
RESOURCE 06 | DON'T CLICK YET COMPANION RESOURCE

Critical Accounts Inventory

Companion resource for Don't Click Yet. Referenced on page 188.

Purpose: Identify the accounts that matter most without writing down passwords.

Storage reminder: If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

This worksheet helps you identify the accounts that would create the most trouble if you lost access, someone else got in, or a trusted person needed to help you during an emergency.

Do not use this worksheet as a place to casually write passwords. Its purpose is to map your important accounts, recovery methods, trusted contacts, and emergency notes. Passwords should be stored in a password manager, secure vault, sealed emergency document, or another safe method appropriate for your situation.

Store this inventory somewhere safe. It may not contain passwords, but it may still reveal sensitive information about your digital life.

How to Use This Inventory

Start with the accounts that protect or connect to other accounts. For most people, that means:

- Main email account
- Mobile phone provider
- Password manager
- Bank and credit card accounts
- Cloud storage
- Apple, Google, or Microsoft account
- Payment apps
- Health portal
- Insurance accounts
- Tax or government accounts
- Important business or freelance accounts

You do not need to list every account you have ever created. Focus on the accounts that would cause real stress, financial risk, identity risk, or recovery problems if something went wrong.

Main Email Account

Your main email account is often the most important account because it receives password reset links, security alerts, bills, family messages, documents, and account recovery notices.

Email provider:

Email address:

Where the password is stored:

MFA method used:

Examples: authenticator app, text message, passkey, security key, device prompt.

Recovery phone number:

Recovery email address:

Backup codes stored where:

Trusted devices signed in:

Notes:

Secondary or Backup Email Account

If you use another email account for recovery, business, family, or older accounts, list it here.

Email provider:

Email address:

Purpose of this account:

Where the password is stored:

MFA method used:

Recovery phone number:

Recovery email address:

Notes:

Mobile Phone Provider

Your phone number may be used for verification codes, calls, account recovery, banking alerts, and family communication. Protect the phone provider account carefully.

Provider name:

Account phone number:

Account owner name:

Where the password is stored:

Account PIN or security code stored where:

Port-out protection, number lock, or transfer protection enabled?

- ☐ Yes
- ☐ No
- ☐ Not sure
- ☐ Not available

MFA method used:

Trusted person who can help with this account:

Provider support number or trusted support route:

Notes:

Password Manager

The password manager may hold the keys to many other accounts. Document how it is protected and how emergency recovery works.

Password manager name:

Account email used:

Where the master password or emergency instructions are stored:

MFA method used:

Backup codes stored where:

Emergency access enabled?

- ☐ Yes
- ☐ No
- ☐ Not sure
- ☐ Not available

Trusted emergency contact:

Recovery method or emergency instructions:

Notes:

Bank Account

List your main bank account first. Add additional banks if needed.

Bank name:

Account type:

Examples: checking, savings, business checking, joint account.

Username or account email:

Where the password is stored:

MFA method used:

Transaction alerts enabled?

☐ Yes

☐ No

☐ Not sure

Trusted phone number or support route:

Debit card stored or used where:

Trusted person who should be contacted in an emergency:

Notes:

Credit Card Account

Card issuer:

Card type or nickname:

Example: household card, travel card, business card.

Username or account email:

Where the password is stored:

MFA method used:

Transaction alerts enabled?

☐ Yes

☐ No

☐ Not sure

Trusted phone number or support route:

Saved in digital wallets or shopping accounts?

☐ Yes

☐ No

☐ Not sure

Notes:

Payment Apps

Use this section for payment services you use to send or receive money.

Payment app name:

Examples: PayPal, Venmo, Zelle, Cash App, Apple Cash, Google Pay.

Account email or phone number:

Where the password is stored:

MFA or security setting used:

Linked bank account or card:

Alerts enabled?

☐ Yes

☐ No

☐ Not sure

Notes:

Additional payment app:

Account email or phone number:

Where the password is stored:

MFA or security setting used:

Linked bank account or card:

Notes:

Apple, Google, or Microsoft Account

These accounts may control email, cloud storage, device backup, app stores, photos, documents, subscriptions, and lost-device tools.

