# NextGen Email Security

The NextGen Email Security tool (powered by Sophos) is continuously working to block potential spam emails for you throughout the day. The following day you will receive an email listing the quarantined messages for your review. You also have the option to log into your Self-Service account, where you can view your quarantined messages and manage the allow/blocklists.

#### Self Service Account Setup

You will receive an email invite to access your self-service account. Once set up, you can log in by navigating to <u>https://central.sophos.com/manage/self-service</u> or the MNP Digital Service Portal.

Below is what you'll see once you log in.



## **Manage Quarantined Emails**

The Quarantine consists of emails identified as potential spam. You can review these messages and either **'Release'** or **'Delete'** them. Releasing a message delivers it to your inbox. Below are the instructions on how to use the Quarantine.

## 1. Click on Quarantine

The Quarantine displays a list of your emails that have been identified as potential spam. The sender, recipient, subject, time and date are shown for each email.



2. Select a subject to view the quarantined email message and choose whether you want to **Release** or **Delete** it.

Note: Quarantined messages are deleted after 30 days.

#### Allow/Block

You can manage which email addresses and domains are allowed or blocked using Allow/Block.

1. Click on Allow/Block.

Allow/Block displays a page to add email addresses or domains you want to allow or block. If you have already added some, a list is displayed. You can filter your results by using the **Search** field.



**Note:** Only personal items added though your self-service account are displayed here. Company-wide allows/blocks will not be shown in your self-service account.

2. Click **Add** to display a dropdown menu that will show the **Add** and **Block** options. Select the action you want to take.

SOPHOS () SELT BERVICE PORTAL	Allow/Block Email / Allow/Block		Help • Chris Ippolito • MANP Hero Dusta
<ul> <li>Email</li> <li>Emergency Inbox</li> <li>Device Encryption</li> </ul>	3 All Allowed & Blocked	3 Allowed	0 Blocked
D Mobile	Search Q Action		Add v Delete Creates on Add allow
	Allow	noreply@idagent.com	Jul 29, 2020
	Allow	nations@e.connectwise.com	Jun 24, 2020
	Allow	no-reply@zoom.us	Mar 23, 2020
	4	1 - 3 of 3 < >	÷

A window will appear with a text box where you can add the email address or domain.

3. Add the email address or domain. You can also override duplicate entries by ticking the **Override duplicates** box.

If you add the same email address or domain to both the allow and block lists, Override duplicates will be based on the most recent option you choose.

Add allow		×	
Email address or domain *			
i.e. example.com, name@example.com. Wildcards are not supported. Override duplicates ④			
	Cancel	Save	

4. Click Save to confirm your choice. Click Cancel if you do not want to save the settings.

**Note**: The spam detection function will not be carried out for email addresses and domains on your selfservice account **Allow** list.

5. If you want to delete addresses or domains from the add or block list, select the items from the list and click Delete.

SOPHOS (	Allow/Block Email / Allow/Block		Help - Chris Ippolito - MNP
Ernail Ernergency Inbox	3 All Allowed & Blocked	3 Allowed	0 Blocked
D Mobile	Search Q		Add 🛩 🛛 Delete
	Action	♦ Address/Domein	Created on ~
	Allow	noreply@idagent.com	Jul 29, 2020
	Allow	nations@e.connectwise.com	Jun 24, 2020
	Allow	no-reply@zoom.us	Mar 23, 2020
	4	1-3 of 3 < >	

A window will appear with the list of email addresses that you chose to delete. To confirm your selection, click Delete, otherwise click Cancel.

## **Emergency Inbox**

The Emergency Inbox may be used when you cannot access your email client (e.g. Outlook or Gmail). Suppose there's an outage affecting access to your email service provider, such as Microsoft 365 or Google Workspace. In that case, you can log into your NextGen Email Security self-service account and view your Emergency Inbox. The Emergency Inbox will hold all incoming emails until the service is restored. Meaning you could view any critical emails you're waiting for even though your email service provider is down.

	Emergency Inbox View and manage your email from the last 14 days				Help 👻	Chris Ippolito 👻	MNP
🖂 Email							Next Digital
Emergency Inbox	Search emeils Q						
Device Encryption	FROM 🐨	SUBJECT	RECEIVED 🔺	SIZE 🔻			
Mobile							
			You currently do not have any mes	sages.			

## **Device Encryption and Mobile**

Device Encryption and Mobile functions are used if your organization leverages device management powered by Sophos.

With **Device Encryption**, you can retrieve a recovery key to unlock your computer when you have forgotten your logon password (BitLocker PIN, password, USB key, or macOS password).

With Mobile, you enroll your device with Sophos Mobile.

You can also remotely locate, lock or wipe your devices and reset your password without having to contact the helpdesk.

	Email Security Manage quarantized messages and email security settings	Help - Christppolito - MNP
Email     Emergency labox     Device Encryption     Mobile	Quarantine(0) Manage messages in your Quarantine. Quarantined messages are held up to 30 days before they are deleted.	Allow/Block Manage email addresses/domains in your allow and Mock list. Email addresses/domains marked as allow will not be quarantimed. Anything you mark as block will be detend.
	Distribution Lists Quarantine (0) Manage distribution list messages marked as spam in your Quarantine. Quarantine messages are held up to 30 days before they are deleted.	

#### NextGen Email Security – Smart Banners

Smart Banners will display at the top of inbound email messages to show if the email is trusted. Email recipients can add senders to their **Allow** and **Block** lists from within the email.

Trusted: This banner is green. It shows that the email sender is in the allowed list and passed verification.

This sender is trusted.

**Unknown**: This banner is yellow. It shows that email sender is outside your organization and didn't fail verification.

Caution! This message was sent from outside your organization.

Allow sender | Block sender

**Untrusted**: This banner is orange. It shows that the email sender is outside your organization and failed verification.



#### NextGen Email Security – Sender Checks

Sender Checks are used to verify the authenticity of an email's origin.

When an email is received, it looks at the address of the sending mail server. If this check fails, the Subject line of the email will include the following prefix:

[CAUTION: SUSPECT SENDER]

This prefix indicates that the email could not be from whom it says it is. Before responding to the email, you should verify that it is authentic.

## Additional Resources

Please visit <u>https://www.mnp.ca/en/cx-knowledge-base</u> for additional resources such as how to request support.