

J. SANDERSON

HOME CYBER SAFETY

# Your Home Cyber Safety Plan

MAC + APPLE

A calm, practical 90-minute consultation for everyday digital life

Guided setup · Recovery planning · A written action summary



# How the session works

Support without handing over control

## 01 You stay in the driver's seat

You make every change and keep passwords, codes and private files to yourself.

## 02 We focus on the accounts that matter most

Email, banking, the main device account, phone service and cloud storage come first.

## 03 We finish with a plan you can actually use

You leave with clear priorities, recovery contacts and a short written action summary.

## 04 Urgent loss follows a different path

Active theft, fraud or identity misuse may need the bank, telco, police, ReportCyber or IDCARE.

# Your digital home map

A five-minute view of what needs protecting

## 01 People and devices

Who uses which computer, tablet and phone? Which devices are shared?

## 02 Main accounts

Primary email, device account, banking, telco, social media and cloud storage.

## 01 Important information

Photos, documents, tax records, family contacts and anything difficult to replace.

## 02 Current recovery routes

Backup email, trusted phone number, recovery contact, recovery code and provider support.

### WORKSHOP

**Write down the five accounts and three devices that would cause the most stress if access disappeared tonight.**

# The accounts that unlock everything

Protection starts with the accounts that can reset the others

## 01 Primary email

A compromised inbox can reset many other accounts and hide warning messages.

## 02 Main device account

Your Microsoft, Apple or Google account may control devices, backups, purchases and recovery.

## 03 Banking and phone service

Money and mobile numbers need strong sign-in protection and known support contacts.

## 04 Password manager

If you use one, protect its master login and recovery method especially carefully.



# Password health check

A small number of changes removes a large amount of avoidable risk

## 01 Find reused passwords

Start with email, banking, social media, shopping and any account holding identity documents.

## 02 Replace weak or exposed logins

Use a unique generated password, or a long unique passphrase where a manager is not available.

## 03 Avoid predictable variations

Changing one number or season still creates an easy pattern across accounts.

## 04 Never approve a login you did not start

An unexpected authentication prompt can be an attack in progress.

### WORKSHOP

**Choose the first three accounts to fix. Do not try to change every password during this session.**

# Passwords across the Apple household

Use the Passwords app consistently and keep recovery outside one device

## 01 Review the Passwords app

Use it to store unique logins, review security recommendations and share only through supported groups.

## 02 Protect the Apple Account

Its password, trusted devices and MFA protect synced passwords and other iCloud data.

## 03 Move unsafe notes gradually

Test each saved login before deleting passwords from paper notes, documents or browser lists.

## 04 Keep a recovery route outside the Mac

A trusted phone number or recovery contact should still work if the Mac is unavailable.

### WORKSHOP

**Save one priority login, sign out, sign back in and confirm where the household's recovery route lives.**

# Apple Account MFA and recovery

Trusted devices help, but one missing phone must not become a lockout

## 01 Confirm two-factor authentication

System Settings → your name → Sign-In & Security → Two-Factor Authentication.

## 02 Add a second trusted phone number

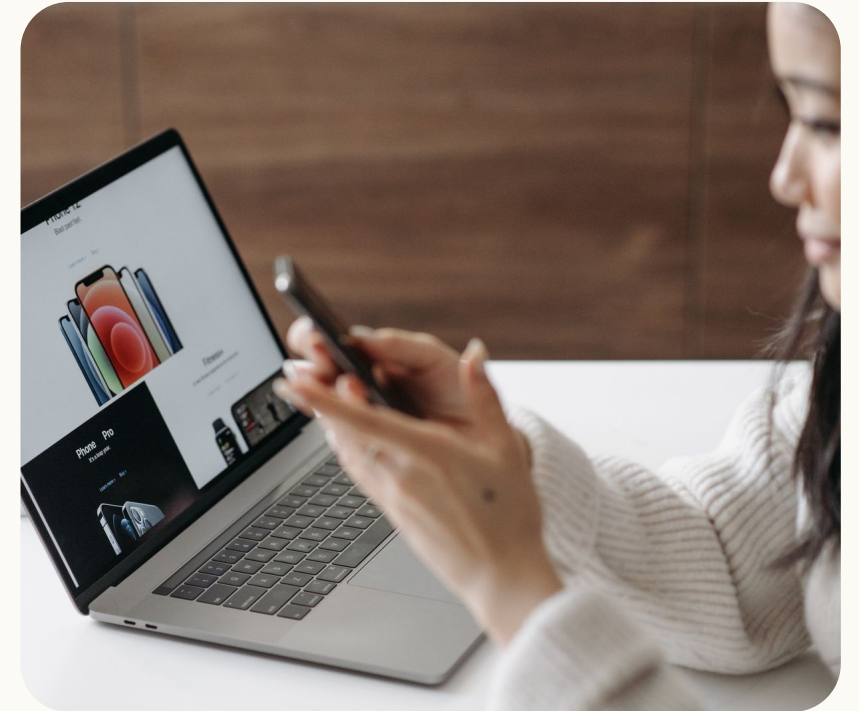
Use a number the household can reach if the main iPhone is lost.

