



Cybersecurity Checklist

1. Enforce Multi-Factor Authentication (MFA)

- ☐ Require MFA on email, payroll, HR, banking, and accounting systems.
- ☐ Blocks most of the credential-theft and account-takeover attacks.

2. Use Callbacks for All Financial Changes

- ☐ Verify direct deposit changes, vendor bank updates, and payment instructions by phone using a known number.
- ☐ Never rely solely on email for financial approvals.

3. Implement Segregation of Duties

- ☐ Separate payroll processing, vendor setup, payment approval, and bank reconciliation.
- ☐ Prevents internal fraud and reduces error risk.

4. Adopt Positive Pay & Payee Validation

- ☐ Use bank-provided tools to detect counterfeit, altered, or unauthorized checks.
- ☐ Essential for small businesses still issuing paper checks.

5. Reduce Paper Checks Wherever Possible

- ☐ Move to direct deposit, digital pay, or secure electronic payments.
- ☐ Minimizes exposure to mail theft, check washing, and duplicate mobile deposits.

6. Strengthen Email Security

- ☐ Train employees to spot phishing and impersonation attempts.
- ☐ Enable DMARC/SPF/DKIM to reduce spoofing.
- ☐ Monitor for forwarding rules and unusual login activity.

7. Require Dual Approval for Payments

- ☐ Apply two-person approval for wires, ACH transfers, vendor setup, and off-cycle payroll.
- ☐ Stops both internal and external fraud attempts.

8. Maintain a Verified Vendor Master File

- ☐ Validate vendor identities, bank accounts, and contact information.
- ☐ Review changes through independent verification.

9. Patch, Back Up, and Protect Systems

- ☐ Keep payroll, HR, and accounting systems updated.
- ☐ Use endpoint protection and maintain offline or immutable backups.
- ☐ Critical for ransomware resilience.

10. Conduct Regular Audits & Monitoring

- ☐ Review payroll changes, vendor activity, bank reconciliations, and access logs.
- ☐ Detects fraud early and strengthens accountability.

For more information:

commpayhr.com
877-245-1159
sales@commpayhr.com

