Haven™ Managed Security Services Deployment Guide

NOTE: Actual services may vary depending on service agreement.

Haven™ Onboarding

Project Definition

The purpose of this project is to implement Haven within your organization to enable your company to maintain normal business operations while being continuously protected from the ever-evolving cybersecurity threat landscape.

Business Case

As technology has evolved, businesses have become reliant on various technologies and platforms to successfully operate and communicate. This reliance on technology results in businesses inheriting vulnerabilities that are continuously exploited, exposing them to the risk of full business compromise.

To successfully defend against these threats and evolve as a company, it is critical that a successful cybersecurity framework be employed to reduce the risk of being attacked. This is done by installing the correct technology, establishing proven processes, and having security experts constantly monitoring and improving framework adherence.

Project Description

Haven utilizes best-in-class technologies, processes, and people to ensure that your business minimizes the risk of being compromised. Haven provides security technology management, 24x7 monitoring, and expert professional support to increase the security of your operations and business as a whole.

Project Approach

Corvid Cyberdefense (CCD) follows an established installation methodology to ensure Haven is optimized for each Client environment. As an overview, there are five stages to a standardized Haven approach:

Project Kick-Off

The Client Sales Representative will notify the CCD Implementation Team to schedule a project kick-off call with contacts you identify from your organization. Prior to the kick-off call, you will receive a Haven In-take form to complete that will provide us the relevant information about your organization and IT environment. We will review the intake form during the initial call to answer any open questions, followed by a Haven deployment schedule. If the contacts from your organization are largely non-technical and you utilize an IT Managed Service

Provider, we recommend including them on the initial call to ensure all technical information is accurately provided.

After the kick-off call the following will be provided to you, including:

- **End-User Guide** – for distribution to your employees, detailing what to expect and including an overview of changes that will happen at the end-user or employee level
- **Email Templates** – templated communications for you to distribute to your end-users or employees for proactive notifications regarding upcoming changes.

Build

During the Build stage, the Implementation Team will begin the custom build-out of the Haven network appliance. An on-site visit may be conducted to confirm the appliance's physical installation location and to provide the Implementation Team an opportunity to identify any network anomalies that could impact or complicate installation. Once the appliance is built and reviewed, it will be delivered to you for installation. All security cloud tenants and install packages will be prepared for later installation.

Install

The various Haven security technologies are installed in your environment during the Install stage. The network appliance, endpoint agent, and secure email gateway will be installed on a semi-staggered schedule to limit any disruption to the business environment. Typically, the endpoint agent is deployed first, followed by the network appliance, and finally the secure email gateway. Depending on your organization's priorities, alternate installation options are available. Typical installations are done during business hours with minimal impact, but given the potential for unforeseen issues to occur, out-of-hours installations are available upon request.

Review

During the review stage all of the Haven solution components are analyzed for initial security findings and recommendations. This ensures there are no previously existing security events of significant interest that go unnoticed and identifies potential technology tuning requirements to support your unique business environment. Throughout the Review process, security policies are optimized and applied to prevent security events, such as access to malicious internet sites, active hacking tools on your workstations and servers, or malicious phishing emails. Following the review of events and policies, you will move to the project Close-Out phase and introduced to the Corvid Cyberdefense Security Operations Center (SOC) for on-going monitoring and management.

Close-Out/Security Operations

Post installation, the Security Operations Center (SOC) Team will become your daily contact point for help or change requests) delivering continuous monitoring and reporting on detected threats. The SOC Team will work to maintain a hardened environment by analyzing network and host activity, such as network traffic by geographic origin, application type, and workstation behavior. Your primary contact will transition from the Engagement Manager to the Director of Security Operations. You will need to identify a group of trusted

individuals in your organization who will have the authority to agree to changes and make change requests, such as website and application exclusions.

Along with regular reporting, the SOC will provide additional ad hoc reporting, communicate updates, and significant policy changes within your security environment to maintain a preventative security posture. Communications will be sent to the internal primary contact at your organization. This individual will be required to authorize larger policy changes and work with the SOC Team to determine the potential change impact and provide change requests based on SOC report recommendations.

Installation Overview

The following section highlights the Haven installation process for the named technologies.

Endpoint Security | Cylance

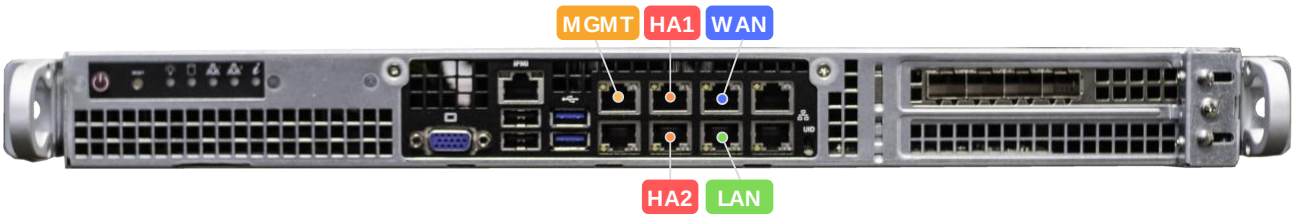
CylancePROTECT and OPTICS for endpoint prevention and detection and response leverages machine learning data models to detect and prevent execution of malicious code on workstations and servers. CylanceOPTICS provides deeper system visibility to understand what is happening on a system prior to an attack is detected and allows the SOC Team to deploy updated detection rules based on evolving attack vectors, which can be used to identify a potential attack before it is carried out.

Depending on the Operating Systems in your environment, the Security Operations Center will create Cylance installers and share them via a web link to the central cloud share. Deploying the agent is very easy and can be distributed using Active Directory Group Policy or other centralized management tools. Specific deployment options will be identified during the initial onboarding. Once Cylance has been deployed a series of follow up reviews will be performed over the next 7-14 days. This will allow various policy rules and exclusions to be created based on your goals and the specifics of your IT environment.

Network Security/Haven Appliance | Palo Alto Networks

The Palo Alto Networks Firewall is a next-generation firewall with advanced network security capabilities and cloud sandbox analysis for potentially malicious files that are detected traversing your network.

Depending on the complexity of the network, the installation of the Haven appliance can vary. The following diagram illustrates the setup for an appliance that is in High Availability.



To install the appliance the following steps are advised:

1. Rack and power up the appliance
2. Connect port 0 MGMT to the internal switch
    a. This will enable the device to call home
3. Connect devices via port 2 HA1 and 3 HA2 to enable HA

The following stage will cause a brief network outage.

