MARIST Department of Information Technology

## Barracuda Link Protection

Barracuda Link Protection scans your email for any potentially known malicious links. You will notice that when you hover over the link in your email, it will be rewritten in the bottom-left corner. See below what the URL will look like after it is rewritten.


Every rewritten URL will start with the same beginning: *https://linkprotect.cudasvc.com*

In some emails that are written in plain text versus HTML, you will see the fully rewritten link in the body of the email. See below what the body of an email will look like if the link has been rewritten.

-----Original Message-----
From: PayrollOffice@marist.edu <PayrollOffice@marist.edu>
Sent: Friday, May 15, 2026 10:11 AM
To: Miranda.Marist <Miranda.Marist@maristtest.com>
Subject: Administrative leave reports for the pay period 5/1/2026 - 5/15/2026 are due by 5/31/2026.

Good morning Miranda,

This is a reminder that administrative leave reports for the pay period 5/1/2026 - 5/15/2026 are due by 5/31/2026.

Please note that any leave report not received by 5/31/2026 needs to be manually released.
This manual process is very time-consuming and is not in compliance with Marist College audit procedures.
Therefore, please submit your leave report in a timely manner by accessing the Employee Self Service Tab on https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fmy.marist.edu%2fhome&c=E,1,a_saafpipJST1pjDQqwjL3_J27hYeijtdkuqlX1YrO8qZm5xlQNuElBYfpZpeapxUlFuafoHOZZwSX6BEluGKm4dmHdAGkYpnvk-OfgXHJ1pq4LceiT20jDF&typo=1.

If you have any questions or concerns, please contact The Payroll Office at payrolloffice@marist.edu.

Thank you,
The Payroll Office

***PLEASE DO NOT REPLY TO THIS EMAIL***

## Malicious Attachments

Documents attached to emails will be evaluated for malware and other threats in a self-contained environment. Artificial Intelligence (AI) is used to determine whether anything is malicious. The mail is then passed to the mailbox if the attachments are deemed safe.

## Quarantine Digest

Email messages that appear to be phishing or otherwise malicious will be securely stored in the Barracuda Message Log, and the individual will receive a notification to review them in their personal quarantine. Please see below for an example of a personal Quarantine digest email.

Please continue to check the Microsoft Quarantine as we transition to the Barracuda Quarantine Digest. If you're unsure about a missing email, please contact the Help Desk and wait for IT personnel to get back to you before taking any action.

**From:** Barracuda Networks <quarantine@ess.barracudanetworks.com>
**Sent:** Sunday, May 17, 2026 8:20 AM
**To:** Miranda Marist <Miranda.Marist@maristtest.com>
**Subject:** Barracuda Networks' Email Gateway Defense Quarantine Notification

Barracuda

**You have 2 new quarantined inbound emails**

View in Email Gateway Defense

**Spencer Pratt torches Chelsea Handler with Epstein dinner part y jab after she mocks his mayoral run** — May 16, 2026 12:33 PM
"Fox News Entertainment" <email@inbox2.foxnews.com>
Deliver Block sender

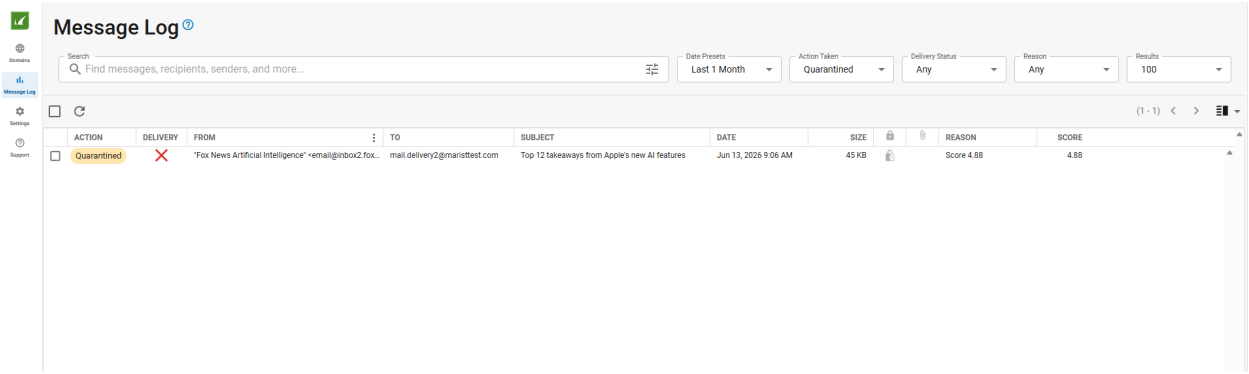
**40% off: Stay updated however you choose.** — May 16, 2026 09:05 AM
CNN Subscriptions <subscriptions@mail.cnn.com>
Deliver Block sender

This email was sent from Barracuda Email Gateway Defense because you or your administrator has requested that you be notified of your quarantined messages. You can manage your quarantine preferences in Email Gateway Defense.

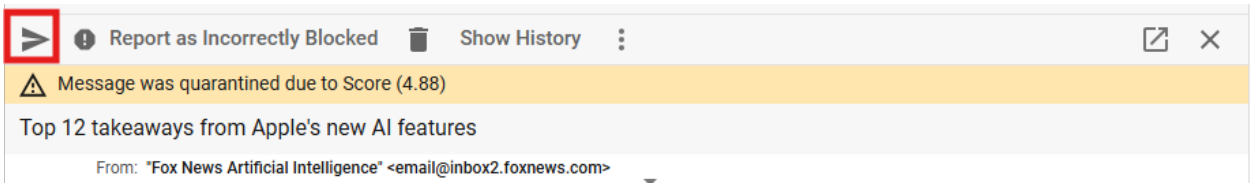
Privacy Policy • Legal Terms, Conditions and Warranties
Barracuda Networks, Inc. • 3175 Winchester Blvd, Campbell CA 95008

**Review Personal Quarantine Log in Email Gateway Defense:**

1. Click on View in Email Gateway Defense, where you will be brought to a web page displaying your Message Log, filtering on the Quarantine, seen below.




2. Select the message in the log, and the email will be displayed; images will not be seen in this email preview.
3. After reviewing the message in the quarantine, you can select the **Deliver button**, which will look like this.




4. When releasing an email message, you must ensure that the email is legitimate. Exercise caution with phishing and spam emails that may appear authentic. If you suspect the message is not genuine, you may click on the “X” at the top of the pop-out window.

**Links to Further Training**

Email Gateway Defense User Interface User Guide

Email Gateway Defense End-User Training Videos

- Introduction Video
- Email Gateway Defense End-User Training
- Email Gateway Defense Hands-On Video