Protecting Your Small Business from Spoofing Scams

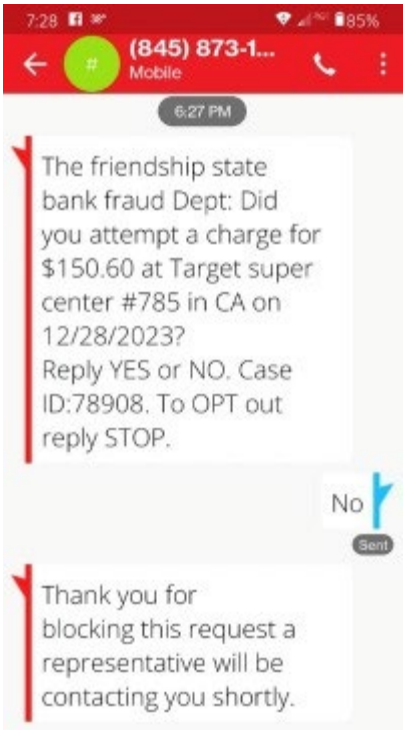
As small business owners, it's crucial to ensure that your staff are well-trained to recognize and avoid spoofing scams. Local businesses have reported incidents where employees fell victim to these scams, putting their business at risk. Equip your team with the knowledge and tools to safeguard your business from these deceptive tactics.

Understanding Spoofing
Spoofing is a type of scam where criminals disguise communication elements to trick individuals into believing they are interacting with a known, trusted source. This can involve deceptive emails, false display names, manipulated phone numbers, misleading text messages, or fraudulent website URLs.

Identifying Spoofing Tactics
To prevent spoofing, your employees need to be vigilant in spotting common tactics used by scammers:

- ***Emails and Text Messages:***
  Scammers may send emails or text messages that appear to come from reputable sources like financial institutions or other trusted business partners. For example, they might mimic official bank communications or use a phone number similar to your bank's number.
- ***Phone Calls:***
  Be cautious of phone calls that seem unusual or ask for sensitive information. Spoofed calls often use fake caller ID information to appear legitimate.
- ***Websites:***
  Fraudulent websites can look almost identical to the real ones. Always check the URL for slight variations that might indicate a fake site.

Here is an example of a spoofing attempt: A scammer manipulated a text to appear as if it came from The Friendship State Bank Fraud Department. Note the typos and the unfamiliar phone number. Always verify such messages directly with the bank.



Other Spoofing Tactics to Watch Out For
Spoofers don't just pretend to be financial institutions. They often pose as other trusted entities to deceive employees. Be aware of these common spoofing methods:

- ***Impersonating Business Partners:***
  Scammers may pose as vendors, suppliers, or business partners. They might send fake invoices or request payment details, tricking employees into transferring money to fraudulent accounts.
- ***Pretending to be Executives:***
  Known as "CEO fraud" or "Business Email Compromise (BEC)," this tactic involves scammers sending emails that appear to be from the company's executives, instructing employees to make urgent wire transfers or reveal sensitive information.
- ***Fake IT Support:***
  Spoofers might impersonate IT support staff, asking employees to provide login credentials or install malicious software under the guise of a security update.
- ***Government Impersonation:***
  Scammers might pose as officials from tax authorities, regulatory bodies, or other government agencies, threatening fines, or legal action to extract sensitive information or payments.

Practical Measures to Protect Your Business

1. Educate Your Employees
- Conduct regular training sessions on recognizing spoofing attempts.
- Share real-life examples and teach them to look for red flags such as typos, unfamiliar phone numbers, and suspicious URLs.

2. **Foster a Culture of Vigilance**

- Encourage employees to share any suspicious communications they receive.
- Create a supportive environment where they feel comfortable reporting potential threats without fear of reprisal.

3. Strengthen Relationships with Your Bank and Other Trusted Partners
- Regularly communicate with your bank and business partners to verify any suspicious communications.
- Inform your staff that trusted entities will never ask for sensitive information via phone, text, or email.

4. Monitor Financial Accounts Regularly
- Implement a routine check of business accounts for any unauthorized transactions.
- Use account alerts to receive notifications of unusual activity.

5. Report Suspicious Activity Promptly
- Train your employees to immediately report any suspicious activity to the appropriate person within your business.
- Contact your bank, business partners, or IT support promptly to report any potential spoofing attempts.

By staying informed, maintaining open communication with your bank and business partners, and fostering a vigilant community within your business, you can protect your financial interests and contribute to the overall security of the local business community.

By: Amy Fryman, Friendship State Bank Business Development Specialist

Bio: Local businesses are vital to thriving communities, and The Friendship State Bank is dedicated to supporting them. Amy Fryman, a Business Development Specialist with 33 years of banking experience, works one-on-one with business owners to provide customized financial solutions and connections to key resources. Amy's goal is to help businesses succeed by handling their financial needs, so owners can focus on what they do best.