4. Connect WAN to port 4 WAN
5. Connect LAN to port 5 LAN
6. Conduct connectivity testing

Once the network appliance is installed, Corvid will begin running a series of network vulnerability scans across your network. Network vulnerability scanning is used to proactively identify missing patches, out of date software and misconfigured services that could be exploited by an attacker. OpenVAS is used for vulnerability scanning and will be deployed in three phases:

1. Discovery Scan – identifies network connected assets and systems
2. Partial Scan – identifies externally visible vulnerabilities and system information
3. Full Scan – performed using an authenticated account for deeper system visibility and analysis

Network Security | Palo Alto Networks GlobalProtect VPN

Corvid Cyberdefense (CCD) will deploy a VPN (virtual private network) agent that will route user network traffic through a cloud-based firewall, referred to as the Haven Cloud. CCD will work with the organization to create a hardened security posture that allows pre-approved applications, websites, and/or specific website categories to be accessible in the environment to reduce risk to the organization.

Corvid Cyberdefense has a standard firewall security policy assigned to all clients. However, you may request custom rules or applications to be allowed in your organization. Please inform CCD if any unique exclusions are required. The SOC Team continuously updates our rules based on emerging threats that are seen in the wild.

There are two options for how the GlobalProtect VPN agent is configured:

1. Always on VPN
   - Users cannot disconnect the VPN agent, which is more secure.
   - Recommended deployment method for company managed workstations.
2. On-demand VPN
   - Users can disconnect the VPN agent, which is less secure.
   - Recommended deployment method for Bring Your Own Device (BYOD).

Email Security | Mimecast

The Haven e-mail security solution is powered by Mimecast. Mimecast provides email security controls designed to protect end users from advanced threats and attacks. Mimecast provides:

- Enhanced security with spam and phishing detection
- Analysis of URLs and attachments for vulnerabilities or threats
- Ability to easily send encrypted emails containing sensitive information

Based on the information provide in the intake form Corvid Cyberdefense will initially stand up a tenant for the primary email domain. Once complete, Corvid Cyberdefense will need access to the DNS records and an administrator account that can add email routing rules. If an administrator account cannot be provided, your IT Support team will need to assist Corvid Cyberdefense during the deployment and implement the necessary changes.

To deploy Mimecast the following steps are taken:

1. Add a TXT file to the DNS records

   a. This will allow Mimecast to confirm ownership of the domain
2. Add users to the domain
   a. This will allow users to be able to log into their Mimecast accounts. This does not change how email currently flows
3. Update DNS records
   a. Change MX and SPF records to have all emails sent to Mimecast. This will initiate email flow changes
4. Add inbound and outbound routing in email host. This will be the final change impacting your email flow to Mimecast

At this point all email traffic will flow through Mimecast. Initial email policies are applied to prevent known threats and additional policies will be applied once mail traffic flow is analyzed. This phased approach will ensure any negative impact to email is minimized.

Education | Symbol Security

Once all security tools are installed Corvid Cyberdefense will use the email addresses added to Mimecast to deliver monthly training videos and simulated phishing campaigns. It is advised to have an internal point of contact within your organization to collaborate and approve training videos and email templates.

Monthly Training Videos

Employees will receive an email with a link to access training videos that were created to be short, entertaining, and educational. A few start-up episodes were selected that teach about core threats like phishing, ransomware, and password security. Episodes are 3-4 minutes in length and they teach a lesson on one specific security threat using a real-life security breach as the story line. Every month, users will receive an email to let them know that a new video episode is available.

Monthly Simulated Phishing Campaigns

Because so many data breaches originate from a phishing email, we'll be sending occasional simulated spoofed (fake) emails designed to test employee awareness of a true phishing email. These spoofed emails will not reveal any sensitive information, but will provide an idea of where improves in employee training are needed. When a user clicks within a simulated phishing email, that person will be automatically prompted to watch a video on the subject of identifying a phishing email.

As our main POC (point-of-contact) you will receive by-user participation and performance reports.

Appendix A - Network Security Solution – Palo Alto Networks

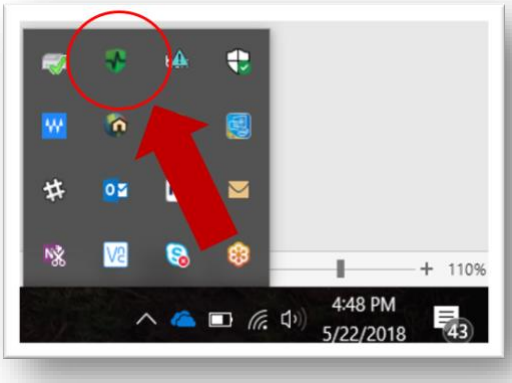
The Network Security Solution is comprised of a next-generation firewall that examines all traffic coming in and out of your organization's network. Corvid Cyberdefense works with your IT team to create sets of policies to allow or deny specific types of traffic (for example, blocking web traffic categorized as gambling or pornography). In addition to examining and filtering web traffic, the firewall can examine and manage computer applications and devices connected to your network. Web traffic analysis happens behind the scenes. Typically, the only time a user will be made aware of the firewall is if an attempt is made to access a blocked website, in which case an error page similar to the example below will be displayed. If your organization believes a website has been blocked in error, you can notify Corvid Cyberdefense Support who will investigate and resolve if the site is deemed safe or a false positive.

Appendix B - Endpoint Security Solution | CylancePROTECT & CylanceOPTICS

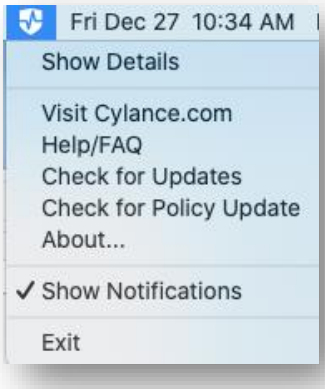
In the event a threat or malware goes undetected by the Network and/or Email Security Solutions, it is likely it will attempt to access a protected endpoint in your organization, which is protected by our Endpoint Security Solution powered by Cylance. CylancePROTECT is a next-generation anti-virus solution that utilizes machine learning to identify and block malware, such as ransomware, malicious scripts, and other advanced threats. Leveraging machine learning algorithms allows Cylance to identify threats before being seen in the wild, which are often referred to as “zero-day” threats.

CylanceOPTICS is a detection and response add-on to CylancePROTECT that is critical for threat hunting, identifying and alerting on potentially malicious activity, and functioning as a flight recorder that captures endpoint actions leading up to a Cylance quarantined event.

