Use this guide to determine if unwanted emails in your inbox are phishing attacks or spam.

### PHISHING ATTACK

- **Want your information**: credit card number, password, bank account, etc.
- **Often targeted**: Sent to a specific individual or group and contains relevant information, e.g., your name
- **Include malicious links** to fake websites or malware downloads
- May contain malicious attachments
- **Has a sense of urgency**
- Should be deleted and reported

### SPAM EMAIL

- **Unwanted advertisements** for products or services
- **Always broad**: Sent to millions of recipients
- **Include links to mostly legitimate websites** offering products or services
- **Does not contain attachments**
- **Does not require immediate action**
- Should be marked as spam and deleted

---

Some spam emails (2.3%) are also phishing attacks.

### SHARED TRAITS

- **Unsolicited**: You didn’t ask for the email
- **Harmful**: Both either attempt to steal your information or waste your time
- **Illegitimate**: Use techniques like spoofing to make it to your inbox

© 2019 InfoSec Institute. All rights reserved.