digicert®

DDoS Crisis Communication: Rapid Response Checklist

This checklist ensures your team remains composed, transparent, and synchronized when your services are under fire.

Phase 1: Immediate Action (0–15 Minutes)

- [ ] Verify the Event: Confirm with Ops/NetSec that the outage is a DDoS attack and not a data breach.
- [ ] Activate the Status Page: Move your status to "Investigating" on your independent (off-site) status page.
- [ ] Deploy Holding Statement: Issue a pre-approved message via Social Media and Status Page.
  Draft Example: "We are aware of connectivity issues affecting [Service]. Our team is investigating, and we will provide an update in 30 minutes."
- [ ] Sync Internally: Send a "Flash Alert" to Support and Sales teams so they can use the same messaging for direct inquiries.

Phase 2: Active Mitigation (15–60 Minutes)

- [ ] Define the Narrative: Explicitly state: *"This is a service disruption; no customer data is at risk."*
- [ ] Set Update Cadence: Commit to updates every 30–60 minutes, even if the status is *"Ongoing."*
- [ ] Filter Specifics: Ensure no technical details (traffic size, specific IP ranges, or vendor names) are shared publicly.
- [ ] Empower Support: Provide scripts to the frontline to deflect ticket volume:
  "We are filtering malicious traffic; please follow our status page for real-time updates."

Phase 3: The Recovery (Intermittent Stability)

- [ ] Avoid "Fixed" Language: Do not declare a resolution yet. DDoS attacks often come in waves.
- [ ] Move to "Monitoring": Update status to:
  "Mitigation is active and services are recovering. We are monitoring for further instability."
- [ ] Internal Check: Confirm with the technical team that the attack traffic has dropped below the threat threshold for at least 30 minutes.

Phase 4: Post-Incident (1 Hour+ Post-Attack)

- [ ] The 60-Minute Rule: Only mark as *"Resolved"* after 60 minutes of sustained network stability.
- [ ] Final Post: Thank customers for their patience across all channels.
- [ ] The Reason for Outage (RFO): Within 24–48 hours, publish a high-level summary of the event and the steps taken to bolster future resilience.

Phase 5: Prevention & Prep (Ongoing)

- [ ] Test Off-Site Tools: Ensure all staff have logins for the third-party status page.
- [ ] Update Templates: Refine holding statements based on "what worked" during the last event.

About DigiCert

DigiCert is a global leader in intelligent trust, securing people, data, and devices with AI-powered solutions built to stop threats today and prepare for a quantum-safe future.