Role of The Endpoint Protection:

The basic measure is installing antivirus and other endpoint security measures on user devices. Modern endpoint protection tools can identify and block obvious phishing messages, or any message that links to malicious websites or IPs listed in threat intelligence databases. They can also intercept and block malicious processes as they are executed on a user's device.

Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn't automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

Keep software and firmware regularly updated, particularly security patches. Don't run your phone rooted, or your network or PC in administrator mode. Even if a social engineering attack gets your user password for your 'user' account, it won't let them reconfigure your system or install software on it. Don't use the same password for different accounts. If a social engineering attack gets the password for your social media account, you don't want them to be able to unlock all of your other accounts too. For critical accounts use two-factor authentication so that just having your password isn't enough to access the account. That might involve voice recognition, use of a security device, fingerprinting, or SMS confirmation codes. If you just gave away your password to an account and think you may have been 'engineered', change the password straight away.