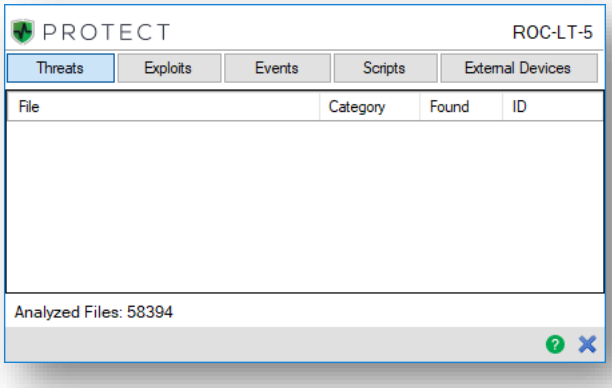
Once installed, the Cylance agent will run in the background. When the Cylance agent is running an icon and any related alerts can be displayed by clicking on the Cylance shield icon in the system tray shown right.



For MacOS users, the icon can be found in the notification bar, shown below.



In the event Cylance blocks a malicious file it will be listed in the Event panes inside the agent details. If a file is believed it to be blocked in error, notify Corvid Cyberdefense to investigate the file and take the appropriate action.



Appendix C - E-mail Security Solution Set-Up | Mimecast

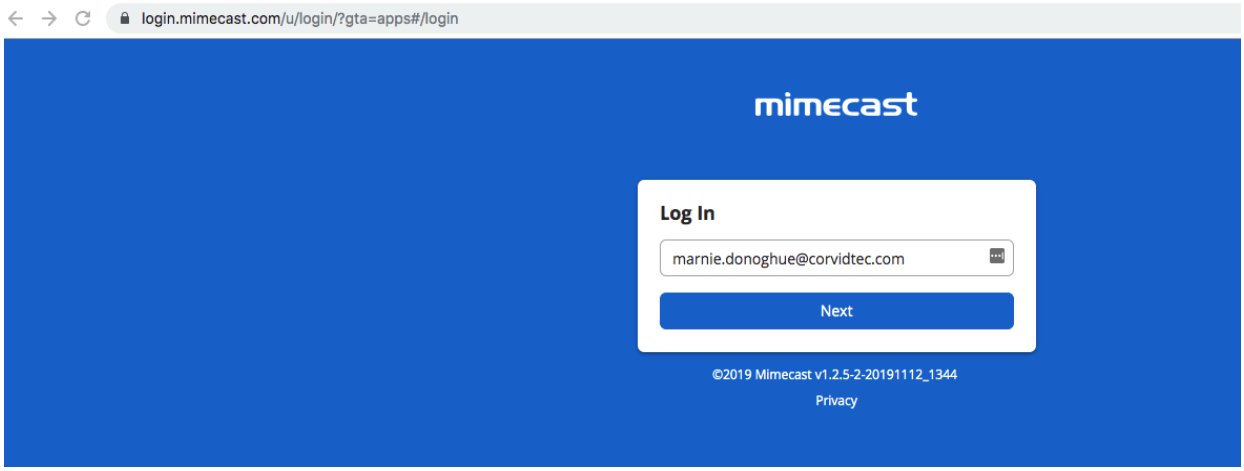
The Haven E-mail Security Solution is powered by Mimecast. Mimecast provides email security controls designed to protect end users from advanced threats and attacks. Mimecast provides:

- Enhanced security with spam and phishing detection
- Analysis of URLs and attachments for vulnerabilities or threats
- Ability to easily send encrypted emails containing sensitive information
- Employee training and awareness

Mimecast Activation

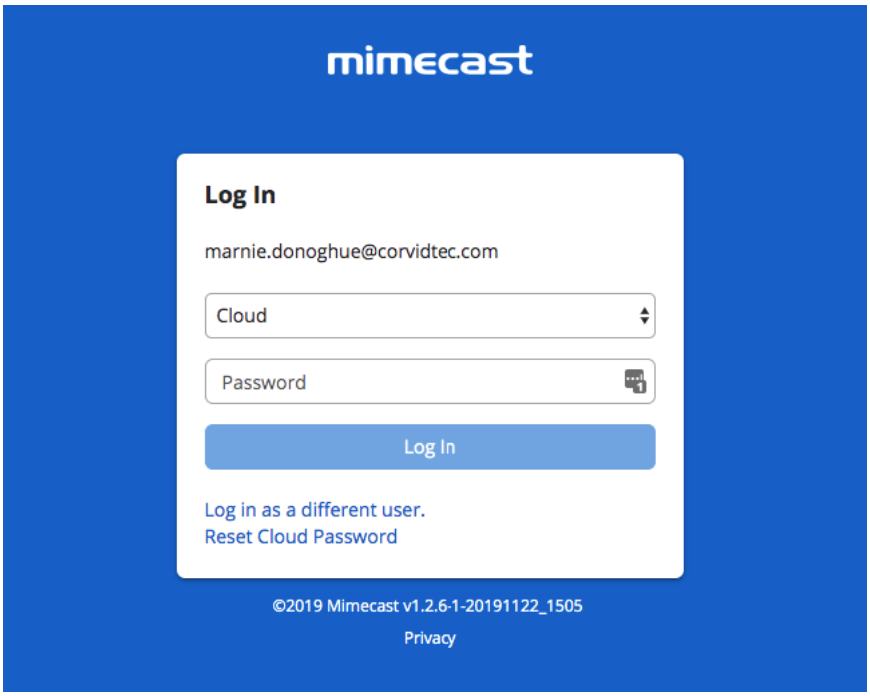
Corvid Cyberdefense will work with your organizations Point-of-Contact to create user Mimecast accounts. Alternatively, the following process can be used to activate individual Mimecast accounts after receiving an email notification:

1. Go to https://login.mimecast.com. This is the Mimecast Personal Portal. ***We recommend bookmarking this webpage in your browser.***

