Top Fraud Threats to Small Businesses

Small businesses are attractive targets for fraudsters due to limited resources, fewer security measures, and employees handling multiple responsibilities. These factors make fraud detection more difficult, increasing the risk of financial losses and cyberattacks.

- **Business Email Compromise (BEC)** – Impersonation emails tricking employees into wiring money.
- **Cybersecurity Threats** – Phishing, ransomware, malware, and data breaches.
- **Financial Fraud** – Check fraud, ACH fraud, wire fraud, credit card fraud.
- **Insider Threats** – Employee fraud, vendor fraud, payroll fraud.
- **Social Engineering Scams** – Fake invoices, impersonation calls, fraudulent business opportunities.

Business Email Compromise (BEC) Scams

How It Works:

- Scammers impersonate executives, vendors, or clients.
- Fake emails request urgent wire transfers or sensitive data.
- Often looks like a real email due to spoofing techniques.

Red Flags

- Unusual payment requests or last-minute changes.
- Sense of urgency and secrecy.
- Slight misspellings in email addresses or domains.

Prevention Tips:

- Verify requests via a second channel (phone, in-person).
- Train employees to spot email spoofing and phishing.
- Implement multi-factor authentication (MFA).

Cybersecurity Best Practices for SMBs

- **Use Strong, Unique Passwords & MFA** – Avoid weak passwords and use a password manager.
- **Educate Employees** – Regular training on phishing, scam emails, and safe browsing.
- **Keep Systems Updated** – Install security patches for operating systems and software.
- **Limit Employee Access** – Only give employees access to what they need.
- **Backup Data Regularly** – Prevent ransomware damage with secure backups.

Financial Fraud & Payments Security

Common Payment Fraud Scams:

- **ACH & Wire Fraud** – Unauthorized transactions due to social engineering.
- **Check Fraud** – Altered or forged checks.
- **Invoice & Vendor Fraud** – Fake bills from fraudsters posing as suppliers.

How to Protect Your Business:

- Implement dual approval for payments.
- Regularly reconcile accounts to spot unauthorized activity.
- Verify new vendors via a second communication channel.
- Use positive pay services with your bank.

Insider Fraud – Employees & Vendors

Common Types:

- **Payroll Fraud** – Ghost employees, falsified overtime.
- **Expense Fraud** – Fake reimbursements.
- **Vendor Fraud** – Fake invoices or kickbacks from suppliers.

How to Reduce Risk:

- Require background checks on employees & vendors.
- Separate financial duties (checks & balances).
- Conduct surprise audits.
- Implement anonymous reporting for whistleblowers.

Social Engineering Scams

Scammers Exploit Human Psychology to Trick Businesses

Popular Social Engineering Tactics:

- Fake CEO or vendor calls requesting payments.
- Phishing emails appearing to be from known contacts.
- Tech support scams claiming your system is infected.

How to Protect Your Business:

- Question Unusual Requests – Call to confirm before acting.
- Train Employees – Awareness is key!
- Use Call-Back Verification – Don’t rely on caller ID