



A PRACTICAL UK FAMILY GUIDE | 2026

# Cyber-Safe at Home

Simple habits, family conversations and emergency steps to protect your money, accounts, devices and children online.

---

UNITED KINGDOM

CYBER  SAFE

Safer accounts. Calmer decisions. Stronger families.

[www.cybersafe-uk.com](http://www.cybersafe-uk.com) | [help@cybersafe-uk.com](mailto:help@cybersafe-uk.com)

KEEP THIS PAGE

# If something has happened, act in this order

Feeling embarrassed or panicked is normal. Speed matters more than blame. Stop further loss, regain control, preserve evidence and ask for help.

|   |          |                                                                                                                                                          |
|---|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | STOP     | End the call or chat. Do not click again, send more money or follow instructions to move funds.                                                          |
| 2 | BANK     | If money or bank details are involved, call your bank using the number on your card or a known official channel. You can use 159 to reach many UK banks. |
| 3 | ACCOUNTS | Use a clean device. Recover the affected account, change any reused passwords, sign out other sessions and turn on 2-step verification.                  |
| 4 | EVIDENCE | Keep messages, usernames, numbers, payment details, dates and screenshots. Do not negotiate with the criminal.                                           |
| 5 | REPORT   | England, Wales or Northern Ireland: Report Fraud online or 0300 123 2040. Scotland: Police Scotland on 101. Call 999 if there is immediate danger.       |

|                                                                     |                                               |                                                                                        |
|---------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------|
| <b>SUSPICIOUS EMAIL</b><br>Forward it to<br>report@phishing.gov.uk. | <b>SUSPICIOUS TEXT</b><br>Forward it to 7726. | <b>SUSPICIOUS WEBSITE</b><br>Report it through the NCSC<br>suspicious website service. |
|---------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------|

THE MOST IMPORTANT RULE

No one is in trouble for telling the family quickly.

START HERE

# The six habits that protect a household

Cybersecurity at home is not a technical project. It is a set of family habits that make unusual requests easier to recognise and incidents easier to contain.

|    |                      |                                                                                   |
|----|----------------------|-----------------------------------------------------------------------------------|
| 01 | Protect email first  | Email resets other accounts. Give it your strongest sign-in protection.           |
| 02 | Use passkeys or 2SV  | A stolen password should not be enough to enter an important account.             |
| 03 | Update automatically | Phones, computers, apps, routers and smart devices need security updates.         |
| 04 | Pause and verify     | Urgency, secrecy and unusual payment requests are reasons to stop.                |
| 05 | Back up what matters | Keep irreplaceable photos and documents in more than one safe place.              |
| 06 | Talk without blame   | Children and adults report mistakes faster when they expect help, not punishment. |

FAMILY PROMISE

If a message makes us frightened, excited or rushed, we pause and check it another way.

## ACCOUNTS

# Passkeys, passwords and 2-step verification

Your email, banking and main phone account deserve the strongest protection because they can unlock much of your digital life.

**DO THIS NOW**

Turn on a passkey or 2-step verification for every adult's email account. Then protect banking, social media and cloud photo accounts.

**WHY IT WORKS**

Passkeys resist many phishing attacks. 2-step verification provides an important second barrier when a password is stolen.

## What your family should know

- Choose passkeys where they are offered. The NCSC says passkeys are at least as secure as strong-password 2SV. [1]
- Where passkeys are unavailable, use a trusted password manager to create a different password for every account.
- If you prefer memorable passwords, use three random words and never reuse the result on another account.
- Do not change a good unique password on a fixed timetable. Change it when it may be compromised, shared or reused.
- Store recovery codes safely and review recovery phone numbers and email addresses.

**OUR FAMILY RULE**

**One account, one unique sign-in. A stolen password must not unlock the rest of the family.**

## SCAMS

# Pause, leave the conversation, verify independently

A convincing logo, caller ID, message history or familiar voice is not proof. Criminals can spoof, copy and impersonate trusted people and organisations.

**DO THIS NOW**

Practise this sentence aloud: 'I do not make decisions during unexpected calls. I will contact the organisation myself.'

**WHY IT WORKS**

Report Fraud advises contacting organisations through a trusted number or by typing the official website yourself. [2]

## What your family should know

- Do not use a link, phone number or contact detail supplied by the person asking you to act.
- Open the official app, type the known website yourself or call the number on the back of your card.
- Never share a one-time code, password, PIN, passkey approval or screen with an unexpected caller.
- Treat secrecy, urgency, threats, investment promises and requests to move money as warning signs.
- Caller ID and email addresses can be spoofed. Familiar details may have come from social media or a data breach.