Provider:☐ Apple☐ Google☐ Microsoft☐ Other: _____**Account email:**

Where the password is stored:

MFA method used:

Recovery phone number:

Recovery email address:

Backup codes stored where:

Devices connected to this account:

Lost-device feature enabled?☐ Yes☐ No☐ Not sure**Notes:**

Cloud Storage and Backup

Use this section for services that hold photos, documents, backups, or important files.

Cloud or backup service:

Examples: iCloud, Google Drive, OneDrive, Dropbox, Backblaze, Carbonite, external backup software.

Account email:

Where the password is stored:

MFA method used:

What is stored here:

Examples: photos, documents, tax records, business files, phone backup, computer backup.

Is automatic backup or sync turned on?

☐ Yes

☐ No

☐ Not sure

Last recovery test date:

Backup codes or recovery information stored where:

Notes:

Health Portal

Medical portals may contain appointments, prescriptions, lab results, billing information, insurance information, and messages from providers.

Health system or provider:

Portal name:

Username or account email:

Where the password is stored:

MFA method used:

Recovery email or phone:

Trusted person authorized to help, if applicable:

Notes:

Insurance Accounts

Use this section for health, home, auto, life, business, or other insurance accounts.

Insurance provider:

Type of insurance:

Username or account email:

Where the password is stored:

MFA method used:

Policy documents stored where:

Trusted phone number or support route:

Notes:

Tax or Government Accounts

Use this section for tax accounts, Social Security, unemployment, benefits, immigration, professional licensing, or other government services.

Agency or service:

Account purpose:

Username or account email:

Where the password is stored:

MFA method used:

Recovery email or phone:

Important documents stored where:

Notes:

Business, Freelance, or Client Accounts

Use this section if you are self-employed, freelance, run a small business, manage client information, or rely on online platforms for income.

Account or platform name:

Examples: business email, website host, domain registrar, accounting software, invoicing platform, client portal, cloud storage, professional marketplace.

Business purpose:

Username or account email:

Where the password is stored:

MFA method used:

Client or financial data stored here?

☐ Yes

☐ No

☐ Not sure

Backup or export method:

Trusted person or professional who can help:

Notes:

Social Media and Messaging Accounts

These accounts may be used to impersonate you, contact family, or spread scams if compromised.

Account or platform:

Username or account email:

Where the password is stored:

MFA enabled?

☐ Yes

☐ No

☐ Not sure

Recovery email or phone:

Who should be contacted if this account is compromised:

Notes:

Home Technology Accounts

Use this section for accounts connected to your router, smart cameras, doorbells, thermostats, smart speakers, printers, security systems, or internet provider.

Service or device account:

Purpose:

Username or account email:

Where the password is stored:

MFA enabled?☐ Yes☐ No☐ Not sure☐ Not available**Device location:**

Trusted support route:

Notes:

Emergency Digital Contacts

List people who can help you in a digital emergency. Choose people who are calm, trustworthy, and reachable.

Primary trusted contact:Name:

Phone:

Email:

Role or relationship:

What this person can help with:

Secondary trusted contact:Name:

Phone:

Email:

Role or relationship:

What this person can help with:

Professional support contact, if applicable:

Name or company: _____

Phone: _____

Email or website: _____

What they can help with: _____
_____**Emergency Access Notes**

Use this section to explain where trusted people can find emergency instructions. Do not expose passwords unless this worksheet is stored in a secure location and you have intentionally chosen to include them.

Where my password manager emergency instructions are stored:

Where important documents are stored:

Where backup codes are stored:

Where my family verification phrase worksheet is stored:

Where backup drives or important physical records are stored:

Attorney, executor, or legal contact, if applicable:

Other emergency notes:

Review Log

Review this inventory at least once a year and after major life changes, such as a new phone, new email address, changed bank, changed phone number, new business, move, marriage, divorce, illness, or death in the family.

Review date: _____
Reviewed by: _____
Changes made: _____

Review date: _____
Reviewed by: _____
Changes made: _____

Review date: _____
Reviewed by: _____
Changes made: _____

Final Reminder

This inventory is not about giving up privacy. It is about avoiding confusion during emergencies.

The right people should know how to help when help is truly needed.

The wrong people should not be given easy access.

Store this worksheet accordingly.