## 03 Set a recovery contact

Choose someone trusted who can provide a recovery code without gaining access to the account.

## 04 Treat a recovery key as an advanced option

A recovery key can strengthen control, but losing it can permanently block account recovery.



### WORKSHOP

**Confirm 2FA, a reachable backup number and a suitable recovery contact. Do not display any code.**

# Mac sign-in and screen lock

A secure Apple Account still needs a locked Mac

## 01 Use a strong Mac login password

The local Mac password and Apple Account password may be different. Know which one a prompt requests.

## 02 Set up Touch ID where available

System Settings → Touch ID & Password. Keep the login password memorable and private.

## 03 Require a password after sleep

System Settings → Lock Screen. Use Control + Command + Q when walking away.

## 04 Separate household users

Give each person an account and keep routine use away from a shared administrator login.

# macOS updates and built-in protection

A supported, updated Mac carries most of the security workload

## 01 Open Software Update

System Settings → General → Software Update. Install compatible macOS and security updates.

## 02 Turn on automatic updates

Allow security responses, system data files and app updates where available.

## 03 Keep Gatekeeper protections intact

Prefer the App Store or the developer's official site and avoid bypassing security warnings.

## 04 Remove old access

Review login items, browser extensions, sharing settings and remote-access apps no longer used.

### DECISION

**If the Mac cannot run a supported macOS version, record an upgrade or replacement decision.**

# FileVault and the recovery route

Encryption protects a lost Mac, provided the owner can still unlock it

## 01 Check FileVault

System Settings → Privacy & Security → FileVault.

## 02 Understand the chosen recovery method

The Mac may use the Apple Account or a recovery key, depending on setup and macOS version.

## 03 Keep an offline recovery copy

If a recovery key exists, store it away from the Mac and do not place the only copy in iCloud Drive.

## 04 Test the surrounding account recovery

Confirm the Apple Account's trusted numbers and recovery contact are current.

# Email and browser continuity

Protect the inbox, then plan how important information survives

## 01 Check recovery details

Confirm the email provider has a current backup address and phone number.

## 02 Review forwarding and rules

Unknown forwarding or Mail rules can hide warnings and copies of sensitive messages.

## 03 Keep Safari warnings on

Leave fraudulent-website warnings enabled and treat certificate warnings as a reason to stop.

## 04 Archive what matters

Time Machine or iCloud sync may not create an independent copy of all cloud email. Export critical records where appropriate.

### WORKSHOP

**Review the primary inbox's forwarding, connected apps and recovery details without opening private messages.**

# A backup plan for the Apple home

iCloud makes data available; Time Machine creates a recoverable history

## 01 Confirm iCloud sync

Check which items sync, including Photos, iCloud Drive, Contacts and Passwords, and verify available storage.

## 02 Set up Time Machine

Use a suitable external drive or supported network destination for automatic Mac backups.

## 03 Include iPhone and iPad

Confirm iCloud Backup or an encrypted computer backup for mobile devices.

## 04 Plan for email and irreplaceable records

Add a provider-specific export or archive when the household needs a separate copy.



### WORKSHOP

**Open Time Machine settings and confirm the destination and date of the latest successful backup.**

# The restore test

A backup becomes trustworthy when one file comes back successfully

## 01 Choose a harmless test file

Use a copy of a small document, never the only copy of an important file.

