Uniform Stores

Whitelisting Emails

Whitelisting emails is often used to prevent important or trusted emails from being mistakenly classified as spam. This can be done in two different levels which are individual and organizational. Individual Whitelisting: When a user adds a specific sender's email address to their IT filter's "safe sender" list , this ensures that future emails from that sender are not filtered out as spam or have the potential of being blocked. Organizational Whitelisting: This is where your IT department would add trusted domains or email addresses to the organization's email gateway or server, this ensures that emails from these sources are delivered to all users without being flagged. Emails that should be whitelisted when receiving any information from us include: any emails that include the email domain "[Name]@uniformstores.com". Making sure this email domain listed above is whitelisted and that your infrastructure is set to receive these emails from this specific domain will enhance the deliverability rates when receiving email communication from our organization.

The following domains are utilized by our Uniform Stores platform. To assist in ensuring that your employees are able to access their Uniform Store while on your organization's network, please whitelist the following domains.

- uniformstores.com
- shopify.com
- myshopify.com
- stripe.com
- email.uniformstores.com, k1.email.uniformstores.com, and em3584.uniformstores.com.

Maintain a Clean Email List

A clean email list is the main foundation to ensure high deliverability rates. It is important to regularly update and purge your list of inactive, invalid, or duplicate email addresses. This in return will help alleviate unwanted email communication. Deleting an employee from your Uniform Stores admin portal upon termination or resignation will also help maintain email deliverability.