False Positives

Emails that are classed as false positives are messages that have **not** been sent by a malicious actor, and are instead legitimate emails that have been incorrectly reported as malicious. There are a number of reasons that false positives can occur:

- **The user believes the email is malicious or potentially malicious**
- **The email has poor formatting** (usually internal emails) **and appears to be suspicious**
- **The email is unexpected and asks the user to complete an action** (click this button, contact us immediately, transfer funds to this account, etc)
- **The user is not familiar with identifying malicious emails due to a lack of phishing awareness training**

Having employees report emails that turn out to be false positives is not necessarily a bad thing. It shows that users are engaged with reporting emails they believe to be suspicious, which is arguably better than them not reporting anything at all. It takes one email to compromise a system and a network, so we're sure most organizations would rather deal with a few false positives than miss genuine malicious emails.