Small Business Fraud: Common Scams & How to Stay Safe

Running a small business comes with many responsibilities, including protecting your company from fraud. Scammers often target small businesses due to their limited security resources, but being aware of potential risks can help you stay one step ahead. Here are some common fraud schemes targeting small businesses, and some tips that can help you stay safe.

Common Small Business Scams

- **Check Fraud & Payment Security** – Mail theft often leads to check fraud where scammers alter, or forge checks to steal money from business accounts.
  Prevention Tips:
  - Use ACH payments or online bill pay instead of mailing checks.
  - Implement Positive Pay with your financial institution to help identify fraudulent checks.
  - Review bank transactions daily to spot unauthorized activity quickly.

- **Fake Invoices & Vendor Fraud** – Fraudsters send fake invoices hoping businesses will pay without verification.
  Prevention Tips:
  - Require verification for all invoices.
  - Maintain a list of approved vendors.
  - Cross-check invoices with purchase orders.
  - Verify new vendors before conducting business.

- **Business Email Compromise (BEC)** – Scammers impersonate executives, vendors, or employees through fake emails to trick businesses into sending funds or disclosing sensitive information.
  Prevention Tips:
  - Verify all payment requests through a second communication method.
  - Train employees to recognize phishing emails.
  - Use multi-factor authentication (MFA) for email accounts.

- **Phishing Scams**– Scammers prey on unsuspecting individuals by leveraging various techniques to compromise personal information, devices, and even financial assets.
  Prevention Tips:
  - Don't open any links, or call the numbers provided in the text or email.
  - Call that company or person directly. Use a number you know to be correct, not the number in the email or text.

- **Tech Support Scams** - Scammers pose as technical support representatives, targeting unsuspecting individuals to gain access to their personal or financial information and computer systems. They often lead to device compromise, identity theft, and monetary loss.
  Prevention Tips:
  - Do not grant remote access to your computer or device.
  - Ask for identification. Call back using only official contact information.
  - NEVER share sensitive information.

- **Gift Cards -** Scammers want you to pay with gift cards because they're like cash. Once you use a gift card, the money's gone, and it's easier to hide your trail.
  Prevention Tips:
  - Gift cards are only for gifts. Not for payments.
  - Be skeptical of urgent demands for payment.
  - The caller usually tells you which gift card to buy and sometimes they tell you to buy cards at several stores.
  - Never provide gift card numbers: or codes to someone over the phone, in a text, or via email.

- **Cyber Attacks & Data Breaches** – Hackers target small businesses with ransomware, malware, and phishing schemes to steal data or demand payment.
  Prevention Tips:
  - Keep software and security systems updated.
  - Train employees on cybersecurity best practices.
  - Back up critical data regularly.
  - Limit access to confidential data and ensure proper encryption.
  - Check if You've Been Affected: Use free tools like https://haveibeenpwned.com/

- **Device Management:** Gateways to our digital existence, holding sensitive information and serving as keys to unlock our devices.
  Prevention Tips:
  - Enable Multi-Factor Authentication and use strong, unique passwords.
  - Beware of Phishing attempts.
  - Regularly review account activity and keep software and firmware updated.

- **STAY ALERT** – Falling victim to a scam can be upsetting, frustrating, and even a little embarrassing. But remember – you're not alone, and there are steps you can take to protect yourself moving forward:

  - Secure the affected accounts immediately.
  - Report identity theft if any personal information is compromised.
  - Report to the Authorities.
  - Report the scam and file with the FTC (https://reportfraud.ftc.gov.)

- **Stay Alert for Follow-Up Attacks:** Scammers may try to exploit the situation further:
  - Watch for fake "help desk" calls claiming to fix the problem.
  - Be wary of follow-up emails pretending to offer refunds or solutions.
  - Monitor your accounts for unusual activity in the coming weeks.

The most important note is to stay vigilant and stay educated on current fraud trends. Education is key to prevention.