# Email For Employees

**END USER EMAIL TEMPLATE**
*Copy and paste this template to send an email to all employees to help educate them on changes they will see regarding your new cybersecurity controls. Please feel free to edit to customize for your organization based on your Haven service package.*

Subject line: Cybersecurity Update

Hi Team,

To improve our IT security, we recently partnered with Corvid Cyberdefense to provide our cybersecurity service. They will help us implement security solutions to protect our network and Internet traffic, email, and computers.

While the technologies will do most of the heavy lifting, you as an employee play a significant role in keeping our company safe. Because of this, we will begin providing security awareness training in the form of short, educational videos designed to teach skills like how to identify phishing emails. You will receive more information about this soon.

Below are answers to common questions about our new cybersecurity service to help you understand what to expect. You can find more information on the Corvid Cyberdefense website: corvidcyberdefense.com/help.

Please don't hesitate to contact me if you have additional questions or need assistance.

Thank you for helping us stay cyber safe,

<Name>

**FAQS**

**How Will I Recognize the New Security Tools?**
While most of the security solutions employed will remain invisible to you, you will directly interact with our Endpoint Security Solution called Cylance and Email Security Solution called Mimecast. You will also receive emails about Symbol awareness training.

# Email For Employees

**What is Network Security?**

A Palo Alto Networks next-generation firewall examines all traffic coming in and out of our organization's network. Corvid Cyberdefense works with us to create sets of policies to allow or deny specific types of traffic (for example, blocking any web traffic categorized as gambling). In addition to examining and filtering web traffic, this security solution can examine and manage computer applications and devices connected to our network.

Daily network security happens almost entirely behind the scenes; the only time you will notice the firewall working is if you encounter a website that has been blocked, in which case you will see an error page. If a website has been blocked that you require for your job, you can send a note to your IT administrator who can help and/or contact Corvid Cyberdefense to allow the website if deemed safe.

**What is Endpoint Security?**

In the event a threat or malware gets past our organization's Network Security Solution or Email Security Solution, it will encounter an endpoint (typically either a computer or a server). Providing a secondary layer of security is Cylance; you can think of it as a new and improved version of antivirus. This endpoint solution utilizes machine learning to identify and block malware, ransomware, advanced threats, and malicious documents and scripts. The machine learning employed by the solution allows it to identify threats even if they've never previously been seen (known as a zero-day threat).

After installation, Cylance will run in the background, requiring no action on your part. You can tell that it's running and view any alerts by looking at your computer's system tray and selecting the shield icon.

In the event you try to open or run a malicious file and Cylance blocks it, you will receive a pop-up notification informing you of the block, assuming your organization has enabled notifications. If you receive a block notification and believe it to be in error, you can reach out to your IT team or provider who can then work with Corvid Cyberdefense to investigate the file to see if it is truly malicious or if it is being erroneously blocked.

**What is Email Security?**

The Haven Email 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
- Mimecast is a filter that runs in the background but you will need to activate your account in order to access the Mimecast email portal at https://login.mimecast.com. The first time you access the portal, please enter your email address and select Reset Cloud Password to be emailed your password and you can then log in. More information can be found in the Mimecast User Guide.

**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 blocked from your inbox and are in quarantine, or "on hold." For each quarantined email, you have the option to Release, Block, or Permit.

Release: This will release the current email from your hold/quarantine queue and send it to your Inbox; future emails from this sender will still be placed On Hold.
Block: Rejects the email and adds the sender's address to your personal Block list to block future emails from this sender.
Permit: Delivers the email to your Inbox and adds the sender's address to your personal Permit list so that future emails are not put On Hold. See the "Note" below regarding permitted senders that continue to be quarantined.

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 hold queue/inbox by logging into the online Mimecast portal through your browser (at login.mimecast.com).

**What if I Am Not Able To Access a URL or Receive an Email That I Need To Do My Job?**

Please contact your IT administrator who will submit a support ticket to Corvid Cyberdefense.

**What is Security Awareness Training?**

Employees are often the first line of defense in preventing cyberattacks. To help improve our overall security awareness, soon you will receive an email from "Cyber Training" that will

include a link to watch short video episodes that explain things like how to identify a phishing email. You will receive a new email each and we request that you watch the 3-4 minute video within 72 hours of notification.