Protect your business from scams and fraud

Safeguard your time, reputation, and bottom line.

Small businesses are essential to strong communities. But scammers know that limited time and lean teams make them vulnerable. Nearly half of all cyber breaches hit businesses with fewer than 1,000 employees (Verizon Data Breach Investigations Report).

Your best defense?
Awareness, preparation— and action.

Common scams targeting small businesses

Fake invoices/ supplier bills	Bills for goods/services the business never ordered.
Phishing/ social engineering	Phone calls, emails, or other communication channels are used to gather personal information, often by impersonating individuals or organizations.
Business email compromise scams	Scammers persuade employees to transfer payment to another bank account. These can be perpetrated via email, text, phone calls, or other communications.
Bank/credit card company imposters	Scammers persuade their targets to share credit card or banking information.
Government imposters	Fake calls or emails claiming license, tax, or compliance issues.
Tech support scams	Fraudsters claim urgent tech issues to access systems.
Directory listing & advertising scams	Paying for ads or listings that don't exist.

Red flags to watch out for:

- **Unsolicited contacts** demanding urgent payment or sensitive information.
- **Requests for payment** via wire transfer, prepaid gift cards, or overpayment by check.
- **Too-good-to-be-true offers** or surprise awards.
- **Urgent deadlines** creating pressure to act quickly.
- **Threats** of penalties, fines, or legal action for non-compliance.
- **Requests for sensitive** business or financial information.

BBB

Tips for protecting your business:

- **Train your team.** Regularly update your staff on common fraud tactics and internet safety.
- **Confirm the identity of anyone who calls or emails requesting money or authorizing the transfer or expenditure of money.** Remember, scammers create official-looking seals and logos, spoof phone numbers, emails, and URLs, and even impersonate your leadership team.
- **Verify invoices and payments to ensure they are authentic.** Create clear procedures for approving invoices and limit the number of people who are authorized to place orders or pay invoices.
- **Back up files and update software.**
- **Don't click on suspicious links ANYWHERE or open attachments.**
- **Only work with verified lenders.**
- **Stay informed.** Regularly check official government websites and reputable business associations for updates on actual requirements and known scams.
- **Use official sources.** For any government filings or renewals, always use the official government websites or offices directly.
- **Reevaluate your cybersecurity measures and email authentication protocols:**
  - ☑ Flag messages from unknown senders for your security team.
  - ☑ Use robust firewalls.
  - ☑ Update antivirus software.
  - ☑ Use multi-factor or two-factor authentication.
  - ☑ Secure files, passwords, and financial information.

What to do if your business experiences a scam

1. **Contact your bank immediately** if you shared financial information or made a payment.
2. **Report the scam to BBB Scam Tracker SM** (all reports are shared with the Federal Trade Commission). Your business name and personal information will not be published.
3. **File a report** with your local police department and your state's Attorney General's office.
4. **Inform industry associations and nearby businesses** to help make others aware of the scam.
5. **Check the BBB Scam Survival Toolkit** for guidance on important next steps.