Team Security Checklist

presented by SiparSecure

Practical security steps every small business team should follow daily

Access & Passwords

- Use unique, strong passwords for every account.
- Enable multi-factor authentication (MFA) on all business logins.
- Never share passwords over email, text, or chat.
- Store passwords only in approved password managers.

Device Safety

- Keep computers, tablets, and phones updated.
- Install updates within 24–48 hours.
- Only use company-approved apps and software.
- Lock your screen when leaving your desk.

Email & Messaging

- Don't open attachments from unknown senders.
- Hover over links before clicking to see the true destination.
- Treat unexpected password reset emails as suspicious.
- Report strange emails immediately.

Internet Safety

- Avoid using public Wi-Fi for business work.
- If unavoidable, use a VPN.
- Never enter sensitive information on unfamiliar websites.

Data Handling

- Store business files only in approved folders/cloud drives.
- Do not use personal email or USB drives for company data.
- Back up files regularly (or follow your company's backup schedule).
- Delete files you no longer need — clutter increases risk.

Incident Response

- Report unusual activity right away (strange pop-ups, unknown apps, suspicious login alerts).
- Never try to "fix it yourself."
- If you clicked something accidentally, report it immediately — speed matters.