REPORT SUSPICIOUS ACTIVITY

Here are some situations where reporting suspicious activity is highly recommended:

Phishing Attempts: If you receive an email, message, or phone call that seems suspicious and requests sensitive information or directs you to click on unfamiliar links.

Unauthorized Access Attempts: If you notice repeated failed login attempts, unusual account activity, or signs of someone trying to gain unauthorized access to systems or accounts.

Malware or Ransomware Infections: If you suspect that your computer or network has been infected with malware or ransomware.

Unusual Network Traffic: If you observe unusual or suspicious network activity, such as large amounts of data being sent or received from unfamiliar sources.

Data Breaches: If you become aware of a potential data breach or unauthorized disclosure of sensitive information.

Social Engineering Attempts: If someone tries to manipulate or deceive you into revealing sensitive information, such as passwords or confidential data, report it immediately to prevent potential harm.

Unusual System Behavior: If you notice unexpected system errors, crashes, or other abnormal behavior that could be indicative of a security incident.

Physical Security Breaches: If you witness unauthorized individuals accessing secure areas, tampering with equipment, or engaging in suspicious activities, report it.