**OUR FAMILY RULE**

**We never transfer money, share a code or install an app because an unexpected caller tells us to.**

## AI IMPERSONATION

# A familiar face or voice may still be fake

AI can make impersonation faster and more believable, but the safest response remains simple: leave the conversation and verify through a separate trusted route.

**DO THIS NOW**

Choose a private family verification phrase. Store it offline or in a secure family password manager - never in a public social post.

**WHY IT WORKS**

Criminals exploit urgency and emotion. A pre-agreed verification method interrupts that pressure.

## What your family should know

- If a relative appears to call in distress, hang up and call their known number yourself.
- Ask a question whose answer is not available on social media. A safe phrase is stronger than a birthday or pet name.
- Do not rely on video alone. Deepfake video, copied profile images and compromised accounts can support the same deception.
- Agree who can authorise urgent family payments and what second check is always required.
- Never keep an emergency secret from another trusted adult merely because the caller demands it.

**OUR FAMILY RULE**

**A voice creates concern, not proof. We verify through a second channel before acting.**

## MONEY

# Banking, shopping and marketplace safety

Payment protection helps, but it is not a substitute for checking who you are paying and why the payment method has been requested.

**DO THIS NOW**

Turn on instant transaction alerts. Review saved cards and remove payment details from accounts the family no longer uses.

**WHY IT WORKS**

NCSC shopping guidance recommends protecting important accounts and using trusted payment routes. [3]

## What your family should know

- Use the retailer's official app or type the web address yourself rather than following an advert or message link.
- Be suspicious when a seller moves a conversation off-platform or insists on bank transfer, gift cards or cryptocurrency.
- For unexpected bank contact, end the call and use a verified bank number. Never disclose a PIN or one-time code.
- Check delivery, refund and subscription terms before paying. Very low prices can be bait for data or payment theft.
- If money has gone, contact the bank immediately and then report the fraud. Keep payment references and messages.

**OUR FAMILY RULE**

**We do not change payment method or bank details without verifying the request another way.**

## EMAIL AND SOCIAL MEDIA

# Protect the accounts that represent you

A hijacked email or social account can be used to reset passwords, impersonate you, deceive friends and search years of private messages.

**DO THIS NOW**

Open your main email security page. Review active sessions, recovery details, forwarding rules and connected applications.

**WHY IT WORKS**

The NCSC recommends using the provider's official recovery process and changing reused passwords after compromise.

## What your family should know

- Use a passkey or 2-step verification, especially for email and social media.
- Remove unknown sessions, app permissions, mail forwarding and recovery details.
- If an account is hacked, use the provider's official recovery process. Change any other account using the same password. [4]
- Tell contacts if the compromised account sent messages or payment requests in your name.
- Keep account recovery details current before a phone is lost or an old number is reassigned.

**OUR FAMILY RULE**

Email is the master key. We protect it before less important accounts.

## CHILDREN

# Safety starts with conversation, not surveillance

Children need a safe route to disclose upsetting content, grooming, bullying, coercion or a mistake. Technology settings help, but trust is the control that brings problems into the open.

**DO THIS NOW**

Ask your child to show you how they block, mute and report on the two services they use most. Let them teach you.

**WHY IT WORKS**

Ofcom advises regular conversations, real ages, reporting tools and parental controls. [5]

## What your family should know

- Register children with their real age so services can apply age-appropriate protections.
- Use device, app, game and router parental controls as support – not as a substitute for conversation.
- Agree that a child can come to a trusted adult without losing all device access merely for asking for help.
- Teach children never to share intimate images, location, school details, passwords or verification codes.
- Save evidence of bullying, threats or grooming, block the account and report through the platform or police as appropriate.

**OUR FAMILY RULE**

You will not be blamed for telling us. We will solve it together.

## TEENAGERS AND GAMING

# Protect identity, money and friendships

Games and social platforms blend entertainment, identity, money and relationships. The risk often arrives through another player rather than through the game itself.

**DO THIS NOW**

Review one gaming account together: privacy, voice chat, friend requests, purchases, linked accounts and 2-step verification.

