Explanation of Reason Reported

https://campus.barracuda.com/doc/98222864/

This table describes why you or someone on your team might have reported an email to Barracuda Networks. For full details about each of these threat types, read the Barracuda Networks ebook,*13 Email Threat Types to Know About Right Now* .

Reason Reported	Explanation	Possible Threat
Incorrectly Delivered	**Message appears to be dangerous.**	**Extortion, Domain Impersonation, Brand Impersonation, Business Email Compromise, Conversation Hijacking, URL Phishing, Spear Phishing, Lateral Phishing, or Malware** For details, refer to the specific responses and threats described in this section.
	Sender is threatening you.	**Extortion**: Cybercriminals leverage usernames and passwords stolen in data breaches to contact and try to trick victims into giving them money.
	Sender is pretending to be someone you know.	**Domain Impersonation**: Attackers attempt to impersonate a legitimate domain as part of a Conversation Hijacking scheme (see below). Hackers might use techniques like typosquatting, replacing one or more letters in a legitimate email domain with a similar letter, adding a hard-to-notice letter to the legitimate email domain, or changing the last three letters of the URL. For example, `barrracuda.com` or `barracada.com`. **Brand Impersonation**: Attackers impersonate a company or a brand to trick their victims into responding and disclosing sensitive information. **Business Email Compromise**: Scammers impersonate an employee within an organization, in an attempt to defraud the company, its employees, customers, or partners. **Conversation Hijacking**: Using information they have gathered from compromised email accounts, cybercriminals insert themselves into existing business conversations or initiate new conversations in an effort to steal money or personal information.

	Sender is trying to get you to reveal personal or sensitive information.	**URL Phishing:** Cybercriminals use email to direct their victims to enter sensitive information on a fake website that looks like a legitimate website. There, the criminals try to obtain sensitive information, such as passwords or banking details, for nefarious purposes. **Spear Phishing**: Cybercriminals research their targets and craft carefully designed messages, often impersonating a trusted colleague, website, or business, in an attempt to steal sensitive information, such as login credentials or financial details. This information is then used to commit fraud, identity theft, and other crimes. **Lateral Phishing**: Attackers use recently hijacked accounts to send phishing emails to unsuspecting recipients, such as close contacts in the company and partners at external organizations, to spread their attack more broadly.
	Sender is trying to get you to access a file.	**Malware**: Attackers can use files or links to send malware, software specifically designed to cause damage to technical assets, disrupt operations, exfiltrate data, or otherwise gain access to a remote system. Either the malware is hidden directly in the document or an embedded script downloads it from an external website.
	Message is unwanted or trying to sell goods or services.	**Scamming, Spam, or Bulk Email** For details, refer to the specific threats described in this section.
	Sender is trying to sell goods or services.	**Scamming**: Cybercriminals attempt to defraud victims or steal their identity by tricking them into disclosing personal information.
	Content is not appropriate for work.	**Spam**: Unsolicited, bulk email messages that can include explicit images or medication offers.
	You either did not sign up for these messages or have never done business with this company.	**Spam**: Unsolicited, bulk email messages, generally of commercial nature. Usually sent without regard to the recipient's identity and without the recipient's consent.
	You signed up to receive these messages, but no longer want them.	**Bulk Email**: Solicited messages that, due to a decrease in the recipient’s interest over time, increases the likelihood that they will be reported as spam.
Incorrectly Blocked	Message from a requested mailing list or newsletter.	**No threat**: This is an email from a service you requested.
	Message is from a known business.	**No threat**: This is an email you want to receive, from a business you trust.
	Message is from a known sender.	**No threat**: This is an email you want to receive, from a sender you trust.