

Proofpoint Spam Management

These FAQs explain our Proofpoint spam filtering system and how we process emails that originate from outside the college.

It will answer common questions about the tools that you can use to manage your personal spam account and quarantine.

- [About Proofpoint](#)
- [Does Proofpoint Protect Against Dangerous URLs?](#)
- [Spam Quarantine](#)
- [End User Digest](#)
- [Safe / Blocked Senders List](#)

About Proofpoint

What is the Proofpoint spam management system and why do we use it? The Proofpoint spam management system is an email filtering tool. To protect A-State from virus attacks and to protect you from receiving hundreds of spam messages, all incoming email is filtered by Proofpoint, which is an anti-spam and anti-virus product.

How does email filtering work? All incoming email is filtered by a server. Messages that contain a virus, or spam, or inappropriate content can either be deleted or "scored." In the case of spam, the message score indicates the probability that the message is spam --- so a message scoring 100 would have 100% chance of being spam (definite spam) and a message scoring 0 would have 0% chance of being spam (legitimate correspondence). Messages scoring high enough to probably be spam are quarantined, and messages scoring below 50 are sent directly to your inbox.

Does Proofpoint Protect Against Dangerous URLs?

Yes, the new Proofpoint spam service will help protect you from specific threats that are distributed via email, including phishing and targeted attacks. Proofpoint's URL Defense protects you and A-State's network resources by blocking access to malicious websites. Links in all email messages are evaluated using a variety of sophisticated techniques to determine the likelihood that they lead back to phishing or malware websites.

If links can't be definitively classified as safe when the message is received, the URL is rewritten so that clicking it will cause URL Defense to evaluate the linked website a second time. If the link is safe, you will see no difference. If it is malicious, you will see a notification in your browser like the following:



Web Site Has Been Blocked!

The web page you are attempting to access has been classified as malicious. This classification is determined by direct analysis of the web page. Although an entire web site may be blocked as malicious, it is very common for a single page on a valid web site to be blocked.

Your organization has enabled this technology to protect you, your system, and the organization from harm. Blocked pages contain material such as:

- **Credential Theft:** A page may be designed to look like a valid financial institution, a well-known organization, or an otherwise trusted source. The page is requesting a login and/or password for malicious purposes.
- **Malware:** A page may contain files or other malicious material which are intended to harm your system or organization. The malicious material may contain a virus, an installation program, or it may expose a vulnerability in a program which exists on your system.

Spam Quarantine

What is the Quarantine?

The **Quarantine** is a location on our [Proofpoint](#) server where email messages that are suspected to be spam are stored temporarily so that they can be reviewed and retrieved if necessary.

System administrators have the ability to search for messages on a user's behalf. You may also review and take action on your own quarantined email through the use of the **End User Digest**.

Messages that are not released from the Quarantine are automatically deleted after a designated period of time.

How do I access the Quarantine?

You can access your spam management account and Quarantine at proofpoint.astate.edu.

Log in with your A-State email address and password.

Can I access the antispam quarantine remotely?

Yes, you can access the system from anywhere.

How do I view messages that have been caught by the email filter and are in the Quarantine?

Log into proofpoint.astate.edu with your A-State email address and password.

Select **Quarantine** on the left side to view your messages in the Quarantine. This page displays messages addressed to you that were classified as spam and are sitting in the Quarantine.

I see an email in the Quarantine that is not spam. How do I release it to my inbox?

You will receive a spam **End User Digest** email listing all emails that have been quarantined by the spam filter. In addition, you can always log into proofpoint.astate.edu with your A-State email address and password and select **Quarantine** to check for emails that have been caught.

End User Digest

What is the End User Digest?

If email messages addressed to you were sent to the Quarantine, you will receive an email with the subject line **End User Digest**, in your mailbox. The Digest provides you with a list of the messages addressed to you that are stored in the quarantine. You can look at the message subject headers to determine their content and decide what actions you want to apply to the messages.

How do I use the digest?

The Digest will provide you with a list of all of the spam that has been quarantined for your account since you received the last Digest update. You will see a list of these messages and columns that indicate the subject, sender, and time received for each email.

You will have three separate links available to you to complete an action on each email message:

- *Release* - releases the message from the Quarantine to your normal email inbox.
- *Release and Allow Sender* - releases the message from the Quarantine to your inbox and adds the sender to your personal Safe Senders list. All future email from this sender will not be checked for spam.
- *Not Spam* - reports that the message was a false positive (that is, it should not have been classified as spam). In this case, the system analyzes the data to ensure that similar messages are not caught as spam in the future.

Other links in the Digest provide additional functionality. These links are not related to individual quarantined messages. The

following links provide additional Digest management:

- *Request New End User Digest* - immediately generates a new Digest with up-to-the-minute information about quarantined messages. Note: this Digest will contain a list of all messages currently in the Quarantine, not just those received since the last scheduled Digest update.
 - *Request Safe/Blocked Senders list* - sends you a list of all entries currently on your personal Safe and Blocked Senders List. *This list of safe and blocked senders is different than any lists you have set up on your email client.*
 - *Manage My Account* - allows you to change account preferences, as well as actively manage your **Safe Senders** and **Blocked Senders** lists using a web interface.
-

How often will I receive an End User Digest?

By default, you will receive an End User Digest twice a day if messages have been placed into your Quarantine since the last digest was sent.

Safe / Blocked Senders List

What is a Safe Senders and Blocked Senders list?

There are two types of Safe Senders lists.

- Global Safe Senders List
- Personal Safe Senders List.

Both are simply lists of legitimate senders of email. The email administrator controls the Global Safe Senders List, which applies to everyone in the organization. You control your personal Safe Senders List to which you can add the addresses of people, organizations, and mailing lists from which you do want to receive mail.

If a sender's address is included in the Safe Senders List, the anti-spam system does not filter the message for spam. However, it still filters the message for a virus or inappropriate content.

There is also a Global Blocked Senders List and a personal Blocked Senders List. As with the Global Safe Senders List, the Global Blocked Senders List applies to everyone in the organization. These lists contain addresses of people, organizations, and mailing lists from which you do not want to receive "junk email."

How do I manually add Safe Senders and Blocked senders to the spam management system?

Log into proofpoint.astate.edu with your A-State email address and password. Select Lists on the left side to view your **Safe Senders** and **Blocked Senders** lists.

To add a Safe Sender to your list:

1. Select **Safe Senders List** on the left side.
2. Select **New** on the top of the page.
3. Enter an email address (e.g., john.doe (at) example.com) into the field to permit all messages from this sender to be delivered. Optionally, enter an email domain (e.g., example.com) into the field to permit all messages from xyz.com to be delivered.

Note: Permitting all email from an entire domain is **not recommended** as this could increase the risk of spam or malicious email.

4. Select **Save**.

Follow the same procedure to add entries to your **Blocked Senders List**.

Email sent from addresses or domains on the Safe Senders List will not be filtered for spam, but will be filtered for viruses.