**What is it?**
Cloud services store information over the Internet on a pay-as-you-go basis, replacing physical hardware such as USB sticks. These services are provided by cloud service providers, who host and manage infrastructure in remote data centres.

**Threats:**
Storing sensitive information, such as client communications, payment details, and personal identifiers on cloud services exposes sex workers to privacy risks.

Sex workers in locations where sex work is criminalised face legal compliance challenges when using cloud services. Providers may be subject to legal pressure to monitor, restrict or report sex work-related activities.

**Resistance:**
You can encrypt your data before uploading it to the cloud to protect it from unauthorised access.
You can review and adjust privacy settings on cloud services to control who has access to your data and how it is shared or displayed.
You can enable two-factor authentication (2FA) on cloud accounts to add an extra layer of security and prevent unauthorised access to accounts.