Are We Really Safe?

Cybersecurity is not a one-and-done project, it's an ongoing process.

Foundational Practices

- [ ] Regularly update and patch all software, operating systems, and applications
- [ ] Multi-factor authentication (MFA) enabled across critical accounts
- [ ] Strong password policies enforced (not just suggested)
- [ ] Data backups are automated, tested, and stored securely

Human Element

- [ ] Employees receive ongoing security awareness training
- [ ] Phishing simulations or testing are conducted regularly
- [ ] Clear policies exist for handling sensitive data and reporting incidents
- [ ] Access to systems is reviewed and revoked promptly for departing staff

Monitoring & Detection

- [ ] 24/7 monitoring for unusual activity or threats
- [ ] Logs are reviewed (not just collected)
- [ ] Intrusion detection or endpoint detection tools are in place
- [ ] Incident response plan is written, tested, and updated

Risk Management & Compliance

- [ ] Periodic risk assessments are performed (not just once)
- [ ] Compliance requirements are mapped to actual security controls
- [ ] Third-party/vendor risks are evaluated
- [ ] Cyber insurance policy reviewed and aligned with current risks

Continuous Improvement

- [ ] Security controls are tested through vulnerability scans or penetration tests
- [ ] Lessons learned from incidents (internal or industry-wide) are applied
- [ ] Security strategy is reviewed at least annually with leadership involvement