

J. SANDERSON

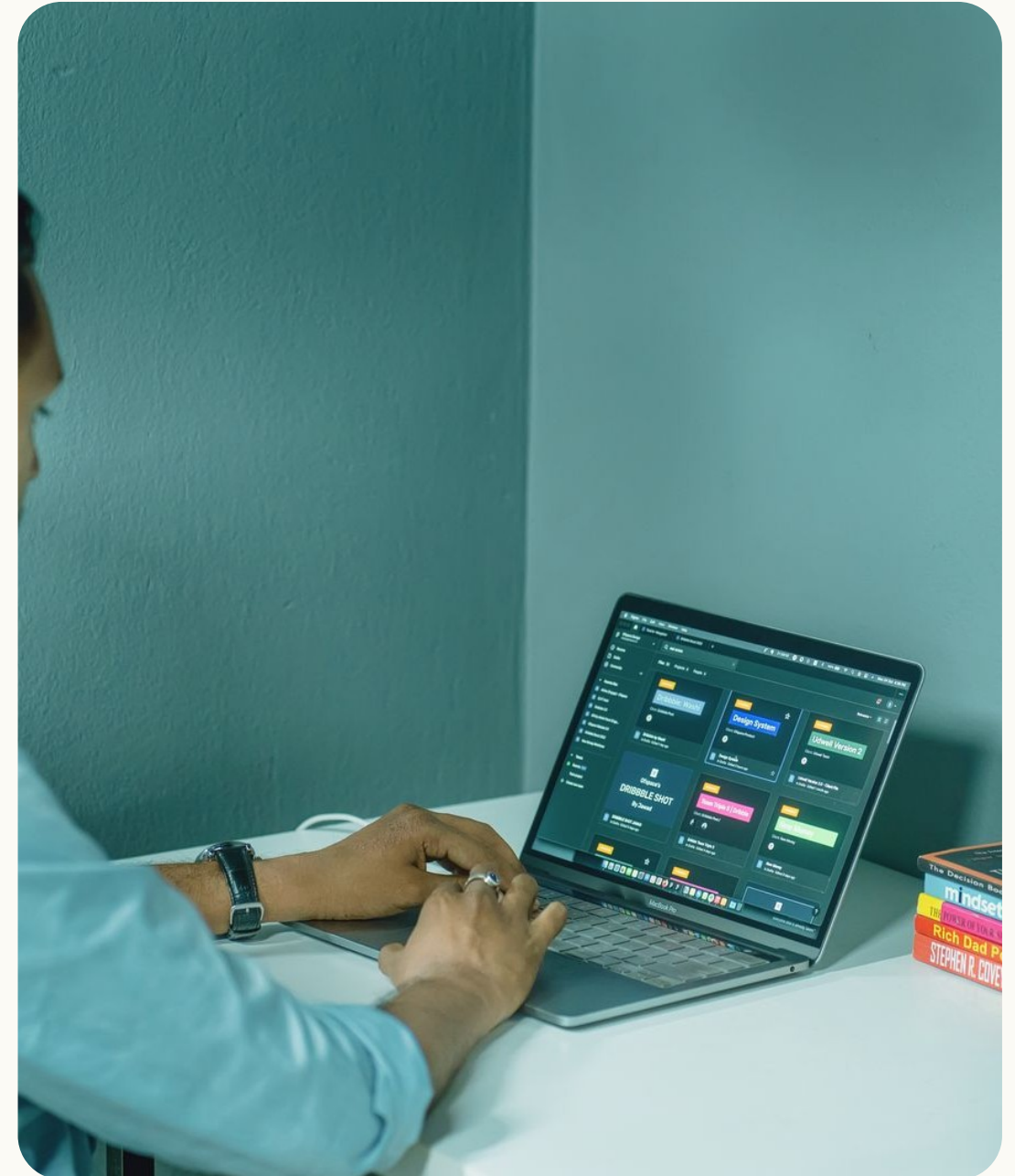
HOME CYBER SAFETY

Your Home Cyber Safety Plan

WINDOWS + MICROSOFT

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.

One password manager, used consistently

The best choice is the one the household can use and recover

01 Choose the household approach

Microsoft Edge can store passwords, or use one reputable independent manager across devices.

02 Protect the main login

Use a unique master password or account password, MFA and a recovery method kept offline.

03 Import slowly and remove duplicates

Start with priority accounts, check each login works, then retire unsafe notes or spreadsheets.

04 Know the recovery route

Test that the backup email or phone number is current before you depend on it.

WORKSHOP

Save one priority login, sign out, sign back in and confirm the household knows how recovery works.

MFA and Microsoft account recovery

Strong sign-in protection still needs a safe route back in

01 Turn on MFA for priority accounts

Prefer an authenticator app or passkey where offered. Keep SMS as a fallback only when needed.

