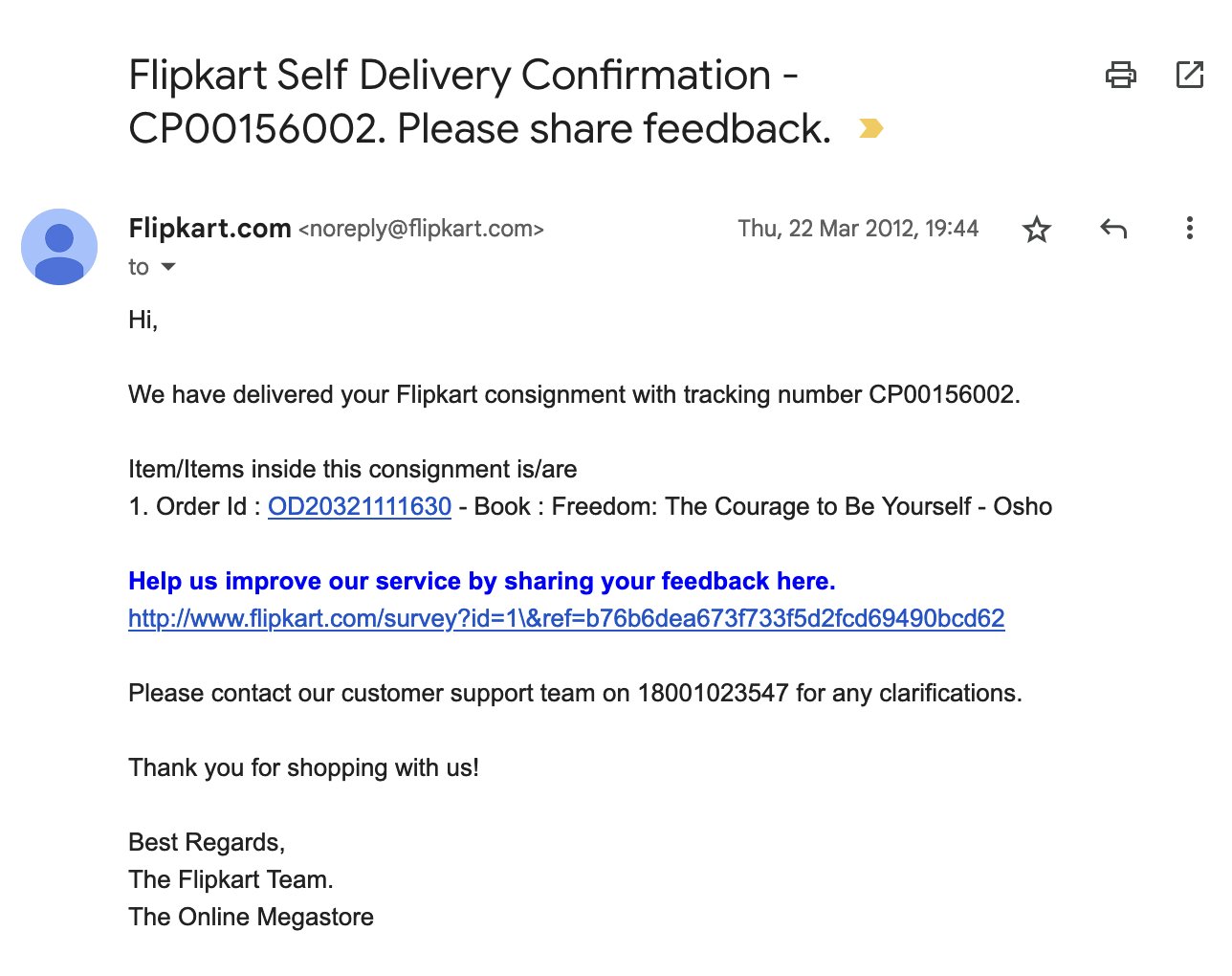
**Task 2: Analyze a Phishing Email Sample**

1. Obtain a sample phishing email (many free samples online).

****

**sender’s email address** is shown as: [**noreply@flipkart.com**](mailto:noreply@flipkart.com)

**Examination for spoofing:**

1. ✅ **Domain check:**
   * The domain is flipkart.com which is the **legitimate official domain** of Flipkart.
   * No obvious misspelling (e.g., flipkarts.com, flipkart-secure.com, or fl1pkart.com).
2. ⚠ **Potential risks:**
   * Some phishing emails **spoof the “From” field**, so while it *looks* like @flipkart.com, the actual sender could be different.
   * To confirm authenticity, you would need to check the **email headers** for the *Return-Path*, *Received from*, and *SPF/DKIM authentication results*.
3. **Suspicious link check:**
   * The survey link shows as http://www.flipkart.com/survey?... but:
     + It uses **http (not https)** — insecure for a major brand.
     + Long random string (b76b6dea673f73f5d2fcd69490bcd62) is unusual for genuine Flipkart feedback links.

