PLANNING

Map your important accounts

Start with the accounts that could affect money, identity, or communication.

DIGITAL SECURITY CHECKUP

CREATE A PRIVATE INVENTORY

List primary email, financial, phone, cloud storage, government, and social accounts without writing passwords in the list. Mark the email address that controls password resets.

- ☐ Record service name, login email, and recovery method
- ☐ Mark accounts with payment or sensitive files
- ☐ Store the inventory in a protected location

EXAMPLE

Example: Priya marks her main email as the reset hub and lists her bank, phone carrier, and photo storage as high priority.

PUT IT INTO PRACTICE

Which account can reset the others?

Which account would cause the most harm if lost?

General defensive security education only. Use official support channels for your services and seek qualified help if you suspect fraud, account compromise, or identity theft.

PLANNING

Use unique strong passwords

A password manager can make uniqueness practical.

DIGITAL SECURITY CHECKUP

REPLACE REUSED CREDENTIALS

Give every important account a long, unique password generated and stored by a reputable password manager. Change exposed or reused passwords first; never share passwords through messages.

- [ ] Start with email, finance, and phone accounts
- [ ] Use a memorable manager passphrase that is not reused
- [ ] Save recovery codes securely, separate from routine notes

EXAMPLE

Example: A reused email password is replaced first; the password manager creates distinct passwords for each remaining priority account.

PUT IT INTO PRACTICE

Where have I reused a password?

How will I securely access recovery codes?

PLANNING

Turn on stronger sign-in

Add a second check where services offer it.

DIGITAL SECURITY CHECKUP

ENABLE MULTI-FACTOR AUTHENTICATION

Use an authenticator app, security key, or another service-supported method for priority accounts. Review the official setup screen and keep backup methods current.

- [ ] Prefer phishing-resistant options when available
- [ ] Do not approve unexpected sign-in prompts
- [ ] Remove old phone numbers and unused devices

EXAMPLE

Example: Jordan enables an authenticator app for email and saves the service·s backup codes in a locked record.

PUT IT INTO PRACTICE

Which priority account lacks multi-factor authentication?

What old device or number should be removed?

PLANNING

Update devices and apps

Updates repair known problems and improve reliability.

DIGITAL SECURITY CHECKUP

SET A MAINTENANCE ROUTINE

Check that operating systems, browsers, apps, routers, and security tools receive updates from official sources. Restart when updates require it and retire devices that no longer receive security support.

- [ ] Enable automatic updates where appropriate
- [ ] Install apps only from trusted stores or vendors
- [ ] Back up important files before major changes

EXAMPLE

Example: Once a month, Ana updates her laptop, phone, browser, and home router through their official settings.

PUT IT INTO PRACTICE

Which device has pending updates?

Is any device no longer supported?

PLANNING

Review access and privacy

Remove access you no longer need.

DIGITAL SECURITY CHECKUP

CHECK CONNECTED SERVICES

Review active sessions, connected apps, sharing links, browser extensions, and account permissions. Revoke unfamiliar or unused access through the service·s official account settings.

- ☐ Sign out of devices you no longer control
- ☐ Limit shared links to the needed people and time
- ☐ Remove extensions you do not recognize or use

EXAMPLE

Example: A forgotten tablet appears in an email account·s sessions list, so Morgan signs it out and reviews recent activity.

PUT IT INTO PRACTICE

Which connection no longer has a purpose?

Who can currently access my shared files?

PLANNING

Recognize suspicious requests

Pause before entering information or approving a request.

DIGITAL SECURITY CHECKUP

VERIFY INDEPENDENTLY

Unexpected urgency, payment demands, login links, and requests for codes can be signs of fraud. Open a known official app or type the official address yourself instead of using a message link.

- [ ] Do not share verification codes with anyone
- [ ] Verify callers using a number you find independently
- [ ] Report suspected phishing through the service·s official channel

EXAMPLE

Example: A delivery text asks for a card update; Luis opens the retailer·s official app and finds no delivery issue.

PUT IT INTO PRACTICE

What independent route can I use to verify this request?

What information should never be sent in reply?

PLANNING

Prepare recovery steps

Recovery is easier when your information is current and protected.

DIGITAL SECURITY CHECKUP

DOCUMENT A RESPONSE PLAN

Keep backup codes, account recovery contacts, device serial information, and support links in a secure place. If you suspect compromise, use a clean device when possible and contact services through official channels.

- [ ] Record the date, account, and suspicious activity
- [ ] Change credentials starting with primary email
- [ ] Tell financial providers promptly about suspected unauthorized activity

EXAMPLE

Example: After an unexpected login alert, Noor records the time, changes her email password, checks sessions, and contacts her bank through its app.

PUT IT INTO PRACTICE

Where is my secure recovery record?

Who do I contact first if my main email is compromised?