## 02 Enter Time Machine

Locate an earlier version and restore the test file to a safe location.

## 03 Open and verify it

Check that the restored file opens and contains the expected information.

## 04 Record the result

Write down the backup source, test date and next review date in the recovery plan.

### WORKSHOP

**Complete one safe restore test now, or schedule it within seven days if the first backup is still running.**

# Lost iPhone, iPad or Mac plan

Find My works best when the household rehearses before anything is missing

## 01 Turn on Find My

Confirm Find My Mac and Find My on each mobile device, including the Find My network where offered.

## 02 Enable Stolen Device Protection

On supported iPhones, it adds protection for sensitive changes away from familiar locations.

## 03 Know the genuine lost-device route

Use the Find My app or [icloud.com/find](https://icloud.com/find) to locate, mark as lost or erase when appropriate.

## 04 Keep access outside the missing phone

A trusted number, recovery contact and offline codes prevent one missing device becoming a full lockout.



### REHEARSAL

From another device, open the official Find My route and confirm the household can see its devices.

# If an Apple Account or Mac is compromised

Secure the trusted account and phone number before making wider changes

## 01 Move to a trusted device

If the Mac behaves strangely, use another known-safe device for password and banking changes.

## 02 Change the Apple Account password

Use a trusted device, then review [account.apple.com](https://account.apple.com) for unfamiliar personal or security information.

## 03 Review the device list

Remove devices you do not recognise and confirm every trusted phone number belongs to the household.

## 04 Protect email, telco and money

Confirm no SMS forwarding exists, secure the primary inbox and contact the bank promptly for active loss.

# Scams, deepfakes and AI accounts

A simple pause-and-verify habit works across new and old scams

## 01 Pause when a message creates urgency

Money, secrecy, fear and sudden account warnings are reasons to slow down.

## 02 Verify through a separate channel

Call a known number or open the organisation's official app instead of using the supplied link.

## 03 Treat voice and video as evidence, not proof

AI can imitate familiar people. Agree on a family verification question for urgent requests.

## 04 Protect AI accounts like email

Use a unique password and MFA, especially when the account connects to files or other services.



# Your household recovery plan

Keep the plan useful without putting secrets in it

## 01 Who to contact

Bank, telco, email provider, insurer, trusted person, IDCARE and ReportCyber.

## 02 Where recovery information lives

Record the location of codes and documents, never the secrets themselves on this page.

## 01 First actions

Secure email and phone service, preserve evidence, review money movement and trusted devices.

## 02 How the household communicates

Agree on an alternative number and a family verification phrase for urgent requests.

### TAKEAWAY

**Print one copy for a safe place and give a second copy to the trusted person named in the plan.**

# Your next 30 days

Three priorities are enough to create momentum

## 01 Within 24 hours

Complete any urgent account, recovery or device update identified today.

## 02 Within 7 days

Finish MFA and recovery details for priority accounts, then confirm the first successful backup.

## 03 Within 30 days

Run a restore test, rehearse the lost-phone plan and review the household recovery sheet.

## 04 After the session

Use the written action summary to track what is complete, pending or needs specialist help.

# Home Wi-Fi and connected devices

Secure the router and the devices that share your home network.

Start with the router and Wi-Fi settings your household can manage. If a setting is hard to find or the router is supplied by your internet provider, check its official instructions or contact the provider.

## Router access

- Replace the default administrator login with a unique password; change the username too if the router allows it.
- Install router firmware updates and check that the model still receives security support.
- If support has ended, ask your provider what replacement options are suitable.

## Wi-Fi network

- Use a network name that does not reveal your name, address or family details.
- Choose a long, unique Wi-Fi password and the strongest encryption supported by your router and devices.
- Use guest Wi-Fi for visitors where available.

## Connected devices

- Update smart TVs, speakers, cameras and other connected devices; remove old devices you no longer use.
- Turn off device features you do not need, such as remote access, where the settings allow it.
- If practical, place smart-home devices on a separate network from phones and computers.

### Keep the household priorities in order

Handle immediate money loss, account takeover or recovery problems first. Add home network work when there is a real gap, such as an unsupported router, default access details or an unsafe setup for connected devices.

Sources: Cyber Safety Project, Cyber Security at Home Guide · Australian Cyber Security Centre, Secure your Wi-Fi and router