CORPORATE TECHNOLOGIES LLC
gocorptech.com

CYBERSECURITY BASICS FOR NON-TECH STAFF CHECKLIST

Executive Tool for Reducing Human Cyber Risk

Built for business leaders and department managers. Use this checklist to reduce employee-driven security risk and improve awareness.

How to Use

1. Takes 20–30 minutes
2. Check each box that applies
3. Count the total number of checked items
4. Identify human-driven security exposure

1

Security Awareness Training

- ☐ Provide annual security awareness training
- ☐ Train staff on phishing recognition
- ☐ Require acknowledgment of security policies
- ☐ Test employees with phishing simulations
- ☐ Document training completion records
- ☐ Update training content annually

2

Password & Access Practices

- ☐ Require strong password standards
- ☐ Enforce multi-factor authentication
- ☐ Prohibit shared user accounts
- ☐ Review user access permissions quarterly
- ☐ Disable inactive user accounts
- ☐ Restrict admin privileges to essentials

3

Email & Phishing Protection

- ☐ Enable advanced email filtering
- ☐ Block malicious attachments automatically
- ☐ Flag external email senders clearly
- ☐ Report suspicious emails to IT
- ☐ Review phishing incident reports
- ☐ Test phishing response procedures

4

Device & Workstation Security

- ☐ Install antivirus on all devices
- ☐ Enable automatic system updates
- ☐ Encrypt laptops and mobile devices
- ☐ Lock screens after inactivity
- ☐ Restrict software installation rights
- ☐ Audit unauthorized applications

5

Data Handling & Protection

- [ ] Define data classification standards
- [ ] Limit access to sensitive files
- [ ] Use secure file-sharing tools
- [ ] Prohibit personal cloud storage use
- [ ] Back up critical business data
- [ ] Test data restoration procedures

6

Incident Reporting & Response

- [ ] Document incident reporting steps
- [ ] Assign internal security contact
- [ ] Require immediate breach reporting
- [ ] Test incident response workflow
- [ ] Log reported security events
- [ ] Review incidents for patterns

Scoring Model

- Count the total number of checked items
- Total Possible Score: 36
- 0–12 → High Risk
- 13–29 → Moderate Risk
- 30–36 → Controlled / Aware

Immediate Red Flags

- No employee security training
- No MFA enforcement
- Shared user accounts in use
- No phishing protection enabled
- No data backup verification
- No incident reporting process

Next Step

If your score indicates exposure, schedule a Security Awareness & Risk Review.

Security Awareness & Risk Review