ONE-PAGE REFERENCE

Holiday Cyber Readiness Checklist

Print it, assign owners, and date each item as it closes.

PRE-HOLIDAY PREPARATION — 30 DAYS OUT

- ❑ List crown-jewel systems and name an owner for each
- ❑ Identify and confirm critical third-party contacts
- ❑ Verify cyber insurance, IR retainer, legal and PR contacts
- ❑ Validate alternate communication channels (out-of-band)
- ❑ Patch internet-facing systems, prioritizing known-exploited vulnerabilities
- ❑ Enforce phishing-resistant MFA on remote access and privileged accounts
- ❑ Disable unused remote access paths (RDP, legacy VPN)
- ❑ Review SPF, DKIM, and DMARC; enable impersonation protection
- ❑ Rehearse service desk identity verification for password and MFA resets
- ❑ Require out-of-band verification for all banking and payment changes
- ❑ Validate offline or immutable backups are isolated from domain credentials
- ❑ Perform a timed restore test of a crown-jewel system
- ❑ Confirm logging coverage and retention for identity, endpoint, and remote access
- ❑ Conduct a holiday ransomware tabletop exercise
- ❑ Publish the holiday on-call roster, escalation tree, and IR playbook
- ❑ Pre-approve emergency security patching during the change freeze

DURING THE HOLIDAY WINDOW

- ❑ Monitor unusual VPN and remote access activity
- ❑ Check for MFA fatigue attempts and abnormal login locations
- ❑ Watch for privileged group and role assignment changes
- ❑ Detect new mailbox forwarding, rules, and delegation changes
- ❑ Monitor large outbound data transfers and mass file access
- ❑ Freeze non-critical changes; require approval for emergency changes
- ❑ Confirm daily that monitoring and alerting pipelines are healthy
- ❑ Re-send employee reporting instructions before each holiday break

IF AN INCIDENT OCCURS

- ❑ Isolate affected devices and disable compromised accounts
- ❑ Block known-malicious IPs and domains
- ❑ Notify security leadership immediately
- ❑ Engage the IR retainer or cyber insurer — HALOCK hotline 800.925.0559
- ❑ Capture logs, memory, and snapshots before remediation
- ❑ Start the notification clock; involve legal counsel early
- ❑ Report to FBI IC3 or CISA where required or beneficial
- ❑ Schedule the after-action review before the team disperses

HALOCK Security Labs · Incident Response Hotline 800.925.0559 · Reasonable security, measured against duty of care.