# Before You Post: A Quick Security Check for Public Communications

Use this guide to review posts, bios, and announcements before they go live. Oversharing can aid phishing, impersonation, and insider attacks.

* ☐ Does the post expose staff names, roles, or direct contact info?
* ☐ Are you naming vendors, platforms, or tools that could help an attacker?
* ☐ Are you posting screenshots or photos of equipment, dashboards, or credentials?
* ☐ Could the information be used for a password reset or security question?
* ☐ Does the post reveal staffing changes, vacations, or out-of-office plans?
* ☐ Are you revealing building layouts, security setup, or camera placement?
* ☐ Have you redacted or blurred sensitive content from images or videos?
* ☐ Is it clear what your privacy and data handling practices are (if collecting info)?

When in doubt, keep it minimal. Every detail helps an attacker build a more convincing phishing or social engineering campaign.