Reporting Suspicious Activity Guide

Early reporting is critical to incident response. The faster a potential threat is reported, the faster it can be investigated and contained. Every employee is a sensor in the security network — your report could prevent a major breach.

Key Points

- ✓ Report immediately — even if you are unsure it is a real threat
- ✓ No penalties for false alarms — under-reporting is far more dangerous
- ✓ Preserve evidence: do not delete, forward, or modify suspicious messages
- ✓ Document what you observed: time, what happened, any files or links involved
- ✓ Use designated reporting channels — not personal email or social media
- ✓ Follow up if you do not receive acknowledgment within the expected timeframe

Action Items

1. Save your security team's contact information in your phone and bookmarks
2. Learn how to use the "Report Phishing" button in your email client
3. Practice reporting a test scenario to familiarize yourself with the process
4. Share the reporting process with new team members during onboarding

Quick Reference

What to Report: Suspicious emails, unknown logins, lost/stolen devices, unauthorized access attempts, unusual system behavior, social engineering attempts.
How to Report: 1) Use the "Report Phishing" button for suspicious emails. 2) Call the security hotline for urgent issues. 3) Submit a ticket for non-urgent observations.
Information to Include: Date/time, description, screenshots if possible, affected systems, actions taken.