**Conclusion:**

* On the surface, the **From address looks legitimate**.
* But phishing emails can forge this, so **checking full headers** is the only way to be sure.

1. **Check email headers for discrepancies (using online header analyzer).**

## Step 1: View full email headers

### In ****Gmail****:

1. Open the email.
2. Click the three dots ⋮ (top-right corner of the message).
3. Select **“Show Original.”**
4. A new tab will open with the full header + body.

### In ****Outlook****:

1. Open the email.
2. Go to **File → Properties**.
3. Look under **“Internet headers.”**

## 🔎 Step 2: Copy headers into an analyzer

* Copy the entire header text.
* Go to a free online analyzer, such as:
  + **Google Message Header Analyzer**
  + **MxToolbox Header Analyzer**

Paste the header there — it will break down the path.

## 🔎 Step 3: Look for discrepancies

When analyzing, pay attention to:

1. **Return-Path vs From:**
   * If the email claims noreply@flipkart.com but the return-path is something like noreply@flipkart-support.ru, it’s spoofed.
2. **Received From chain:**
   * Genuine emails from Flipkart should originate from Flipkart’s servers (look for domains like flipkart.com).
   * If you see strange servers (e.g., IPs from unrelated countries), it’s suspicious.
3. **SPF/DKIM/DMARC results:**
   * Look for lines like:
     + SPF=pass
     + DKIM=pass
     + DMARC=pass
   * If you see **fail**, the sender is likely forged.

**Example of red flag in a header**:

Received-SPF: fail (example.com: domain of attacker@evil.com does not designate 192.168.1.50 as permitted sender)

1. **Identify suspicious links or attachments.**

**🔗 Suspicious Links**

In the body of the email, we see this line:

**http://www.flipkart.com/survey?id=1\&ref=b76b6dea673f73f5d2fcd69490bcd62**

🚩 **Why it’s suspicious:**

1. **HTTP, not HTTPS** → A genuine Flipkart survey link should always use secure https://.
2. **Long random string** (b76b6dea673f73f5d2fcd69490bcd62) → Often used by attackers to track victims or redirect them.
3. **Context mismatch** → Flipkart usually sends surveys via branded, secure forms or official in-app links — not raw URLs with random IDs.
4. **Hover test** → If you hover over this link in a real email client, check if the actual redirect domain is *different* (e.g., flipkart-survey.xyz). That’s a major phishing red flag.

**📎 Attachments**

* This email doesn’t appear to contain file attachments.
* But phishing emails often include files like:
  + .zip, .rar (compressed malware)
  + .pdf (with malicious links inside)
  + .doc/.xls (with macros that download malware)

🚩 Rule: Legit companies rarely send unsolicited attachments for surveys or order confirmations.

✅ **Lesson:**

* Always **hover before you click** — check if the visible link matches the true destination.
* Be suspicious of **HTTP links**, random strings, or unknown domains.
* Never download unexpected attachments.

1. **.Look for urgent or threatening language in the email body.**

**🔎 Checking the Flipkart email you shared:**

📩 **Message body text:**

*“We have delivered your Flipkart consignment with tracking number CP00156002. … Help us improve our service by sharing your feedback here.”*

**⚠ Analysis:**

* This message is **polite and neutral**, not threatening.
* No **scare tactics** like:
  + *“Your account will be suspended in 24 hours”*
  + *“Failure to act will result in permanent loss”*
  + *“Unusual activity detected, verify immediately”*
* Instead, it uses a **soft call-to-action** (*“please share your feedback”*).

✅ **Conclusion:**  
This particular email **does not contain urgent or threatening language** — which makes it appear more trustworthy.  
But remember: **not all phishing uses threats**. Some use *enticement* (e.g., fake rewards, gift cards, or surveys) to trick users.

1. **.Note any mismatched URLs (hover to see real link).**

**🔎 In the Flipkart email you shared:**

The visible text is:  
**http://www.flipkart.com/survey?id=1&ref=b76b6dea673f73f5d2fcd69490bcd62**

⚠ **Suspicious factors:**

1. **HTTP instead of HTTPS** – a real Flipkart link should be https://….
2. **Survey path looks unusual** – Flipkart surveys are usually hosted on secure branded platforms, not with long random tokens.
3. **Hover test** (in a real email client):
   * If you hover over the link, check the *actual destination shown in the status bar*.
   * Sometimes it looks like www.flipkart.com, but actually redirects to something like:  
     http://flipkart-survey.secure-check.info/...
   * This is called a **mismatched URL**.

