FRAUD PREVENTION CHECKLIST



1.) Identify High-risk Users

Identify your high-risk users such as HR, executives, IT managers, accounts and financial personnel

- Review each for what is posted on social media, company websites and in the public domain, especially job duties/descriptions, hierarchal information, and out of office details
- Identify email addresses that may be searchable in the public domain

2.) Implement Technical Controls

Implement appropriate technical controls for your technology

- Email filtering
- Two-factor authentication
- Complex passwords
- Patching/updating of all IT and security systems
- Manage your network boundaries

- Manage access and permission levels
- Adopt whitelists or blacklists for external traffic
- Register as many as possible company domains that are slightly different than the actual company domain

3.) Develop Critical Policies

Develop critical policies and review with stakeholders

- Develop a wire transfer policy that documents your established processes and corresponds with the products and services we provide. Review it with all parties involved periodically.
- Institute policy concerning access to and release of financial information, IP, customer records and employee records
- Institute a security policy

4.) Develop Response Plan

Develop a comprehensive cyber incident response plan

- Consider comprehensive cyber security insurance that covers data breaches and CEO fraud
- Understand what information you need to protect: identify the corporate "crown jewels"
- Understand how to securely store the information, who has access to it and how to protect it

5.) Perform Regular Training

Perform security training regularly to keep it top of mind

- Train users on the basics of cyber and email security
- Train users on how to identify and deal with phishing attacks with new-school security awareness training
- Frequently phish your users to keep awareness up

🟹 6.) Identify Red Flags

 Watch out for fraudulent or phishing emails bearing the following red flags such as urgency, spoofed email addresses, demands for wire transfers

