

2.3 Identity and Cloud Account Safety

Core Concept: Protect Yourself, Protect Your Data

Your identity and your cloud accounts are two of your most valuable digital assets. Your identity can be used to open accounts, file fraudulent tax returns, and ruin your credit. Your cloud accounts, Google, Microsoft, Apple, hold years of emails, photos, documents, and are often the gateway to resetting passwords for everything else.

A compromised identity or cloud account can create a cascading failure across your entire digital life. This section covers how to protect yourself.

2.3.1 Understanding the Risks

What is identity theft?

Identity theft is when someone uses your personal information, social security number, name, date of birth, address, etc, to impersonate you.

Common identity theft scenarios:

- Opening credit cards or loans in your name
- Taking over existing accounts
- Filing fraudulent tax returns to steal refunds
- Creating fake IDs with your information
- Using your insurance for medical care

How identity theft happens:

- Phishing emails and scam calls
- Data breaches (companies losing your information)
- Data brokers selling your information
- Public WiFi snooping
- Lost or stolen wallet
- Mail theft (stealing statements, pre-approved credit offers)

2.3.2 The Basics

- Guard your personal information
- Review third-party app access
- Configure account privacy settings
- Shred sensitive documents

Guard Your Personal Information

Do not ever give out any information to someone who calls you! If you receive a call asking you to confirm your identity by providing personally sensitive information, explain that you do not provide this on a call you did not initiate.

- Ask them for their name, who they represent, the purpose of the call, and a reference number so you can call back (do not accept a number they provide as valid)
- Look up the number of your bank or other service on their official website or contact card (credit card companies have the fraud reporting numbers on the back) and call that number.
- Do not continue to engage with the caller; if it is a legitimate call they will not threaten, coerce, or be upset at you verifying

Before you ever give sensitive, personal information out to anyone, ask these questions:

- "Why do you need this?"
- "Is it required by law?"
- "Can I use an alternative identifier?"
- "How will you protect it?"

Review Third-Party App Access

Apps you've authorized can access your cloud account data. Review and revoke unnecessary access.

How to review:

Google:

- myaccount.google.com > Security > Third-party apps with account access
- Review each app, remove ones you don't use or recognize

Microsoft:

- [account.microsoft.com](https://account.microsoft.com/Privacy) > Privacy > Apps and services
- Remove apps you don't use

Apple:

- appleid.apple.com > Sign-In & Security > Apps Using Apple ID
- Stop using Apple ID for apps you no longer use

Do this quarterly.

Configure Account Privacy Settings

Cloud providers collect extensive data about you. Limit what they collect and share. Do the same for social media accounts, such as facebook, instagram, etc.

Google:

- myaccount.google.com > Data & privacy
- Web & App Activity: Consider turning off or auto-delete after 3 months
- Location History: Turn off unless actively using
- YouTube History: Auto-delete after 3-18 months
- Personalized advertising: Turn off

Microsoft:

- [account.microsoft.com](https://account.microsoft.com/Privacy) > Privacy
- Manage your activity data > Clear activity
- Turn off diagnostic data sharing where possible

Apple:

- Settings > Privacy & Security (on each device)
- Review Location Services, limit to "While Using" for most apps
- Turn off "Share iPhone Analytics"
- Turn off personalized ads

Shred Sensitive Documents

Physical documents can reveal your identity.

Documents to shred:

- Bank statements
- Credit card offers

- Medical records and EOBs
- Tax documents (after 7 years)
- Insurance documents
- Anything with SSN, account numbers, or personal info

Shredder type: Use cross-cut or micro-cut shredder, not strip-cut (too easy to reconstruct).

2.3.3 Better Protection

Opt Out of Pre-Approved Credit Offers

Pre-approved credit offers in the mail can be stolen and used to open accounts.

How to opt out:

- Call 1-888-5-OPT-OUT (1-888-567-8688)
- Or visit optoutprescreen.com
- Choose 5-year opt-out or permanent opt-out

This reduces mail clutter and risk of identity theft

Use Privacy Services for Online Signups

Avoid giving your real email and phone number to every website.

Email masking:

- Firefox Relay <https://relay.firefox.com/>
- Apple Hide My Email (iCloud+ subscribers)
- 10-Minute Mail <https://10minutemail.com/> (temporary mailbox)

Phone masking:

- Google Voice for a free, US phone number
- Use for non-critical signups, not banking or important accounts so you can refresh it periodically to keep spam calls and texts down

Review Cloud Storage Sharing

Make sure you're not unintentionally sharing files or folders.

How to check:

- Google Drive: drive.google.com > Shared with me / Shared (check both)
- OneDrive: onedrive.com > Shared
- Dropbox: dropbox.com > Sharing
- iCloud Drive: icloud.com > iCloud Drive > Shared folders

What to look for:

- Public links you forgot about
- Shares with old colleagues or friends
- "Anyone with link" permissions

2.3.4 Extra Credit

Opt Out of Data Brokers

Data brokers collect and sell your personal information. You can opt out, but it's tedious.

Major data brokers:

- Spokeo, WhitePages, PeopleFinder, BeenVerified
- Each has their own opt-out process
- Search your name to see what's listed
- Follow opt-out instructions for each site

DeleteMe <https://joindeleteme.com> is a paid service that handles opt-outs (~\$130/year)

Revision #2

Created 2026-07-12 21:26:17 UTC by Chris Landis

Updated 2026-07-12 21:47:13 UTC by Chris Landis