5 Security Steps to Take when Using AI

1. Lock down sign-ins first: turn on the strongest sign-in protections for email and admin accounts, and require trusted devices where possible.

2. Make email harder to fool: reduce “fake-from” emails, filter risky links/attachments, and give staff a one-click way to report suspicious messages.

3. Be ready to contain an incident fast: make sure you can quickly isolate a compromised computer and stop it from spreading.

4. Prove you can recover: test restores (not just backups) and keep at least one backup copy protected with separate access so attackers can’t wipe it out.

5. Set AI rules and practice the “bad day”: publish an approved AI tools policy (what’s allowed and what’s off-limits) and run a quick drill for each client type so everyone knows what to do.

410.877.3625

DTCtoday.com

sales@dtctoday.com

DTC