Protecting Contractors from Cyber Hacks

1. Strengthen Email Verification and Payment Procedures

- Most contractor-related breaches begin with **business email compromise (BEC)**
- hackers impersonate an owner, PM, or vendor to redirect payments.
- Require **two-step verification** for *any* payment change, wire transfer, or banking update **never approve based on email alone**.
- Use a documented process: phone verification to a known number, not one provided in an email.

2. Mandate Strong Passwords and Multi-Factor Authentication

- Hackers often gain access through weak or reused passwords.
- Require **MFA** on email, project management platforms, and accounting systems.
- Encourage password managers to create and store strong, unique passwords for every employee.

3. Train All Staff and Subs on Phishing Awareness

- Phishing emails now look extremely legitimate and often target busy field staff or office personnel handling payments.
- Regularly share examples of suspicious emails: odd sender addresses, urgent requests, slightly altered domain names.
- Remind crews: **"When in doubt, don't click."** Report anything questionable to IT or leadership.

4. Protect Jobsite Devices and Remote Access

- Tablets, laptops, and phones are now core tools for contractors—and prime targets for hackers.
- Require device passcodes, auto-locking, encrypted storage, and approved apps only.
- Ensure VPN or secure remote access for anyone logging into company systems offsite.

5. Keep Systems Updated and Backed Up

- Outdated software is one of the easiest entry points for attackers.
- Set automatic updates on all devices and ensure firewalls/antivirus tools stay current.
- Maintain **offline or immutable backups** of financial, project, and communication data to recover quickly if systems are compromised.

Contractor Cybersecurity Checklist

1. Email & Communication Security

- ☐ Verify any **payment requests** or banking changes with a phone call to a known number (never rely on email alone).
- ☐ Inspect sender addresses for misspellings or unusual domains.
- ☐ Be cautious of urgent, unexpected, or poorly written messages.
- ☐ Report suspicious emails to your IT lead immediately.

2. Passwords & Account Protection

- ☐ Use **unique, complex passwords** for all accounts.
- ☐ Enable **Multi-Factor Authentication (MFA)** on email, project management systems, and financial platforms.
- ☐ Use a **password manager** (1Password, Bitwarden, etc.).
- ☐ Never share passwords with coworkers or subs.

3. Device & Jobsite Security

- ☐ Require passcodes or biometric locks on all smartphones, tablets, and laptops.
- ☐ Auto-lock devices after short inactivity periods.
- ☐ Keep company data off personal devices whenever possible.
- ☐ Use secure Wi-Fi or a VPN—avoid public Wi-Fi networks.
- ☐ Store devices securely when unattended on jobsites.

4. Software & System Updates

- ☐ Turn on **automatic updates** for operating systems, browsers, and apps.
- ☐ Ensure antivirus and firewall protections are current.
- ☐ Regularly update project management and accounting platforms.

5. Vendor & Subcontractor Requirements

- ☐ Require subs to follow basic cyber hygiene practices.
- ☐ Confirm vendors use MFA and secure portals for exchanging sensitive documents.
- ☐ Avoid sending sensitive plans, bids, or financial data over unsecured email.

6. Backups & Data Protection

- ☐ Back up critical files daily or weekly.
- ☐ Keep at least one **offline** or cloud-protected backup.
- ☐ Encrypt sensitive data, especially financial and employee information.

7. Training & Awareness

- ☐ Conduct brief quarterly training on recognizing phishing and scams.
- ☐ Share examples of recent fraud attempts in the industry.

- ☐ Encourage a culture of "**Think Before You Click**."

8. Incident Response Readiness

- ☐ Create a simple incident response plan (who to call, what to isolate, what to document).
- ☐ Know how to disconnect a compromised device from the network quickly.
- ☐ Maintain updated contact information for IT support, banks, and cyber-insurers.

9. Financial Safeguards

- ☐ Use dual approval for large payments or wire transfers.
- ☐ Monitor accounting systems for unusual activity.
- ☐ Change default passwords on banking portals and equipment.

10. Insurance & Legal Preparedness

- ☐ Review your **cyber liability insurance** annually.
- ☐ Document compliance with basic cybersecurity practices (often required for claims).
- ☐ Know state and federal breach notification rules.