1. **Spam filtering:**
   - **Data availability**: To apply this technique, a labeled dataset of emails (i.e., a dataset of emails that have been manually labeled as spam or non-spam) is required for training the model. This data can be collected from a variety of sources, such as publicly available datasets or by collecting and labeling emails from an organization's own email traffic.
   - **Time to set up**: Setting up a spam filtering system can be time-consuming, as it involves collecting and labeling a large dataset of emails and then training and tuning a machine learning model on this data. This process can take anywhere from a few days to several weeks, depending on the size and complexity of the model being used.
   - **Time to produce results**: Once the model has been trained and deployed, it should be able to classify new incoming emails in real-time.
   - **Output**: The output of a spam filtering system is a classification of each email as either spam or non-spam. This output can be used to automatically delete or quarantine spam emails, or to flag them for manual review by the recipient.
2. **Spam detection:**
   - **Data availability**: To apply this technique, a dataset of email traffic is required. This data can be collected from an organization's own email servers or by analyzing publicly available data on email traffic patterns.
   - **Time to set up**: Setting up a spam detection system typically involves training a machine learning model on a dataset of email traffic, which can take several days to a few weeks, depending on the size and complexity of the model.
   - **Time to produce results**: Once the model has been trained and deployed, it should be able to detect unusual patterns in email traffic in real-time.
   - **Output**: The output of a spam detection system is a notification or alert when unusual patterns in email traffic are detected. This output can be used to trigger further investigation or to block spam emails that are identified as part of the unusual pattern.
3. **Phishing detection:**
   - **Data availability**: To apply this technique, a labeled dataset of emails (i.e., a dataset of emails that have been manually labeled as phishing or non-phishing) is required for training the model. This data can be collected from a variety of sources, such as publicly available datasets or by collecting and labeling emails from an organization's own email traffic.
   - **Time to set up**: Setting up a phishing detection system can be time-consuming, as it involves collecting and labeling a large dataset of emails and then training and tuning a machine learning model on this data. This process can take anywhere from a few days to several weeks, depending on the size and complexity of the model being used.
   - **Time to produce results**: Once the model has been trained and deployed, it should be able to classify new incoming emails in real-time.

Output: The output of a phishing detection system is a classification of each email as either phishing or non-phishing. This output can be used to automatically delete or quarantine phishing emails, or to flag them for manual review by the recipient.