**1. Safe Mail**

**Definition:**  
Messages that are **legitimate, expected, and relevant** to the recipient.

**Rule to classify:**

* The sender is **known and trusted**.
* The message is **expected or requested**.
* The content is **relevant and appropriate** (work, family, services you use).
* No attempt to mislead, frighten, or pressure you.

**Examples:**

* Your bank sending your monthly statement (if you signed up).
* A colleague replying to your email.
* A newsletter you subscribed to.

**2. Spam Mail**

**Definition:**  
Messages that are **unsolicited and unwanted**, usually promotional or irrelevant, but not directly harmful.

**Rule to classify:**

* You **did not ask** for the message.
* It is sent to **many people at once** (bulk).
* Content is **mainly advertising or irrelevant offers**.
* Usually not dangerous, but **annoying**.

**Examples:**

* Random sales offers you never signed up for.
* Mass emails about weight loss, loans, or lottery wins.
* Unwanted promotional newsletters.

**3. Malicious Mail**

**Definition:**  
Messages that **try to cause harm** — by stealing information, spreading viruses, or tricking you into unsafe actions.

**Rule to classify:**

* The message **pressures you into urgent action** (click, download, pay, share password).
* It contains **fake identity** (pretends to be from your bank, employer, or government).
* It often includes **links or attachments** designed to infect or steal.
* Goal is to **deceive or damage**, not just advertise.

**Examples:**

* “Your account is locked, click here to verify.”
* Fake invoices with malicious attachments.
* Phishing emails pretending to be tax refunds.

**4. Warning Mail**

**Definition:**  
Messages that are **suspicious or unusual**, not outright proven harmful, but raising concern.

**Rule to classify:**

* Something looks **out of place** (odd sender name, strange wording, broken language).
* The message may come from a **new or unexpected source**.
* Not clearly spam or malicious, but **uncertain enough to be cautious**.
* Treated as **“check before trust”**.

**Examples:**

* An email from a colleague’s personal Gmail about work.
* A sudden prize offer from a brand you once shopped at.
* A message with too many spelling errors, but no clear attack.