15 Steps to Protect Your Business from Phishing Scams

STAFF TRAINING

- Educate staff on recognizing phishing attempts (urgency, misspellings, unexpected requests)

EMAIL SECURITY

- Verify sender addresses (watch for slight variations)
- Look for red flags (misspellings, generic greetings)
- Don't click suspicious links (hover to see actual URL)

ACCOUNT PROTECTION

- Enable Multi-Factor Authentication (MFA)
- Update security software regularly (antivirus, anti-malware)
- Use strong, unique passwords (consider a password manager)

NETWORK & DATA

- Avoid public Wi-Fi for sensitive information
- Use secure networks or a VPN for remote access
- Back up critical data regularly

BE CAUTIOUS OF...

- Pop-ups requesting information (avoid entering anything)
- Unexpected emails asking for personal or financial data

REPORTING & AWARENESS

- Report suspicious emails to IT or designated personnel
- Implement email filtering tools (if possible)
- Monitor account activity for unusual behavior
- Stay informed on latest phishing tactics and cybersecurity news

DEVELOP A CYBERSECURITY POLICY

- Create a policy covering email use, data protection, and incident response
- Ensure everyone follows the guidelines