# Business Fraud Toolkit

Best practices for small businesses and accounting teams

### Common Fraud Risks for Businesses

Business Email Compromise (BEC) scams requesting wire transfers or sensitive data.
Payment fraud — fake invoices, altered account details, or unauthorized charges.
Insider threats — employees misusing access to accounts or data.
Vendor fraud — impersonation of suppliers with fraudulent payment instructions.
Phishing emails targeting accounting staff with malicious links or attachments.

### Best Practices for Prevention

Always verify payment requests by phone using a known number — never trust only email.
Use dual approval for wire transfers, ACH, and large transactions.
Reconcile bank statements and accounts daily to spot suspicious activity quickly.
Train employees regularly on fraud awareness and phishing red flags.
Limit access rights — give staff only the access they need to perform their roles.
Keep software and antivirus programs up to date across all devices.

### Accounting Team Safeguards

Require strong passwords and multi-factor authentication for accounting software.
Segregate duties — no single employee should control all aspects of a transaction.
Confirm changes to vendor payment details through a second trusted channel.
Store sensitive documents securely and restrict access to financial records.
Report suspicious activity immediately to the bank and law enforcement if necessary.

### Response Plan if Fraud is Suspected

Stop the payment or transaction immediately if possible.
Notify your bank's fraud department right away.
Gather evidence: emails, invoices, account logs.
Report to local law enforcement and, if applicable, the FBI's IC3.gov.
Review internal controls and strengthen policies to prevent future fraud.

💡 **Pro Tip: Fraud prevention isn't just about technology — it's about people and process. Strong internal controls, staff awareness, and clear reporting channels are the best defense.**

Cybersecurity Awareness Month
October 2025