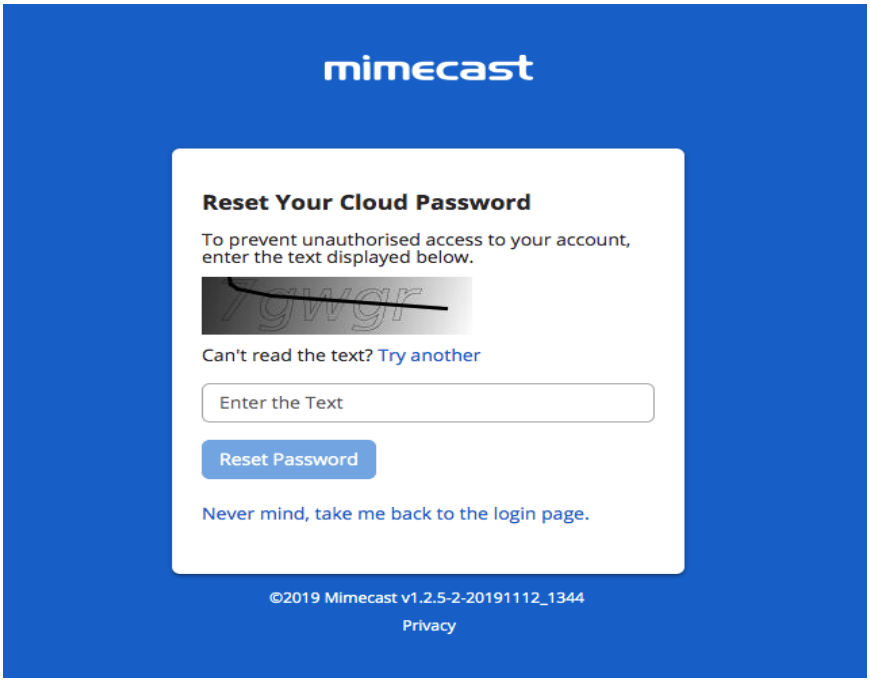


2. Enter your email address and select “Next.”

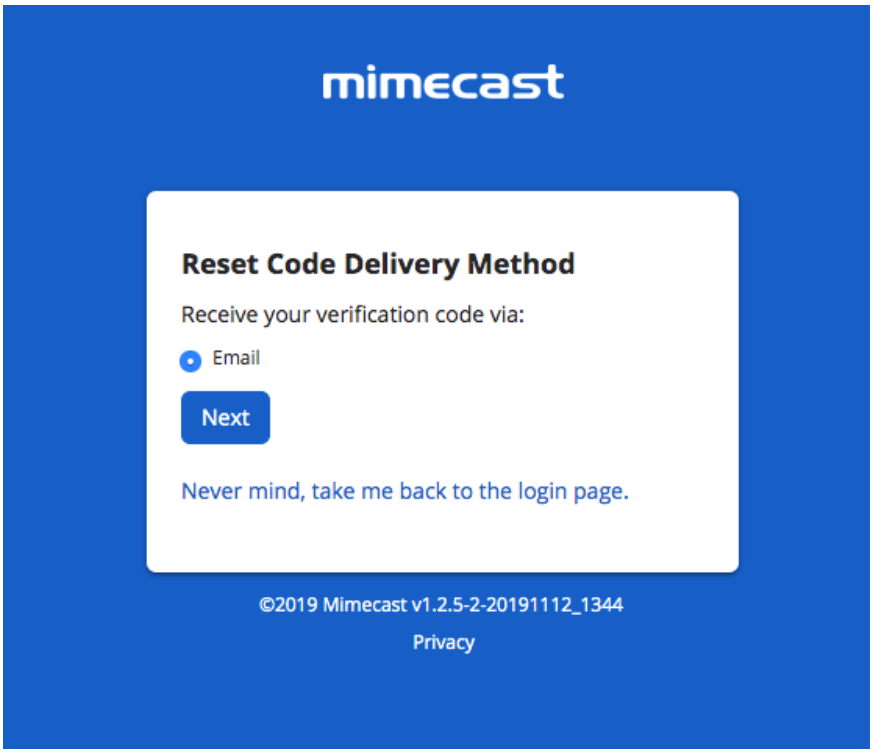
3. Below the “Log In” button, select the option “Reset Cloud Password.”



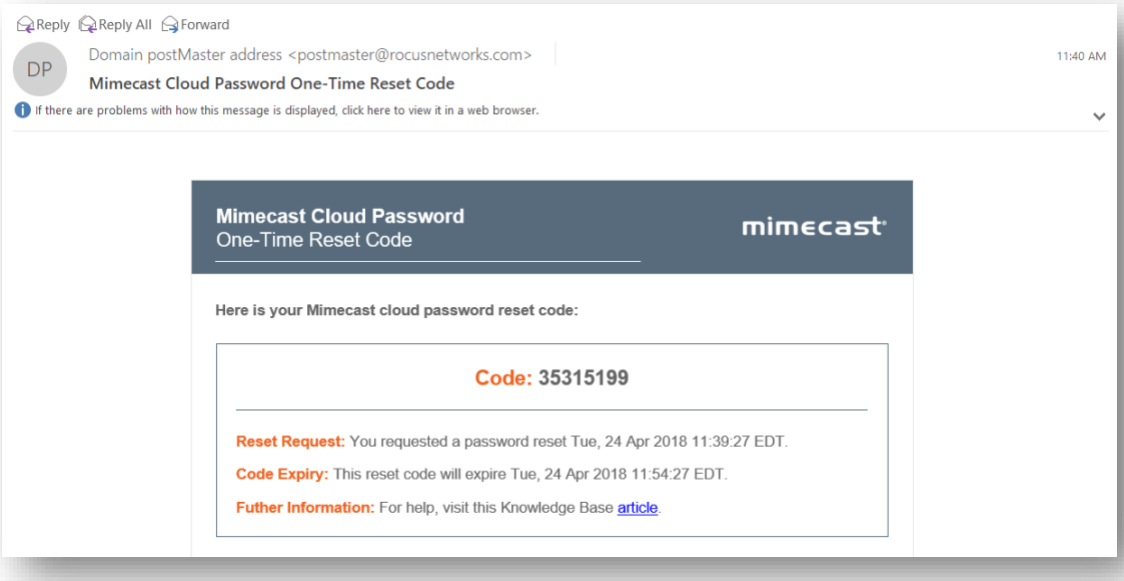
4. Enter the Captcha text for security purposes and select “Reset Password.”



