You Should Avoid Sending Personal Information via Unsecured Email:

1. **Email is not always secure** – Standard email is transmitted over the internet without encryption, meaning it can be intercepted and read by unauthorized individuals.
2. **Risk of identity theft and fraud** – Sending sensitive information like Social Security numbers, financial details, or passwords over unsecured email could expose you to identity theft or financial loss.
3. **Hacking and phishing risks** – Hackers often target email accounts, and if personal information is shared through unsecured means, it becomes an easier target for exploitation.

What You Can Do:

1. **Use encrypted email services** – Many email providers offer encryption features (e.g., Gmail's Confidential Mode or Outlook’s encryption options) to keep your messages safe.
2. **Share sensitive info through secure platforms** – For sharing personal or financial information, consider using secure messaging apps, file-sharing services with encryption (e.g., Dropbox or Google Drive), or dedicated portals provided by the organization or service you’re communicating with.
3. **Avoid including personal details in the subject line** – Even if your email is not encrypted, try to avoid including sensitive information in the subject line, as it may be exposed in transit or by email preview features.

If you must send sensitive information by email, be sure to use encryption or passphrase protection for attachments and double-check the recipient's email address to ensure it's correct.

Your privacy and security are important, so it's always worth taking extra precautions when communicating sensitive data. Please feel free to reach out if you have any questions or need help setting up a secure communication method.