

FRAUD AWARENESS & PREVENTION

Business Protection Checklist

STOP

Don't click, reply, or act immediately.

EVALUATE

Verify requests using a trusted source.

TALK TO YOUR BANKER

Contact your local banker or a trusted advisor.

STRENGTHEN ACCESS & SECURITY

- ☐ Enable Multi-Factor Authentication (MFA)
- ☐ Use strong, unique passwords (12+ characters)
- ☐ Keep software and devices updated
- ☐ Limit access based on employee roles
- ☐ Use antivirus and endpoint protection
- ☐ Never share login credentials

PROTECT PAYMENTS & ACCOUNTS

- ☐ Verify all payment instruction changes using a trusted source
- ☐ Require dual approval for ACH and wire transactions
- ☐ Review account activity and reconcile accounts regularly
- ☐ Set up account alerts
- ☐ Use gel pens when writing checks
- ☐ **Enroll in positive pay for check fraud protection and ACH debit block**

TRAIN EMPLOYEES

- ☐ Educate staff about phishing, vishing, and smishing scams
- ☐ Verify unusual requests for money or information
- ☐ Discuss Business Email Compromise (BEC)
- ☐ Encourage reporting of suspicious activity

PREPARE FOR INCIDENTS

- ☐ Maintain an internal fraud response plan
- ☐ Keep bank, IT, and law enforcement contacts readily available
- ☐ Review user access and permissions regularly

Red Flags to Watch For

- Urgent requests requiring immediate action
- Requests for passwords or security codes
- Unexpected requests for wire transfers
- Requests for secrecy or confidentiality
- Changes to vendor payment instructions
- Suspicious links or attachments