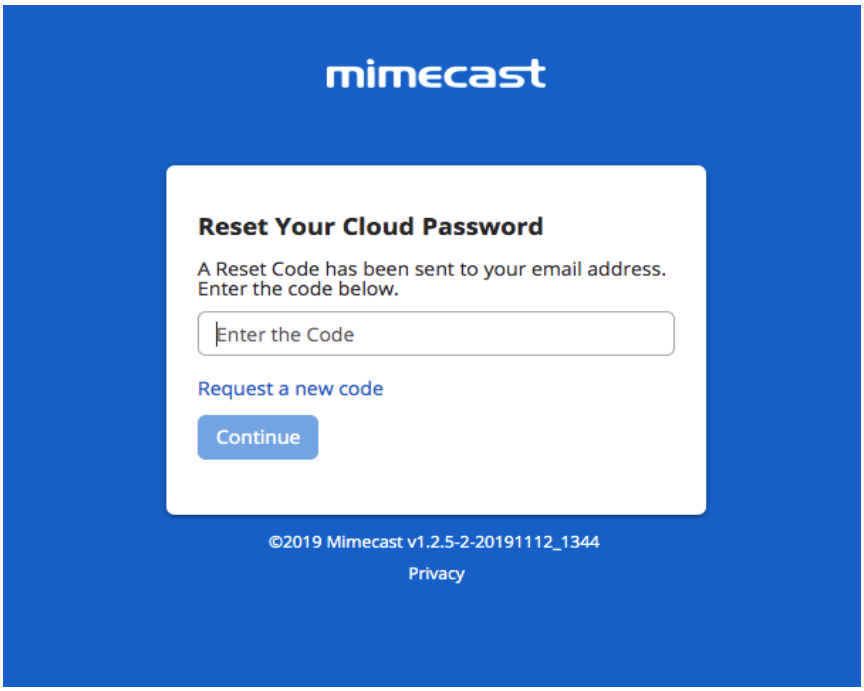
5. Select the password reset link delivery method. Generally, “Email” should be the only option available and the default selection. Select “Next” to continue.



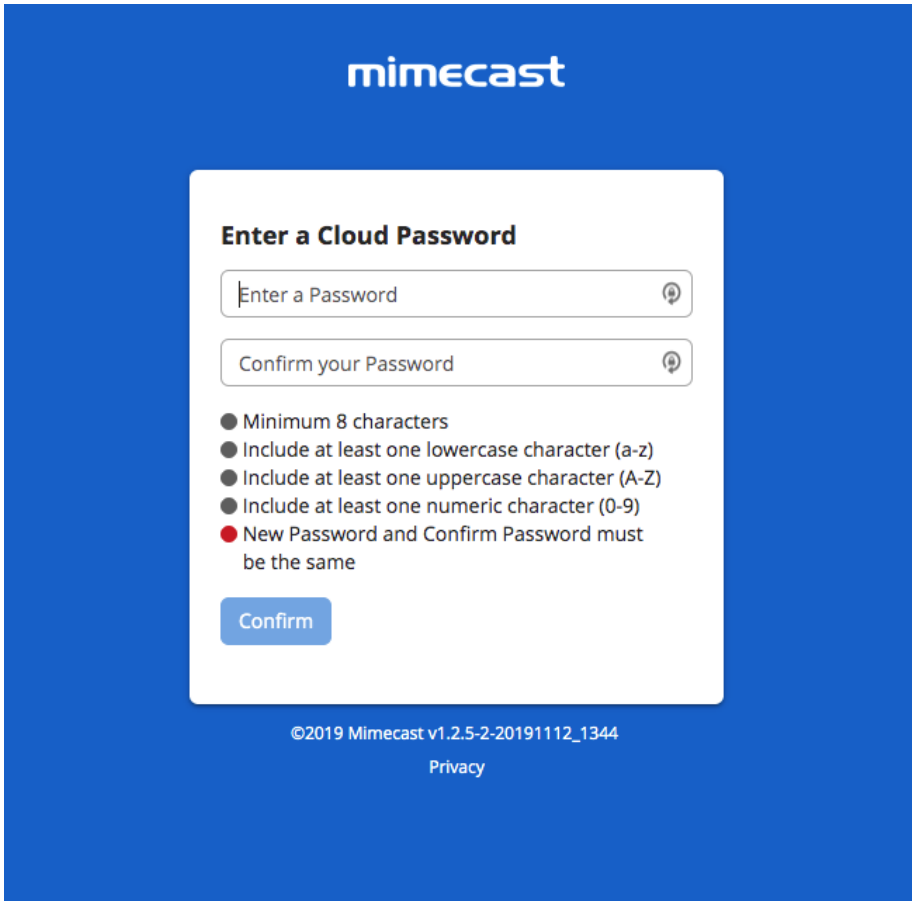
6. An email from sender “Mimecast Domain Postmaster” will be delivered to the user mailbox with a one-time password reset code.



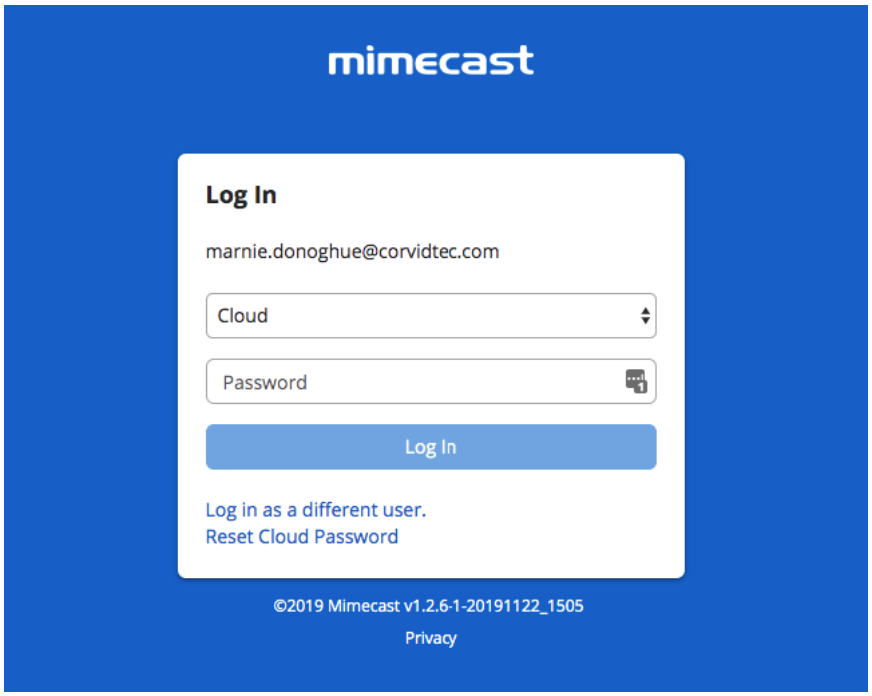
7. Enter the one-time passcode from the email into the empty field in your browser.



8. Create your new unique password by following the instructions. Select “Confirm” once all password criteria are check-marked green.

