**Ensuring End User Email Deliverability for Email Communications**

EVA, our Employee Vulnerability Assessment, is included in the Breach Prevention Platform (BPP), HIPAA BPP, and EVA MD services and automatically sends emails on your behalf to end users. There are various emails that may be sent with this subscription, including:

* Weekly Micro-Training
* Monthly Security Newsletter
* Breach Notification Emails
* Welcome Message [For New Users]
* Welcome Back Message [For Returning Users]

These emails are sent to end users of clients you have signed up for the BPP, as well as employees of yours that have registered for training.

The header of the emails will look like this:

A screenshot of a cell phone

Description automatically generated

In order to ensure maximum deliverability, we ask that you do the following:

1. Whitelist the email addresses: [No-reply@security-reminders.com](mailto:No-reply@security-reminders.com) and [no-reply@pii-protect.com](mailto:no-reply@pii-protect.com) in SPAM filters. You can also make adjustments within your client’s email system (Exchange, Outlook, etc.) to make sure that emails from this address get delivered to the Inbox and not to Junk, Clutter, etc.
2. Currently, we use two email services to send out emails. The weekly Micro-Training and monthly Security Newsletter emails are sent from our email service, Sendgrid. Below are the two IP addresses we recommend whitelisting to ensure all end-users will receive these emails.

* 149.72.184.111
* 168.245.40.98

In addition to Sendgrid, we are using Mandrill, a Mailchimp service for sending emails on your behalf when a user is enrolled in the portal via Azure Active Directory Sync. We are in the process of moving these emails over to our Sendgrid service, but for the time being, please also follow Mandrill’s recommendations for ensuring maximum deliverability.

1. Mandrill provides the following information on email deliverability in regard to whitelisting:

Whitelisting by IP is not recommended because Mandrill’s shared IPs may change without notice, and the recipient would be whitelisting all mail from Mandrill. If whitelisting by IP is the only option, the recipient domain will want to check for the most up-to-date IP information in the TXT record for spf.mandrillapp.com. On a Mac or Linux, this information can be obtained using the following command: dig TXT spf.mandrillapp.com

This record will be updated whenever new IPs are added to Mandrill’s sending IP range. If a receiving server is whitelisting the range, it’s recommended they periodically check to ensure they have the current range used by Mandrill.