Task 2

Phishing

Phishing is a social engineering cyberattack that tricks people into giving up sensitive information, like passwords or bank details, by impersonating a trustworthy person or organization. Attackers use fraudulent emails, texts, websites, or phone calls to lure victims into clicking malicious links, downloading malware, or revealing their data, which is then used for identity theft or financial loss.

Sample Email

- HramazOn@gmail.com
- hrflipkart123@gmail.com

What is Phishing and How does it work?
The first thing you need to know about phishing scams is that it's not the same as hacking. Phishing scams are all about tricking people into giving up their personal information, like credit card numbers or online banking passwords, by masquerading as a trustworthy entity in an email or text message.

It's called "phishing" because the criminals are fishing for your sensitive data from behind a computer screen. It only takes one click on the wrong link for everything you care about-your cash, contacts, photos-to be gone forever!
Phishing emails often:

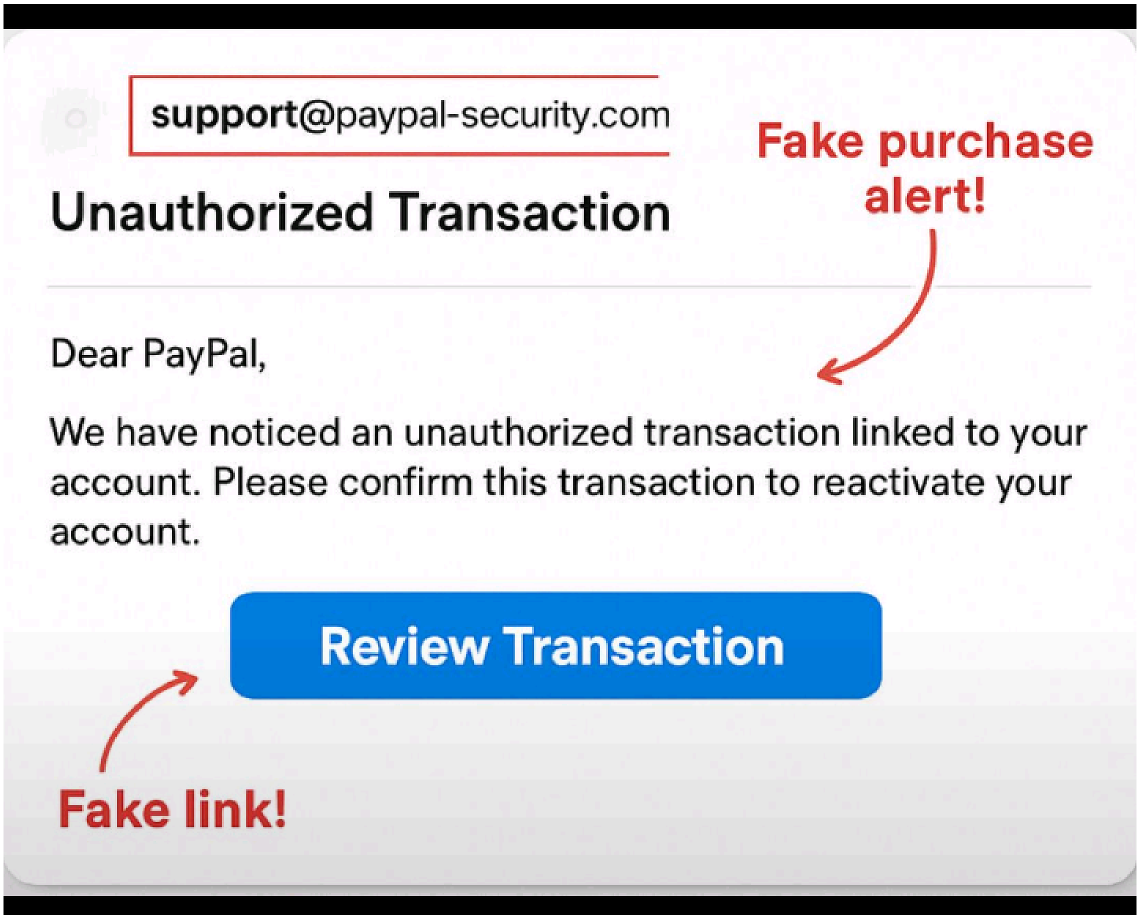
- Seem to be from legitimate companies like banks, internet service providers, credit card companies, etc.

- Are unsolicited (you didn't ask for it; they just sent it to you)

- Ask for things like usernames, passwords, account numbers, etc.

- Offer something seemingly valuable, like a prize or discount - Use poor spelling and grammar

- Have strange email addresses or typos in the email address - Have crazy titles



support@paypal-security.com

Unauthorized Transaction

Dear PayPal,

We have noticed an unauthorized transaction linked to your account. Please confirm this transaction to reactivate your account.

Fake purchase alert!

Fake link!