# SAUTECH | BUSINESS CYBERSECURITY CHECKLIST

Use this checklist to guide a practical security conversation.
Assign an owner and a review date to each action.

[ ] Verify payment and bank-detail changes via a known phone number.
[ ] Use phishing-resistant MFA / passkeys where supported.
[ ] Remove stale accounts and limit administrative access.
[ ] Review cloud app consent, forwarding rules and sign-in alerts.
[ ] Inventory internet-facing services and supported software.
[ ] Prioritise actively exploited flaws; verify patches were applied.
[ ] Maintain offline or immutable backups with separate access.
[ ] Test restoration and record realistic recovery times.
[ ] Check supplier access and rehearse an incident response plan.
[ ] Define safe AI use; keep sensitive data out of unapproved tools.
[ ] Train staff to report suspicious messages without blame.
[ ] Keep offline contact details for your IT and incident teams.

## WARNING SIGNS

Unexpected MFA prompts, changed payment details, urgent secrecy,
new mailbox rules, unfamiliar logins and disabled security tools.

## IF YOU SUSPECT AN INCIDENT

Contact your security/IT team through a trusted channel.
Follow your response plan, preserve evidence and record the timeline.
Avoid uncoordinated wiping or recovery that could destroy evidence.

General guidance, not a security guarantee or legal advice.
Read the full briefing and source links at:
https://www.sautech.net/information/articles-press/

Owner: _____ Review date: _____