iS2 DIGITAL

Website Hacked... **Recovery Playbook** for SMBs

☑ Step 1: Immediate Containment

1. **Isolate the Website**
   - Take the website and server offline
   - Notify internal stakeholders, hosting company
2. **Assess the Situation**
   - Scan for malware and other signs of hacking
   - Check server and user activity logs
3. **Change All Passwords**
   - Update website and hosting passwords
   - Enforce strong password policies

☑ Step 2: Thorough Remediation

1. **Identify the Root Cause(s)**
   - Analyze logs for suspicious patterns
   - Identify unauthorized logins, uploads, or changes
2. **Fix or Backup**
   - Update all website and server software
   - Restore from clean backup or fix hacked code
3. **Relaunch and Test**
   - Restore the website and monitor for anomalies
   - Confirm all functionality is working as expected

☑ Step 3: Restoration and Recovery

1. **Strengthen Security**
   - Use a CDN and Web Application Firewall (WAF)
   - Implement backup retention policies and MFA
2. **Notify Stakeholders and Customers**
   - Update customers, clients, and vendors
   - Address legal and data privacy issues
3. **Fix Reputation**
   - Review and respond to social and search engine fallout
   - Mend and improve brand perception through story and action