Security and Privacy

Best practices for security and privacy including privacy settings, sharing guidelines, account protection, conversation security, and compliance considerations.

- Security And Privacy Best Practices

Security And Privacy Best Practices

This guide covers security features and privacy best practices to help you use Junovy Talk safely and protect sensitive information.

Privacy Settings

Read Receipts

Control whether others can see when you've read their messages:

1. Open App Settings (gear icon)
2. Navigate to the "Privacy" section
3. Toggle "Send read receipts"

When disabled, others won't see read indicators for your messages, but you also won't see read receipts from others.

Typing Indicators

Control whether others see when you're typing:

1. In App Settings > Privacy
2. Toggle "Share typing status"

When disabled, the "typing..." indicator won't appear for your messages.

Sensitive Conversations

For conversations containing confidential information:

1. Open Conversation Settings > Personal
2. Enable "Sensitive conversation"

This will:

- Hide message previews in notifications
  - Hide message previews in the conversation list
  - Protect content from appearing on lock screens

Sharing Best Practices

Before Sharing Files

- Review files before sharing to ensure they don't contain sensitive information
  - Use password-protected documents for highly confidential content
  - Remember that shared files from Junovy Cloud maintain their sharing permissions

Guest Access Considerations

When enabling guest access:

- Share conversation links only with intended recipients
  - Consider using time-limited access for temporary collaborators
  - Remember that guests can see all messages after they join
  - Disable guest access when external collaboration is complete

Screen Sharing Safety

Before sharing your screen:

- Close applications containing sensitive information
  - Consider sharing only a specific window rather than your entire screen
  - Be aware of what's visible on your desktop and notifications
  - Disable notifications temporarily to prevent private messages from appearing

Account Security

Protect Your Account

- Use a strong, unique password for your Junovy account
  - Enable two-factor authentication (2FA) if available
  - Don't share your login credentials with others
  - Log out when using shared or public computers

Recognizing Suspicious Activity

Be cautious of:

- Unexpected password reset emails
  - Messages asking for your login credentials
  - Suspicious links in messages, even from known contacts
  - Requests to share sensitive information via chat

Conversation Security

Moderator Responsibilities

As a conversation moderator:

- Regularly review participant list and remove inactive or unauthorized users
  - Monitor for inappropriate content or behavior
  - Use permission settings to control what participants can do
  - Delete sensitive messages when no longer needed

Private vs. Public Conversations

Choose the right visibility for your conversations:

Private conversations (default):

- Only invited participants can access
  - Not discoverable through search
  - Best for sensitive discussions

Public conversations:

- Discoverable by registered users
  - Anyone in the organization can join
  - Best for general announcements or open discussions

Data Handling

Message Retention

- Messages are stored on Junovy servers
  - Deleted messages may still exist in backups temporarily
  - For highly sensitive information, consider time-sensitive sharing methods

Leaving Conversations

When you leave a conversation:

- You lose access to the conversation history
  - Your previous messages remain visible to other participants
  - You'll need to be re-invited to rejoin

Reporting Issues

If you encounter security concerns or suspicious activity:

1. Do not engage with suspicious messages or links
2. Contact your organization's IT administrator
3. Report the issue to Junovy Support
4. Change your password if you suspect account compromise

Compliance Tips

For organizations with compliance requirements:

- Use the lobby feature for controlled meeting access
  - Enable "Restricted" permissions for webinar-style events
  - Keep conversation membership current and remove former team members
  - Document retention policies for important conversations
  - Use sensitive conversation settings for confidential discussions