1. A text message claims to be from a courier, asking to pay a “re‑delivery fee” via a shortened link and requesting card OTP to confirm identity. What will you do?  
   (A) Open the link in incognito mode to check authenticity  
   (B) Delete the message and report the SMS as spam/phishing to the telecom and the courier’s official channel  
   (C) Reply asking for the delivery person’s number  
   (D) Share card OTP only after confirming the parcel number
2. A browser popup says your device is infected and urges downloading a “security cleaner” immediately; a phone number is displayed for “Microsoft Support.” What will you do?  
   (A) Call the number and follow instructions  
   (B) Close the browser, run trusted endpoint security, and report the domain to the IT/security team  
   (C) Download the cleaner but scan it before installing  
   (D) Ignore it and continue browsing risky sites to test if it reappears
3. An email appears from a colleague’s address asking you to urgently buy e‑gift cards and share the codes; the message has unusual grammar and no signature. What will you do?  
   (A) Purchase cards since the sender is known  
   (B) Reply asking which denominations to buy  
   (C) Verify out‑of‑band (phone/chat) and report as suspected account compromise; do not transact  
   (D) Forward the mail to friends to warn them
4. You receive a “KYC update” email with a bank‑like logo and an attachment “KYC\_Update.xlsm” requesting macros to be enabled. What will you do?  
   (A) Enable macros after saving the file  
   (B) Upload the file to a public malware scanner, then open it if clean  
   (C) Do not open; contact the bank through official channels, report the phishing attempt, and delete the mail  
   (D) Forward the file to coworkers to crowd‑check
5. A social media contact sends a shortened link promising a government subsidy; the landing page asks for Aadhaar, PAN, and bank login. What will you do?  
   (A) Enter only Aadhaar to see if it’s genuine  
   (B) Open the link on mobile data instead of Wi‑Fi  
   (C) Exit immediately, report the account for impersonation/phishing, and warn the contact via verified channel  
   (D) Share details because many friends liked the post
6. Your password manager flags a credential stuffed on a shopping site you rarely use; the same password secures your email. What will you do?  
   (A) Ignore because you rarely log in  
   (B) Change only the shopping site password later  
   (C) Immediately rotate unique passwords for all affected accounts, enable MFA, and review recent activity  
   (D) Close the shopping account and keep the email password unchanged
7. A caller claims to be from your bank’s “fraud desk,” knows your last four account digits, and asks for CVV to “cancel a suspicious transaction.” What will you do?  
   (A) Share CVV as proof of identity  
   (B) Ask the caller to email a confirmation first  
   (C) Hang up, call the bank using the number on the card/official site, and report a probable vishing attempt  
   (D) Continue the call but refuse to share OTP
8. A conference organizer you registered with emails a PDF invoice; on opening, it requests an “Adobe extension” from an external site to view. What will you do?  
   (A) Install the extension to access the invoice  
   (B) Upload the PDF to an online viewer to bypass the extension  
   (C) Do not install anything; verify the request via the organizer’s official portal and report the suspicious file  
   (D) Forward the PDF to your personal email to open at home
9. Your cloud drive receives a “shared document” from an unknown domain with a file name “Salary\_Revision\_2025.htm.” The link asks you to sign in again. What will you do?  
   (A) Provide credentials since the interface looks identical  
   (B) Try a decoy password first to test  
   (C) Close the tab; access your drive directly via bookmark to confirm any share and report the phishing site  
   (D) Save the link for later on a work chat
10. After selling a phone online, a buyer insists on paying via a QR code he sends on WhatsApp and asks you to “scan to receive money.” What will you do?  
    (A) Scan and enter UPI PIN to collect the payment  
    (B) Ask for a bank transfer screenshot as proof  
    (C) Refuse QR‑initiated “receive” scams; request verified pull‑payment (request money) or standard bank transfer and report the account if pressured  
    (D) Share only your UPI ID and proceed with the QR