Pour plus d'informations sur le portail d'état des e-mails :
https://talosintelligence.com/tickets/email_submissions/help

Additional Information

Documentation relative à la passerelle de messagerie sécurisée Cisco

- [notes de version](#)
- [Guide de l'utilisateur](#)
- [Guide de référence CLI](#)
- [Guides de programmation API pour Cisco Secure Email Gateway](#)
- [Open Source utilisé dans Cisco Secure Email Gateway](#)
- [Guide d'installation de Cisco Content Security Virtual Appliance](#) (inclut la passerelle virtuelle de cloud)

Documentation de la passerelle de messagerie sécurisée

- [notes de version](#)
- [Guide de l'utilisateur](#)

Documentation relative à Cisco Secure Email and Web Manager

- [Notes de version et matrice de compatibilité](#)
- [Guide de l'utilisateur](#)
- [Guides de programmation API pour Cisco Secure Email and Web Manager](#)
- [Guide d'installation de Cisco Content Security Virtual Appliance](#) (inclut Virtual Email et Web Manager)

Documentation relative aux produits Cisco Secure

- [Architecture de nommage de portefeuille Cisco Secure](#)