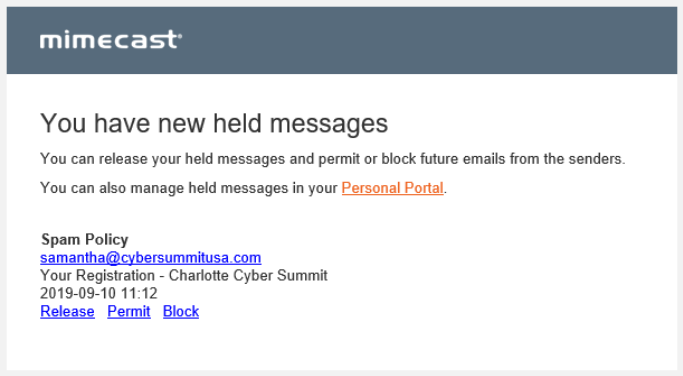


9. You will be redirected back to the login page. Ensure the dropdown box reads “Cloud” and **not** “Domain” and login with your new password. After a successful login, you will be taken to your Mimecast Online Mailbox. Further down, this guide will explain how to use this mailbox.



How will my email change?

Throughout the day, you will receive digest emails from “Domain Postmaster Address” with the subject line “[Postmaster] Messages on Hold” listing emails that were quarantined from your inbox. For each quarantined email, you have the option to Release, Block, or Permit.



Release: Releases the email from the quarantine queue and send it to your Inbox; future emails from this sender may still be placed On Hold.

Block: Rejects the email and adds the sender's address to your personal block list to prevent receiving future emails from the sender.

Permit: Permits or delivers the email to your inbox and adds the sender's address to your personal permit list to allow future emails from this sender. See the "Note" below regarding permitted senders that continue to be quarantined.

Note: Spam Filter policies implemented for your organization may cause emails to be quarantined. In some cases, permitting a sender will still result in their emails being quarantined. If this occurs, there are likely other Policy Rules blocking the email based on matching characteristics. Please contact Corvid Cyberdefense Support for assistance.

If you do not select one of the above options, the email will remain in your "on hold" inbox. You can access emails in your "on hold" inbox by either logging into the Mimecast web portal through your browser (at https://login.mimecast.com), the Mimecast smartphone application (available for iOS and Android), or the Mimecast Outlook Plugin.

Mimecast Plug-in

Note: The Mimecast Plugin is currently only available for Outlook users. If your organization does not use Outlook, skip to the section "What is Mimecast.com for?"

The Mimecast Plugin for Outlook allows you to access your online inbox and hold queue, manage your blocked senders list, report spam and phishing emails, and more, all from the Outlook application.

Installing the Mimecast Plugin

Your organization may have the ability to remotely push this plugin to users. Alternately, your organization may have security controls in place requiring credentials to download plugins such as Mimecast for Outlook. If your IT administrator gives you the ability to download the plugin, follow these steps.

1. Close Microsoft Outlook.
2. Go to: https://community.mimecast.com/community/knowledge-base/application-downloads/pages/mimecast-for-outlook and then select whether to download the 32-bit or 64-bit client (most users on Windows 7 or above will need the 64-bit client).
3. Run the Mimecast for Outlook installer.
4. When the welcome window is displayed, click the Next button to start the installation.
5. Read and accept the End User License Agreement.
6. Click the Next button. Next the installer will check your system to ensure all technical prerequisites are met and that Outlook is closed.
7. Once all prerequisite checks have been performed, click the Next button to continue with the installation.
8. Specify the Installation Directory (typically this is the default folder location suggested unless specified otherwise by your administrator).
9. Click the Install button to begin the installation.
10. Once complete, click the Finish button. Microsoft Outlook should start automatically when exiting the installation wizard.
11. As with any Windows application installation, we recommend restarting your computer to ensure installation was successful.

Authenticating the Mimecast Plugin

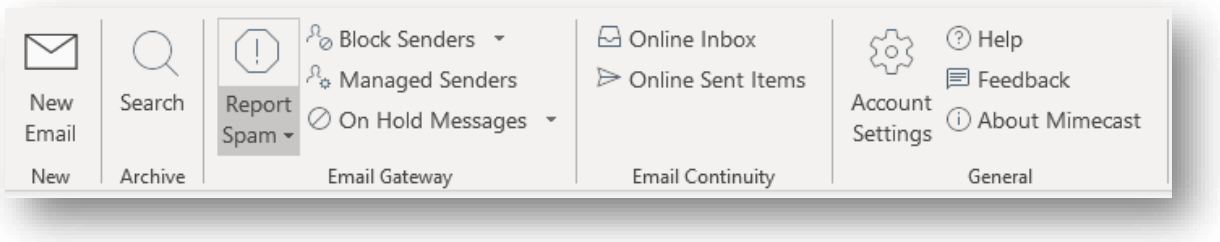
After installing the Outlook plugin, Outlook should start automatically. To authenticate your Mimecast account and enable the Mimecast ribbon function, follow these steps.

1. Navigate to the Mimecast ribbon in Outlook.
2. Under the "General Selection" select "Account Settings".
3. You will be taken to the Authentication dialogue box. Select "Fix" and enter your credentials.

Note: If you do not have your Mimecast credentials, please contact your IT administrator or follow the password reset process outlined in the "Mimecast Activation" section.

Navigating the Mimecast Ribbon

Below is a sample of what the ribbon in your Outlook application may look like:



In the "Archive" section of the ribbon, you can:

- Search for archived files and documents.
- Export search results back into Outlook.

In the "Email Gateway" section of the ribbon, you can:

- Report suspected spam emails, sending them to a blocked spam folder.
- Report suspected phishing emails to your Mimecast administrator for further investigation.
- Manage your blocked senders list (add or remove blocked senders).
- View your email hold/quarantine queue – if you do not take action on an email through the daily digest emails, you can access that email through this ribbon menu option (detailed below).