**✅ How to detect mismatched URLs:**

* **Visible link vs real link:**
  + If they don’t match → 🚩 Phishing.
* **Trick domains:**
  + flipkart.secure-check.com ≠ flipkart.com (real domain is only the part before .com).
* **URL shorteners:**
  + Links like bit.ly, tinyurl, goo.gl may hide the true destination.

✅ **Conclusion:**  
The email’s visible link *looks like Flipkart*, but because it uses http:// and an odd structure, it deserves suspicion. If the **hover preview shows a different site**, it’s definitely a phishing indicator.

1. **Verify presence of spelling or grammar errors.**

**🔎 In the Flipkart email you shared:**

* The text is:

*“We have delivered your Flipkart consignment with tracking number CP00156002. … Help us improve our service by sharing your feedback here.”*

**✅ Grammar & Spelling Check:**

* **Grammar:** Sentence structure is correct.
* **Spelling:** No obvious misspellings (e.g., “consignment,” “service,” “feedback” are correct).
* **Tone:** Reads naturally, unlike many phishing attempts that sound awkward (e.g., “Dear Customer, you account is suspend, please click link”).

**⚠ What to watch for in phishing emails:**

* Misspelled brand names → *“Flipkarrt,” “PayPall”*
* Awkward grammar → *“Your account are limited”*
* Inconsistent capitalization → *“Kindly Click Here to Verify your Information”*
* Overuse of urgent caps → *“ACT NOW OR LOSE ACCESS!!!”*

✅ **Conclusion:**  
This particular email **does not contain grammar/spelling errors**, which makes it look more convincing.  
⚠ But remember: some phishing emails today are **well-written** — so lack of mistakes doesn’t guarantee safety.

1. **Summarize phishing traits found in the email.**

**📋 Phishing Indicators**

1. **Suspicious Link**
   * Visible link: http://www.flipkart.com/survey?...
   * Uses **HTTP (not HTTPS)** → insecure for a major brand.
   * Long random string in the URL → common in phishing campaigns.
   * Needs hover check — if it redirects to another domain, that’s a clear mismatch.
2. **Possible Email Spoofing**
   * From address appears as noreply@flipkart.com, but spoofing is possible.
   * Authenticity can only be confirmed by checking **email headers (SPF/DKIM/DMARC)**.
3. **Unexpected Request**
   * Asking for survey participation via a raw link is unusual.
   * Legitimate Flipkart usually directs customers to secure in-app surveys or official branded forms.
4. **No HTTPS Encryption**
   * Any real Flipkart link should be https://, especially for customer-related data.

**✅ What was NOT present (common phishing traits absent here):**

* No spelling or grammar mistakes → the email is written cleanly.
* No urgent or threatening language → tone is neutral (“please share feedback”).
* No attachments → reduces risk of malware, but phishing can still happen via links.

**📌 Overall Assessment:**

* The email **looks polished** but shows red flags: **suspicious survey link, insecure HTTP, and potential spoofing risk**.
* These traits suggest it’s **likely phishing**, designed to harvest clicks or data under the guise of a Flipkart survey.

**Interview Questions:**

1. **What is phishing?**

Phishing is a type of **cyberattack** where attackers try to trick people into revealing sensitive information—such as passwords, credit card numbers, or personal details—by pretending to be a **trustworthy entity** (like a bank, social media platform, or government agency).

1. **How to identify a phishing email ?**

**1. Check the Sender’s Email Address**

* Look closely at the email address, not just the display name.
* Phishers often use addresses that look similar to a real one:
  + Example: support@paypa1.com (instead of paypal.com)

**2. Look for Generic Greetings**

* Legitimate companies usually use your name.
* Phishing emails often start with “Dear Customer” or “Dear User.”

**3. Inspect Links Without Clicking**

* Hover over links to see the actual URL.
* Fake links may look real but redirect elsewhere.
* Avoid clicking suspicious links.

**4. Check for Urgent or Threatening Language**

* Phrases like “Your account will be suspended!” or “Immediate action required!” are red flags.

**5. Look for Spelling and Grammar Errors**

* Official companies rarely send emails with poor grammar or typos.

**6. Examine Attachments Carefully**

* Be cautious of unexpected attachments, especially .exe, .zip, .scr, or .docm files.
* They could contain malware.

**7. Verify Through Other Channels**

* If unsure, contact the company directly using official contact information.

**8. Check Email Headers (Optional, for Advanced Users)**

* Email headers can reveal the real sender’s IP and server, which may not match the company’s servers.

1. **What is email spoofing?**

**Email spoofing** is a technique used by attackers to make an email **look like it’s coming from someone else**, usually a trusted source, even though it’s actually sent by the attacker. It’s a common tactic in phishing attacks.

1. **Why are phishing emails dangerous?**

Phishing emails are dangerous because they are designed to **trick people into revealing sensitive information or installing malware**, which can lead to serious consequences. Here’s why:

**1. Theft of Personal and Financial Information**

* Phishing emails often try to steal passwords, credit card numbers, Social Security numbers, or bank details.
* Attackers can use this information for **identity theft or fraud**.

