

BUSINESS CYBER SECURITY

Practical steps to eliminate the biggest modern AI & digital risks today

⚠️ **Current AI Related Risks:** AI powered phishing, stolen passwords, ransomware, fake invoices, accidental AI data leaks, and compromised workspace accounts.

HIGHEST PRIORITY ACTIONS

1. Turn On Multi Factor Authentication (MFA)

Enable MFA everywhere: Email, Microsoft 365, Google Workspace, Banking, Accounting software, and Cloud storage. **This stops most account takeovers.**

2. Use a Password Manager

Use tools like **Bitwarden** or **1Password** to automatically generate and store unique, strong passwords for every single account. Avoid reuse.

3. Keep Devices Updated

Turn on automatic updates across Windows, Mac, mobile phones, browsers, and antivirus software. Patches close vulnerabilities before exploitation.

4. Back Up Everything (3-2-1 Rule)

Keep **3 copies** of data across **2 different storage types**, with **1 copy offsite/cloud**. Regularly test restoring files.

5. Train Staff to Verify Requests

Always phone to verify banking changes, invoice updates, or unusual requests. **AI generated emails, voices, and documents look real.**

EMAIL SECURITY BEST PRACTICES

Email remains the primary entry point for cyber attacks. If using Microsoft 365 or Google Workspace:

- Enable robust phishing protection & suspicious login alerts.
- Review system login activity monthly.
- Immediately remove old, unused user accounts.

STRICT AI POLICY RULES

Do not enter company sensitive information into public AI tools:

- Customer personal details & financial records.
- Internal confidential documents or contracts.
- Passwords or proprietary business code/information.

Simple One-Page Team Policy Guidelines:

Allowed 👍

Drafting daily emails
Brainstorming & ideas
Marketing copy text

Not Allowed ❌

Uploading client records
Confidential contracts
Financial data sheets

ESSENTIAL SECURITY STACK

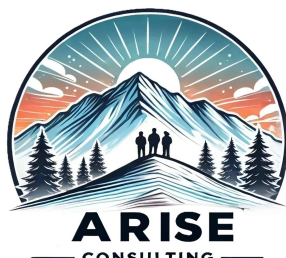
Area	Recommendation
Passwords	Use a central Password Manager
Accounts	Enforce MFA everywhere
Devices	Turn on Automatic Updates
Data	Secure Cloud Backups
Email	M365 / Google advanced security
Staff	Basic phishing awareness training
Antivirus	Microsoft Defender or equivalent



HAVE 10 MINUTES TODAY?

- **Turn on MFA** for every core business account.
- **Check backups** to ensure they are actively running.
- **Remove** unused user or ex-employee accounts.
- **Start** using a dedicated password manager.
- **Tell staff** to verbally verify any banking/payment changes.

These basic, high-impact steps protect businesses against a large percentage of modern automated attacks.



www.Ariseconsultingnz.com

Info@ariseconsultingnz.com