In the "Email Continuity" section of the ribbon, you can:

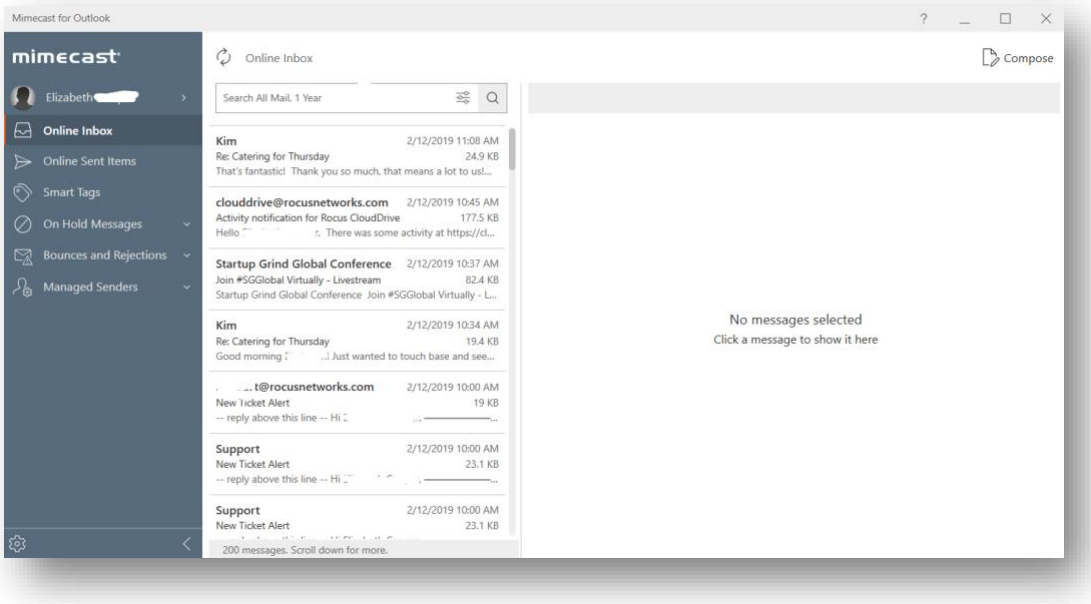
- Check your online inbox (useful if your Outlook is having trouble connecting to your Exchange server).

In the "Account Settings" section of the ribbon, you can:

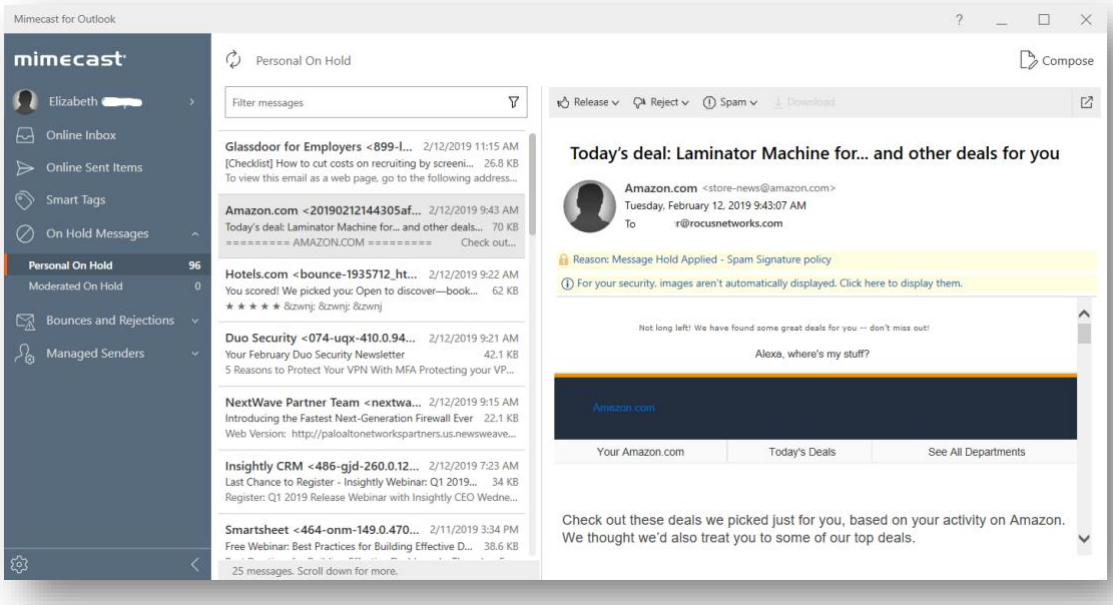
- Select "help" to take you to the Mimecast Knowledge Base.
- Select "About Mimecast" to verify you are running the most up-to-date version of the plugin.
- Send Feedback. **Note that this feedback only goes to Mimecast, not to your IT team or Corvid Cyberdefense.**

Your Online Inbox

Selecting “Online Inbox” in the Mimecast ribbon, your online inbox will pop open in another window. This allows you to access your inbox and send and receive mail as usual in the event Outlook is unable to connect to your mail server. You can also use your Online Inbox to access your hold queue and view messages that have been blocked or bounced due to the Mimecast policies implemented by your organization.



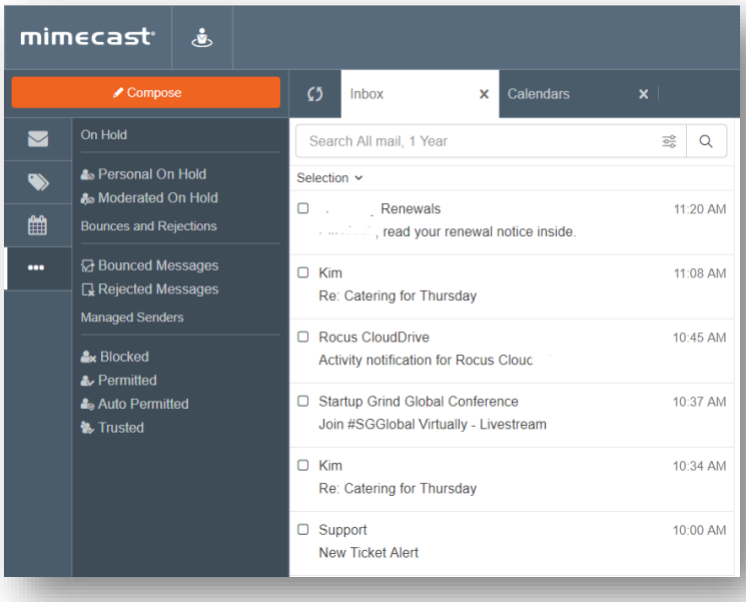
To see emails in quarantine before your next digest email, select “On Hold Messages” in the left column. This will display all of your messages currently on hold. You can view why the message was quarantined and choose to release the email, permit the sender, permit the domain, reject the sender, reject the domain, or mark the email as suspected spam or phishing for further investigation.



What is Mimecast.com for?

The online Mimecast user interface (accessed at https://login.mimecast.com) is a secure web-based portal offering the following features:

- Manage user account information
- Update user preferences.
- Create and manage trusted and blocked sender lists.
- Search email logs.
- Access to inbox and send/receive emails similar to a typical email client.