02 Review Microsoft security information

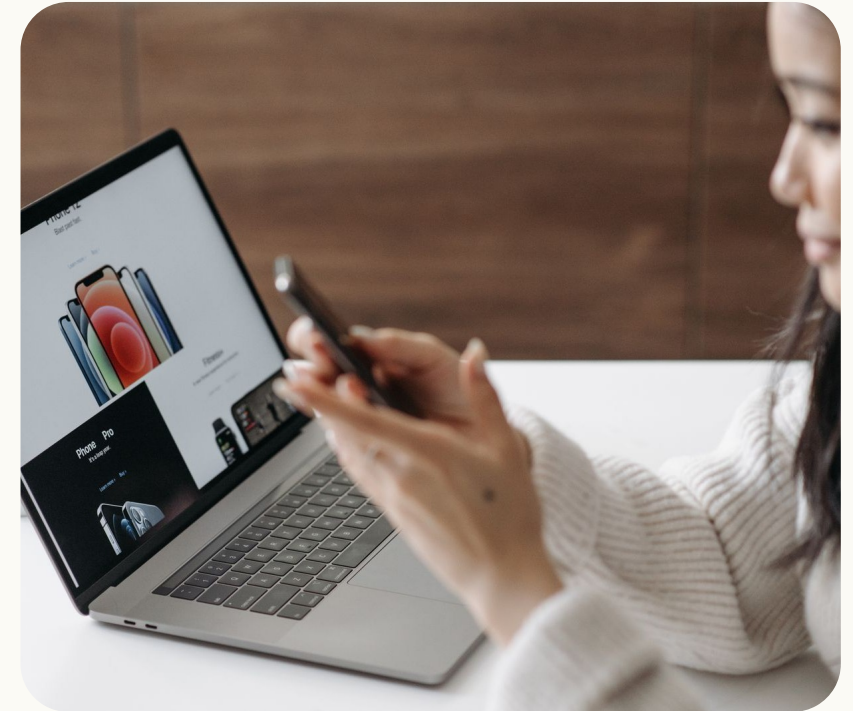
Check the backup email, trusted phone number and sign-in methods in the Security dashboard.

03 Create a Microsoft recovery code

Store the 25-digit code offline, away from the computer and away from the password manager login.

04 Keep two ways to recover

One lost phone should not lock the household out of its most important accounts.



WORKSHOP

Complete MFA on the primary email and confirm a second recovery route without sharing any code.

Windows sign-in and screen lock

A strong account still needs a locked front door

01 Use Windows Hello

Settings → Accounts → Sign-in options. Set a PIN and add face or fingerprint recognition if supported.

02 Require sign-in after absence

Set the screen to lock when the computer sleeps and use Windows + L when walking away.

03 Separate household users

Give each person their own account and keep children or guests out of the administrator account.

04 Know the difference

The Windows Hello PIN belongs to this device. The Microsoft account password protects the online account.

Updates and built-in protection

Windows 11 should update automatically and Windows Security should stay on

01 Check the Windows version

Settings → System → About. Most Windows 10 home users no longer receive free security updates.

02 Run Windows Update

Settings → Windows Update → Check for updates. Restart and repeat until important updates finish.

03 Open Windows Security

Review Virus & threat protection, Firewall & network protection and App & browser control.

04 Remove unused software

Old remote-access tools, browser extensions and abandoned apps create unnecessary exposure.

DECISION

If the PC is on Windows 10, record an upgrade, ESU or replacement decision in the action summary.

Device encryption and the recovery key

Encryption protects a lost computer, but the recovery key protects the owner

01 Check Device encryption or BitLocker

Settings → Privacy & security → Device encryption, or search for Manage BitLocker on supported editions.

02 Confirm the recovery key exists

From another device, sign in to the Microsoft account and check the listed BitLocker recovery keys.

03 Keep an offline copy

Store a printed or securely saved copy away from the encrypted computer.

04 Match the correct device

Record the device name or key ID so the household can identify the right key in a stressful moment.

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, inbox rules or automatic replies can hide signs of account takeover.

03 Keep browser protection on

Use Microsoft Defender SmartScreen or the equivalent protection in the chosen browser.

04 Archive what matters

Device backup does not always create a separate copy of cloud email. Export or save 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 Windows home

Use one convenient copy and one independent copy

01 Windows Backup and OneDrive

Use Windows Backup for supported settings and OneDrive folder backup for selected files.

02 Independent file backup

Use File History with an external drive or another trusted backup service for a separate copy.

03 Photos and phone data

Confirm the phone's photo and device backup is active under its own Apple or Google account.

04 Email and irreplaceable records

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



WORKSHOP

Choose one folder containing irreplaceable files and confirm exactly where its independent copy lives.

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 Restore from OneDrive or File History

Recover a previous version or restore the test file to a different location.

03 Open and verify it

Check that the 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 phone and device plan

Prepare while every device is still in your hands

01 Turn on device finding

Enable Apple Find My or Google's device-finding service on the phone. On Windows, enable Find my device where supported.

02 Write down the telco route

Know how to suspend the SIM and replace the number from another device.

03 Protect money and identity

Know which bank cards, authenticator apps and identity documents are accessible from the phone.

04 Keep access outside the phone

Store recovery codes and trusted contact details somewhere the missing phone cannot take with it.



REHEARSAL

From another device, locate the official device-finding page and confirm the household knows how to reach it.

If an account or PC is compromised

Secure the recovery channels first, then work outward

01 Move to a trusted device

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

02 Secure the primary email

Change the password, confirm MFA, review recent activity and remove unknown recovery methods.

03 Remove hidden access

Review forwarding, connected apps and inbox rules, then use Microsoft's sign-out-everywhere option if needed.

04 Escalate active loss

Call the bank and telco promptly. Preserve messages, dates and transaction details for reports.

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