**Datasets**

Here are a few notable datasets:

1. Enron Email Dataset: The Enron Email Dataset is a widely used dataset for email analysis and has been used for various purposes, including phishing detection. It contains a large collection of real emails exchanged by Enron Corporation employees. While it doesn't specifically focus on phishing emails, it can be useful for studying email patterns and identifying suspicious activities.
2. Phishing Email Dataset (PhishTank): PhishTank is a community-driven initiative that collects and shares information about phishing websites. They provide a dataset containing URLs and associated metadata, including the email content used in phishing attacks. It can be used to train machine learning models for phishing detection.
3. UCSD Email Phishing Dataset: The University of California, San Diego (UCSD) has released a dataset of real-world email phishing attacks. It includes over 15,000 labeled phishing and legitimate emails, along with the associated metadata, such as email headers, body, and attachments. This dataset is designed specifically for phishing detection research.
4. Kaggle Phishing Websites Dataset: Kaggle, a popular platform for data science competitions, hosts several datasets related to phishing. One such dataset contains features extracted from web pages to classify them as phishing or legitimate. While it focuses on website-based phishing detection, it can still be relevant for understanding phishing techniques.

Please keep in mind that these datasets might not fulfil all your specific requirements, such as complete details of headers, bodies, and attachments for a large number of samples.