



Ensuring data security is critical for today's businesses. Whether your employees are working remotely, using their own devices for work purposes, or handling sensitive information, you need to know that their Gmail and Google Workspaces are secure.

Use this list to ensure you have strong Gmail and Google Workspace security settings in place across your organization. When you follow these best practices, you can feel confident that your employees are communicating and collaborating safely and effectively.

Safeguard your data – and your business.



As a Google Workspace administrator, you should:

- 1 Turn on two-step verification for all users.
- 2 Enforce the use of a verification code app (such as Google Prompt or Google Authenticator).
- 3 Set up team drives.
- 4 Set team drive users' sharing permissions by group or by role.
- 5 Set a custom drive alert when documents are shared outside your domain.
- 6 Restrict calendar sharing outside your domain to busy/available information only.
- 7 Set up SPF and DKIM to validate outgoing messages.
- 8 Enable enhanced pre-delivery scanning of incoming messages.
- 9 Turn on screen locks after 5 minutes or less.
- 10 Enable automatic updates for apps and internet browsers.