PACIFIC EDGE TECHNOLOGY

Ransomware Incident Quick Reference

What to do in the first hour after a suspected ransomware event.

Do This Immediately

- [ ] Isolate affected devices from the network (unplug the ethernet cable or disable Wi-Fi). Do not power them off.
- [ ] Contact your IT provider and your cyber insurance carrier right away.
- [ ] Preserve evidence, don't attempt to clean up, delete files, or run removal tools yet.

Do Not

- [ ] Do not reboot or reimage affected machines before your IT provider or a forensics team has examined them.
- [ ] Do not pay a ransom demand without legal and cyber insurance guidance.
- [ ] Do not delay notifying your cyber insurance carrier, delays can affect what's covered.

Five Controls That Stop Most Attacks

- [ ] Unique passwords enforced per account, checked against known breach databases.
- [ ] Phishing-resistant MFA on finance, admin, and executive logins.
- [ ] External email forwarding blocked at the tenant level.
- [ ] Security alerts actively monitored, not just generated and ignored.
- [ ] Staff trained not to overshare role and responsibility details publicly.

Three Questions for Your IT Provider

- [ ] Are we using phishing-resistant MFA (FIDO2 keys, passkeys, or Windows Hello for Business) for finance, admin, and executive logins?
- [ ] Is external email forwarding blocked at the tenant level?
- [ ] Are our security alerts going somewhere, and is someone actually reviewing them?

Ransomware Incident Quick Reference

What to do in the first hour after a suspected ransomware event.

Keep this page somewhere your team can find it fast, printed and posted near IT-relevant workstations, or saved somewhere accessible outside your normal network in case that network is what's affected.