While cyber hygiene isn’t ironclad protection, it’s important for everyone in contact with your network, from the CEO to the lowly intern, to act securely with these ten tips:

1. **KEEP AN INVENTORY OF HARDWARE AND SOFTWARE ON THE COMPANY NETWORK**

2. **DEVELOP A PROCESS FOR SOFTWARE INSTALLATION BY END USERS**
   That could include limiting installation of trusted software or prohibiting and blocking all installation without prior approval from IT.

3. **EDUCATE USERS ON PRACTICING GOOD CYBER BEHAVIOR**
   Including password management, identifying potential phishing efforts, and which devices to connect to the network.

4. **IDENTIFY VULNERABLE APPLICATIONS THAT AREN’T IN USE AND DISABLE THEM**

5. **CONSISTENTLY BACK UP DATA AND KEEP MULTIPLE COPIES**
   Consider using a secure cloud solution as well as on premise.

6. **TURN TO INDUSTRY-ACCEPTED SECURE CONFIGURATIONS/STANDARDS LIKE MITRE, NIST, AND CIS BENCHMARK**
   These can help organizations define items like password length, encryption, port access, and double authentication.

7. **PATCH ALL APPLICATIONS RIGHT AWAY—REGULARLY**
   Unpatched systems are one of the biggest risk factors in attacks.

8. **MAINTAIN HIGH STANDARD PASSWORD POLICY**

9. **LIMIT THE NUMBER OF USERS WITH ADMINISTRATIVE PRIVILEGES**

10. **UPGRADE AGING INFRASTRUCTURE AND SYSTEMS**

---

**by SentinelOne**