Template: Remote Work Cybersecurity Checklist

Generated: 2/18/2026

Based on Article: "Top Cybersecurity Tools for Protecting Remote Work Environments"
Website: https://remotesuccesshub.com/

A practical checklist for remote employees to enhance cybersecurity and protect sensitive data.

Checklist Items:

- [ ] **1. Keep Devices Patched**
  Apply operating system and application updates within days to ensure all vulnerabilities are fixed promptly.
  Reference Section: Core security principles every remote professional must master

- [ ] **2. Use Strong Authentication**
  Enable Multi-Factor Authentication (MFA) for every account that supports it to add an extra layer of security.
  Reference Section: Core security principles every remote professional must master

- [ ] **3. Segment Work Data**
  Store company files only in approved cloud locations to avoid accidental exposure of sensitive information.
  Reference Section: Core security principles every remote professional must master

- [ ] **4. Report Suspicious Activity**
  Immediately escalate odd emails or alerts to your IT security team to mitigate potential threats.
  Reference Section: Core security principles every remote professional must master

- [ ] **5. Implement Endpoint Protection**
  Use reputable endpoint protection solutions like CrowdStrike Falcon or Microsoft Defender to detect and block malware.
  Reference Section: Core security principles every remote professional must master

- [ ] **6. Utilize a VPN**
  Adopt a Virtual Private Network (VPN) for encrypted access to company resources, especially while using public Wi-Fi.
  Reference Section: Core security principles every remote professional must master

- [ ] **7. Harden Device Security Settings**
  Disable unused services and enable built-in firewalls on work devices to minimize attack surfaces.
  Reference Section: Core security principles every remote professional must master

- [ ] **8. Regularly Monitor Endpoints**
  Run regular reviews of endpoint alerts and adjust settings as necessary to maintain security integrity.
  Reference Section: Core security principles every remote professional must master

- [ ] **9. Conduct Phishing Tests**
  Organize short phishing simulations to educate employees on recognizing and reporting phishing attempts.
  Reference Section: Operational practices and habits that reinforce tools

- [ ] **10. Train Continuously**
  Engage in ongoing security training to stay updated on the latest cybersecurity threats and best practices.
  Reference Section: Operational practices and habits that reinforce tools