# Network Security Scenario Based Interview Questions

## Scenario 1

An employee receives a suspicious email with a link to a phishing website. How would you handle this situation to prevent a security breach?

## Scenario 2

A security vulnerability is identified in a critical network device. How would you prioritize & remediate this vulnerability to minimize the risk to organization?


## Scenario 3

A DDoS attack is targeting the company's network infrastructure. How would you respond to mitigate the impact of the attack & restore normal network operations?

## Scenario 4

A network intrusion is detected, and sensitive data may have been compromised. How would you contain the breach & initiate incident response procedures?

## Scenario 5

An audit reveals weak authentication practices across the network infrastructure. How would you strengthen authentication mechanisms to improve overall network security?

## Scenario 6

A zero-day vulnerability is discovered in a critical network application. How would you mitigate the risk posed by this vulnerability until a patch becomes available?


## Scenario 7

A mobile device containing sensitive company data is lost or stolen. How would you protect the data and prevent unauthorized access?

## Scenario 8

A company merger or acquisition is underway, and network integration is required. How would you ensure a seamless & secure transition while preserving data integrity & confidentiality?

## Scenario 9

A company's web server is targeted by a SQL injection attack, leading to unauthorized access to the database. How would you mitigate and prevent future incidents?


## Scenario 10

A company's network is targeted by a sophisticated Advanced Persistent Threat (APT) actor. How would you detect & respond to this persistent & stealthy threat?



Rashmi Bhardwaj