**2. Account Compromise**

* Providing login details can give attackers access to **email, social media, or work accounts**.
* They may impersonate you to scam your contacts or steal more data.

**3. Malware and Ransomware Infection**

* Attachments or links in phishing emails can install **malware, spyware, or ransomware** on your device.
* This can **encrypt your files, monitor activity, or damage systems**.

**4. Financial Loss**

* Scammers can **transfer money from accounts, make unauthorized purchases, or demand ransom**.

**5. Reputation Damage**

* In businesses, a phishing attack can expose **customer or company data**, harming trust and credibility.

**6. Widespread Impact**

* A single phishing email can trigger **network breaches**, especially in organizations, affecting many people at once.

1. **How can you verify the sender’s authenticity?**

Verifying the sender’s authenticity is crucial to avoid falling for phishing or spoofed emails. Here are the main ways to do it:

**1. Check the Email Address Carefully**

* Look beyond the display name; inspect the actual email address.
* Phishers often use addresses that **look similar but have small differences**:
  + Example: support@paypa1.com instead of support@paypal.com.

**2. Hover Over Links**

* Hover (don’t click) over any link in the email to see the real URL.
* Ensure the link matches the legitimate website’s domain.

**3. Look at Email Headers**

* Advanced method: check the **full email header** to see the actual sender server and path.
* This can reveal if the email was **sent from an unauthorized server**.

**4. Verify Through Official Channels**

* If unsure, contact the company or person **directly using official contact info**, not any number or link in the email.

**5. Check Digital Signatures**

* Some organizations use **DKIM, SPF, or DMARC authentication**.
* Email clients like Gmail or Outlook sometimes show **“Verified” or “Signed by”** labels.

**6. Be Skeptical of Unusual Requests**

* Legitimate companies usually **don’t ask for passwords, OTPs, or sensitive info via email**.
* Requests for urgent action or secrecy are red flags.

✅ **Rule of Thumb:**

When in doubt, verify independently rather than trusting the email itself.

1. **What tools can analyze email headers?**

There are several tools—both online and software-based—that can help you **analyze email headers** to verify sender authenticity and detect spoofing or phishing. Here’s a list of commonly used tools:

**1. Online Email Header Analyzers**

* **MxToolbox Email Header Analyzer**
  + URL: https://mxtoolbox.com/EmailHeaders.aspx
  + Analyzes routing, IP addresses, SPF, DKIM, and DMARC records.
* **Google Admin Toolbox Messageheader**
  + URL: https://toolbox.googleapps.com/apps/messageheader/
  + Parses headers and shows the email’s path and authentication checks.
* **Mail Tester / Email Checker Tools**
  + Many sites allow you to paste headers and check for **suspicious sources or spoofing**.

**2. Email Clients’ Built-In Tools**

* **Gmail**
  + Click the three dots → “Show original” to see headers and authentication results.
* **Outlook**
  + Open message → File → Properties → Internet headers.

**3. Command-Line Tools (Advanced Users)**

* **dig, nslookup, or whois** to check the sender’s domain.
* **traceroute / ping** to inspect sending servers.

**4. Security Software & Email Gateways**

* Many enterprise email security platforms (e.g., Proofpoint, Mimecast) **analyze headers automatically** to detect spoofing or phishing.

1. **What actions should be taken on suspected phishing emails?**

If you receive a **suspected phishing email**, taking the right actions quickly can protect your personal information and your organization. Here’s a clear guide:

**1. Do Not Interact**

* **Do not click** on links or download attachments.
* **Do not reply** to the email.

**2. Verify the Sender**

* Check the email address and hover over links to see where they lead.
* Contact the organization **directly using official contact info** if unsure.

**3. Report the Email**

* **To your organization**: forward it to your IT/security team.
* **To authorities**: e.g., in the U.S., forward phishing emails to reportphishing@apwg.org.
* **Email providers**: Gmail, Outlook, etc., have “Report phishing” options.

**4. Mark as Spam or Phishing**

* Use your email client’s **“Mark as spam” or “Report phishing”** feature to block future attempts.

**5. Delete the Email**

* After reporting, **delete it from your inbox and trash**.

**6. Change Passwords if Necessary**

* If you accidentally clicked a link or entered credentials, **change your passwords immediately**.
* Enable **two-factor authentication (2FA)** on your accounts.

**7. Scan Your Device**

* Run a **full antivirus/malware scan** if you suspect an attachment may have been harmful.

1. **How do attackers use social engineering in phishing?**

Attackers use **social engineering** in phishing to **manipulate human psychology** rather than exploiting technical vulnerabilities. They trick people into taking actions that compromise security, like clicking malicious links or revealing sensitive information.