Malicious emails encompass a variety of deceptive and harmful messages sent via email. These emails are designed to exploit recipients by tricking them into taking actions that compromise security, steal sensitive information, or cause damage. Let’s classify these malicious emails based on pre-defined criteria:

1. **Phishing Emails**:
   * **Definition**: Phishing emails falsely claim to be from legitimate authorities or organizations. They aim to deceive recipients into revealing sensitive information or performing specific actions.
   * **Objective**: Cybercriminals use phishing emails to steal login credentials, credit card details, or other personal information.
   * **Example**: An email pretending to be from a bank, asking the recipient to click a link and update their account information.
2. **Malware-Infected Emails**:
   * **Definition**: These emails contain attachments or links that, when opened, install malicious software (malware) on the recipient’s device.
   * **Objective**: Malware can steal data, encrypt files (ransomware), or take control of the system.
   * **Example**: An email with an attached ZIP file claiming to be an invoice but actually containing malware.
3. **Business Email Compromise (BEC)**:
   * **Definition**: BEC attacks target businesses by impersonating executives, vendors, or partners. They request wire transfers, sensitive data, or other actions.
   * **Objective**: To defraud the organization or gain unauthorized access.
   * **Example**: An email pretending to be from the CEO, instructing the finance department to transfer funds urgently.
4. **Advance Fee Fraud (419 Scams)**:
   * **Definition**: These scams promise large sums of money in exchange for a small upfront fee. They often claim to be from wealthy individuals or foreign governments.
   * **Objective**: To extract money from victims.
   * **Example**: An email offering a share of a multimillion-dollar inheritance if the recipient pays a processing fee.
5. **Malicious Links and Drive-By Downloads**:
   * **Definition**: Emails contain links that lead to malicious websites or initiate automatic downloads.
   * **Objective**: To infect the recipient’s system with malware.
   * **Example**: An email claiming to have important information, with a link that leads to a fake login page designed to steal credentials.
6. **Spear Phishing**:
   * **Definition**: A targeted form of phishing where cybercriminals customize emails for specific individuals or organizations.
   * **Objective**: To increase the likelihood of success by tailoring the message to the recipient.
   * **Example**: An email addressed to an employee by name, appearing to come from their manager, requesting sensitive data.
7. **Social Engineering Tactics**:
   * **Definition**: Malicious emails often use social engineering techniques to manipulate recipients emotionally. These tactics include urgency, fear, curiosity, or trust.
   * **Objective**: To lower the recipient’s defenses and increase the chances of compliance.
   * **Example**: An urgent email claiming the recipient’s account has been compromised, prompting them to click a link to verify their identity.