If your organization uses Microsoft Outlook, almost all Mimecast features will be available to you through the Mimecast ribbon in Outlook, so you will rarely need to log into the Mimecast.com website. For users not using Microsoft Outlook, we recommend bookmarking the https://login.mimecast.com website. This will be your primary destination for managing your hold/quarantine queues, sender lists, and more.

Other Mimecast Features

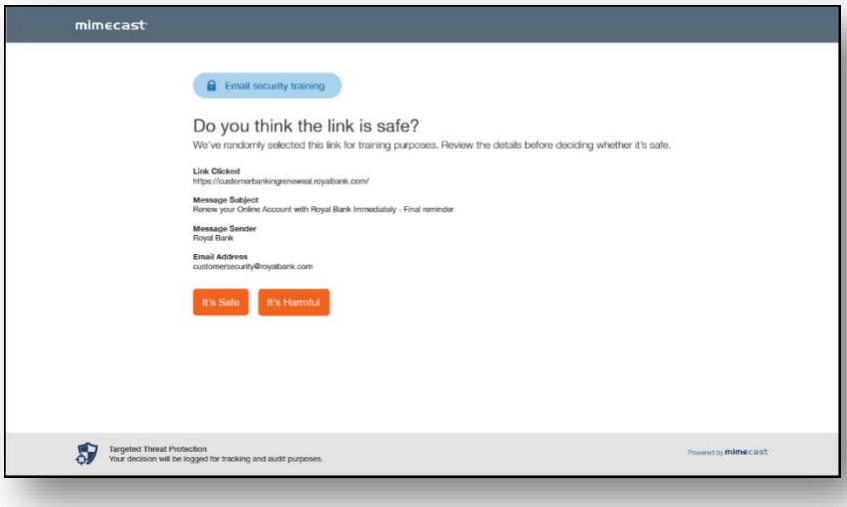
The following features may not be enabled for all users at all organizations. Please speak with your organization's primary IT contact for additional information.

Device Registration

A feature of Mimecast's Targeted Threat Protection is user device registration. The first time you click an email link on a new device, use a new browser, or clear your browser cache, you will be redirected to a registration page to register the new device or browser to your Mimecast account. Through this cookie-based system, Mimecast tracks who opens links, the device the link was opened on, and what links have been opened; this is useful in the event someone clicks a malicious link, intentionally or otherwise, as it allows administrators to identify "Patient Zero" and create a remediation strategy. Depending on your organization's security settings, you may have to periodically re-enroll your device (typically every 90 days).

URL Testing and Training

To enhance employee education and awareness, at least 5% of all URLs opened (your organization can opt to make this percentage higher), Mimecast will redirect the user to a training page where they will be shown information about the link opened and asked to re-affirm that the link is safe.



What happens next depends on:

- The settings configured in the organization's URL protection policies.
- Whether the URL is considered safe or harmful.
- What action the user chooses when presented with the user awareness prompts.

If the website is identified to be safe and the user chooses to continue to the website, they will be redirected as normal. If the website is determined to be harmful they will be notified, and an alert will be generated for the SOC to review. The URL Testing and Training feature serves to increase user awareness and train users to be

diligent in examining emails and links for authenticity to prevent successful phishing attacks against your organization.

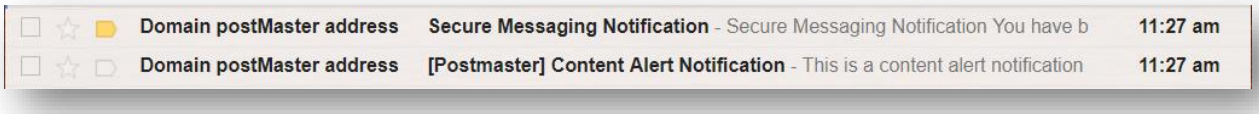
How to Send an Encrypted/Secure Email

Encrypting an email is a way to securely send an email to ensure that only the intended recipient is able to open the email and read its contents. While it is a good habit to secure all emails, it is particularly important to encrypt any emails that are sent over a unsecure networks, such as public Wi-fi or emails that contain sensitive information such as personally identifiable information (PII), banking info, proprietary or trade secrets, or sensitive client data, etc.

Mimecast makes it simple and easy to send encrypted emails. By adding "**<e>**" at the beginning or end of the email subject line, Mimecast will send the message securely. Once sent, the sender will receive a confirmation email from Mimecast confirming email encryption was successful.

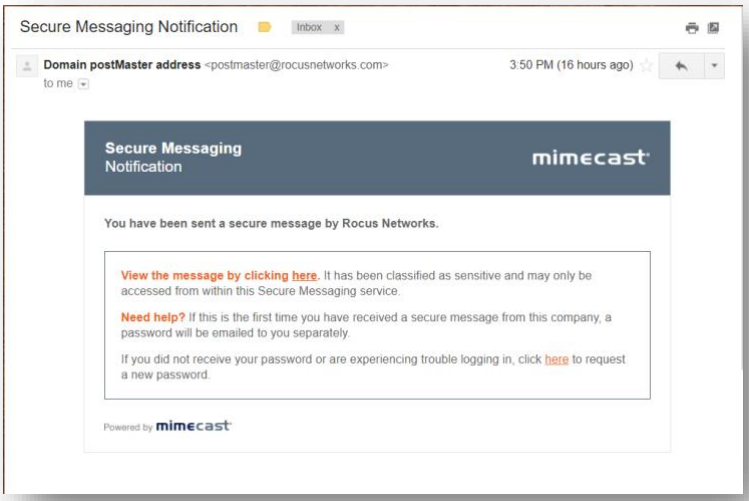
While it may be easy to send an encrypted email using Mimecast, it is important that the sender communicates with the recipient(s), informing them that they will receive an encrypted email and that they will need to access it through the Mimecast Secure Mail inbox rather than opening it as a normal email. The following section provides an overview of what the recipient will see.

The recipient will receive an email from "Domain postmaster address" instead of the senders name and email address.



If this is the recipient's first time receiving a secure email from someone at your organization, they will receive both the Secure Message Notification as well as a temporary password for accessing the Mimecast Secure Portal.

Selecting “View the message by clicking here” opens up a browser window to the Mimecast Secure portal. Here the recipient will be asked to login using either the temporarily created credentials or their normal login information, if they previously registered. Once logged in, the user will be taken to their Secure Mail inbox to view the message, download attachments, and reply with another encrypted email.



What if I have questions?

Please reach out to your network or IT administrator if you have any questions. If they are unable to help you, he or she can work with the Corvid Cyberdefense Email Administration team to resolve your issue. You can also check Mimecast resources and troubleshooting guides at https://community.mimecast.com/docs/DOC-1526.