**WHY IT WORKS**

Ofcom requires services to make blocking, muting, reporting and other child-safety controls more accessible. [5]

## What your family should know

- Treat free currency, skins, cheats, account upgrades and prize links as likely bait.
- Do not trade accounts or share sign-ins. A stolen gaming account can expose payment and identity information.
- Limit who can send messages, voice chat or invitations. Block and report abusive or coercive users.
- Use purchase PINs and spending notifications. Discuss loot boxes and recurring subscriptions openly.
- Never move to a private messaging app because a stranger asks, and never meet an online contact alone.

**OUR FAMILY RULE**

Someone who asks for secrecy, images, money or a move to private chat is not acting like a safe friend.

## DEVICES AND BACKUPS

# Update, lock, locate and back up

A secure account cannot protect an unlocked phone or an unsupported laptop. Device settings should reduce both cyber risk and the damage from loss or theft.

**DO THIS NOW**

Switch on automatic operating-system and app updates. Confirm that every phone has a screen lock and a working find-my-device feature.

**WHY IT WORKS**

Updates close known weaknesses; tested backups reduce the harm from loss, failure, malware and ransomware.

## What your family should know

- Use a strong device PIN and biometric unlock where appropriate. Avoid simple patterns and birthdays.
- Turn on device encryption, automatic updates and remote locate or erase features.
- Back up irreplaceable photos and documents. Test that at least one important file can be restored.
- Remove unused apps and do not install software from unexpected links or unofficial stores.
- Before selling or giving away a device, sign out, remove it from the family account and perform a factory reset.

**OUR FAMILY RULE**

If losing this device would lose the memory, document or account, we create a second safe copy.

## HOME NETWORK

# Make the router boring and dependable

The home router connects family devices to the internet. It should be updated, protected by its own admin password and replaced when the provider no longer supports it.

**DO THIS NOW**

Open the router or broadband provider's official app. Check firmware updates, admin password, wifi encryption and the list of connected devices.

**WHY IT WORKS**

Secure configuration, updates and support status matter more than changing settings for their own sake.

## What your family should know

- Change a default or reused router administration password. Keep the wifi password separate from the admin password.
- Use WPA2 or WPA3 security. Disable obsolete options and remote administration unless genuinely required.
- Install firmware updates or allow the broadband provider to manage them automatically.
- Create a guest network for visitors and, where useful, for less trusted smart devices.
- Replace an unsupported router. Keep recovery details and provider contact information somewhere accessible.

**OUR FAMILY RULE**

Only expected devices belong on our home network.

## SMART HOME

# Cameras, speakers, doorbells and connected toys

A smart device may contain a microphone, camera, location history or household routine. Buy it as though it will become part of the family's private space.

**DO THIS NOW**

List every internet-connected camera, doorbell, speaker, television, toy and appliance. Remove devices nobody recognises or uses.

**WHY IT WORKS**

The NCSC advises checking support dates, changing defaults, enabling 2SV and applying updates. [6]

## What your family should know

- Check the manufacturer's security-support end date before buying and before continuing to use an older device.
- Create a unique password, enable 2-step verification and install updates automatically where available.
- Switch off remote access, microphones, cameras, location or cloud recording when they are not needed.
- Review who can access household feeds and remove old users, installers or shared accounts.
- Factory-reset a device before resale, disposal or transfer to another household.

**OUR FAMILY RULE**

**If a smart device no longer receives security updates, it does not stay silently connected forever.**

## PRIVACY AND DATA BREACHES

# Share less, recover faster

Personal details can help criminals impersonate relatives, answer security questions or make a scam feel authentic. A breach does not guarantee fraud, but it changes what the family should watch.

**DO THIS NOW**

Search each adult's main email inbox for recent data-breach notices. Confirm that affected passwords are unique and 2-step verification is enabled.

**WHY IT WORKS**

Report Fraud advises limiting oversharing and monitoring bank and credit records for unusual activity. [7]

## What your family should know

- Avoid public posts showing full birth dates, addresses, travel plans, school uniforms, tickets or identity documents.
- Review privacy settings and old public posts. Remember that friends' accounts may also be compromised.
- After a breach, change exposed or reused passwords, monitor accounts and be alert to more convincing follow-on scams.
- Check bank and credit records for unfamiliar activity and act quickly on unexpected bills or account letters.
- Shred sensitive paper records and secure household documents as carefully as digital files.

**OUR FAMILY RULE**

Information shared for fun today may become a security answer or impersonation detail tomorrow.

## SUPPORTING RELATIVES

# Help without taking away independence

People of every age are targeted. A trusted support arrangement should make verification easier without giving one person unnecessary control over another person's money or identity.

**DO THIS NOW**

Agree a named person each relative can call before acting on an unexpected financial or technical request.

