SCHOOL CYBERSECURITY BEST PRACTICES CHECKLIST

CyberNut

1. Network Security

- ◯ Ensure firewalls are configured to block unauthorized traffic
- ◯ Enable intrusion detection/prevention systems (IDS/IPS)
- ◯ Conduct regular vulnerability scans on school networks
- ◯ Enforce network segmentation (separate student/staff networks)
- ◯ Implement DNS filtering to block malicious sites

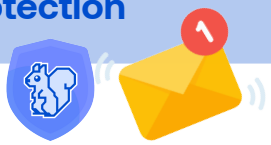
2. Account & Access Management

- ◯ Require multi-factor authentication (MFA) for all admin accounts
- ◯ Enforce strong password policies (length, complexity, expiration)
- ◯ Implement role-based access control (RBAC) for staff and students
- ◯ Set automatic account lockouts after failed login attempts
- ◯ Regularly audit user access & remove inactive accounts

3. Device & Endpoint Security

- ◯ Ensure all devices have endpoint protection & antivirus software
- ◯ Enable automatic software & OS updates on all school-owned devices
- ◯ Restrict USB and removable media access to prevent data theft
- ◯ Deploy mobile device management (MDM) for remote monitoring
- ◯ Require full-disk encryption for staff and admin laptops

4. Email & Phishing Protection



- ◯ Configure DMARC, SPF, and DKIM to prevent email spoofing
- ◯ Implement phishing simulation training for staff & students
- ◯ Enable email filtering to block spam & malicious attachments
- ◯ Use safe browsing tools to prevent credential theft
- ◯ Implement a real-time threat reporting system to streamline user-reported attacks, rapidly remove malicious emails, and reinforce ongoing security awareness.

***CyberNut** provides phishing simulation training and a real-time threat reporting system.*

START YOUR FREE PHISHING AUDIT HERE

5. Data Protection & Compliance

- ◯ Encrypt sensitive student & staff data (both in transit & at rest)
- ◯ Ensure backups are performed daily and stored securely
- ◯ Regularly test data recovery procedures
- ◯ Implement data retention & deletion policies
- ◯ Comply with FERPA, CIPA, and COPPA regulations

6. Incident Response & Disaster

- ◯ Develop a cybersecurity incident response plan
- ◯ Conduct quarterly security drills (ransomware, data breach scenarios)
- ◯ Ensure staff knows who to contact in case of a cyber incident
- ◯ Maintain cyber insurance coverage for potential breaches
- ◯ Review & update disaster recovery plans annually