

Cybersecurity

Most attacks on small businesses start with an email or a stolen password. We put protection at each point an attacker can get in, and a plan in place for when one does.

FIVE LAYERS OF PROTECTION



Email

Phishing and malicious attachments filtered before they reach an inbox.



Accounts

Multi-factor sign-in on Microsoft 365 and every business login.



Devices

Detection and response on every computer, with infected machines isolated.



Network

Firewall rules and DNS filtering block known bad sites and traffic.



People

Short training modules and simulated phishing tests through the year.

IF SOMETHING GETS THROUGH

01

Detect

Alerts from devices, email and sign-ins come to our team.

02

Contain

The affected device or account is cut off before it spreads.

03

Recover

Passwords reset, devices cleaned or restored from backup.

04

Report

A plain-language summary of what happened and what changed.

BASELINE FOR EVERY CLIENT

- ✓ Multi-factor sign-in for every user
- ✓ Administrator rights removed from daily accounts
- ✓ Full-disk encryption on laptops
- ✓ Automatic screen lock and updates
- ✓ Former employees' access removed the same day
- ✓ Security settings reviewed at each strategy meeting

CYBER INSURANCE

Controls insurers ask about

Insurers ask about multi-factor sign-in, endpoint protection, backups and training before they quote. These controls are part of our service, and we can answer technical questions as you complete the application.