CROWDSTRIKE
business resilience

Best Practices

Security Awareness: Reporting Incidents

Organizations require security systems for their operations to run safely. It is essential to report an incident to reduce attacks that could put the organization in jeopardy. The organization's policies and standards outline the appropriate reporting circumstances.

What to Report

- Computer system breach
- Loss or theft of YubiKey, laptop or phone (includes BYOD and company-issued devices)
- Potential data mixing
- Suspicious emails
- Unauthorized access, use or change of systems, software or data
- Denial-of-service attack
- Interference with the intended use of IT resources
- Compromised user accounts
- Suspicious human activity:
    - A person — employee or otherwise — asking overly invasive questions or attempting to gain information or access to something they are not normally privy to, or that seems outside of their job duties; this might be a colleague at a conference, a coworker asking you about internal organizational operations, or someone reaching out on social media such as LinkedIn
- Is your situation not listed here? When in doubt, report it!

Where to Report

Organizations have multiple reporting channels for different reporting incidents linked to various security departments. It allows individuals to reach out directly — via email, phone and/or internal messaging platform, depending on the urgency and severity of the report.

For example:

- **Lost or stolen devices**: Start with your help desk — you may need the assistance of a colleague if you don't have access to your device
- **Physical security**: Escalate to management or your company's security team
- **Suspicious emails**: Forward the email to your company's phishing desk or help desk, or use a phishing report button if there's one available
- **Cyber incident concerns**: Notify your organization's incident response team or security team
- **Insider risk concern or suspicious human activity**: Report it to the ethics team if your company has one or report it to human resources

Note: Reporting to the correct team reduces the response and resolution time. Don't report to colleagues based on personal relationships.

No Risk in Reporting

You should feel safe reporting incidents and there should be no negative repercussions for reporting incidents. Even if you have done something you shouldn't have, it is better to report than keep quiet. After reporting an incident, you should receive an acknowledgement from the team working on its resolution.

Your Company's Reporting Policy

You should find instructions for reporting on your company's intranet or in its security policies. Keep in mind, you are the last line of defense — organizations depend on you to be open and vigilant. If you see something, say something.

Get more resources from CrowdStrike for creating your own Security Awareness Program →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

© 2024 CrowdStrike, Inc. All rights reserved.