**WHY IT WORKS**

Report Fraud provides reporting and victim-support routes; relatives should also contact their bank immediately after financial loss. [2]

## What your family should know

- Write verified bank, broadband and device-support numbers on a card kept near the phone.
- Create a calm rule: no financial decision is made during an incoming call.
- Turn on transaction alerts and account protections with the account holder's knowledge and consent.
- Discuss courier fraud: banks and police do not send a courier to collect a card or ask for the PIN.
- If someone is victimised, focus on limiting harm. Shame and secrecy make repeat targeting easier.

**OUR FAMILY RULE**

**We will never be angry because you checked with us before sending money.**

RECOVERY

# Four incident cards for the fridge or family folder

Do not improvise under pressure. Use the card closest to what happened, then move to the emergency sequence at the front of this guide.

|                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>HACKED ACCOUNT</b></p> <p>Use the provider's official recovery page. Change reused passwords. Sign out other sessions. Remove unknown recovery details and forwarding rules. Tell contacts if you were impersonated.</p>               | <p><b>LOST OR STOLEN PHONE</b></p> <p>Use find-my-device. Lock or erase if necessary. Contact the mobile provider. Remove payment cards. Secure email and banking. Watch for messages pretending the phone was found.</p>                              |
| <p><b>MALWARE OR FAKE SUPPORT</b></p> <p>Disconnect if an attacker has remote control. End the call. Remove remote-access software. Use a clean device to protect accounts. Follow official device recovery guidance or trusted support.</p> | <p><b>MONEY SENT TO A SCAMMER</b></p> <p>Call the bank immediately through a verified route. Ask it to stop or recover the payment. Preserve messages and references. Report the fraud. Do not pay a recovery agent who contacts you unexpectedly.</p> |

RECOVERY WARNING

Anyone who unexpectedly offers to recover lost money for a fee may be targeting you again.

FAMILY EXERCISE

# The 30-minute Cyber-Safe home check

Set a timer. Do the checks together. Stop when the timer ends and book another short session rather than turning security into an exhausting annual event.

| CHECK | FAMILY ACTION                                                    |
|-------|------------------------------------------------------------------|
| [ ]   | Email protected with a passkey or 2-step verification.           |
| [ ]   | Unique passwords or a trusted password manager in use.           |
| [ ]   | Recovery details and backup codes checked.                       |
| [ ]   | Automatic updates enabled on phones and computers.               |
| [ ]   | Important photos and documents backed up and one restore tested. |
| [ ]   | Router and smart-device support dates reviewed.                  |
| [ ]   | Children can demonstrate block, mute and report controls.        |
| [ ]   | Family verification phrase and payment-check rule agreed.        |
| [ ]   | Bank alerts enabled and official reporting numbers stored.       |
| [ ]   | One person knows where the emergency page is kept.               |

SUCCESS IS NOT PERFECTION

Complete the highest-impact action today and schedule the next one.

UNITED KINGDOM CYBER-SAFE

# How [www.cybersafe-uk.com](https://www.cybersafe-uk.com) can help families

The website can become a trusted home-cyber hub: short guidance, printable family plans and calm incident steps written for ordinary households rather than technical specialists.

|          |                                                                                                                |
|----------|----------------------------------------------------------------------------------------------------------------|
| LEARN    | Plain-English briefings on scams, passkeys, devices, gaming, smart homes and privacy.                          |
| PREPARE  | Downloadable family rules, emergency cards, checklists and age-appropriate conversation guides.                |
| PRACTISE | Short family tabletop scenarios: fake bank call, hacked social account, lost phone and AI voice impersonation. |
| RESPOND  | A clear first-hour route showing who to contact, what to preserve and how to regain control.                   |
| SUPPORT  | Guidance for parents, teenagers, carers and relatives who may need help without blame or loss of independence. |

OUR PURPOSE

Make home cybersecurity feel practical, human and possible.

Visit [www.cybersafe-uk.com](https://www.cybersafe-uk.com)  
Contact [help@cybersafe-uk.com](mailto:help@cybersafe-uk.com)

## TRUSTED HELP

# Official sources and reporting routes

This guide is general awareness material. Follow the instructions of your bank, account provider, device manufacturer, police or emergency services for your circumstances.

[1] NCSC - Passkeys: what you need to know

<https://www.ncsc.gov.uk/passkeys>

[2] Report Fraud - reporting fraud, cyber crime and suspicious activity

<https://www.reportfraud.police.uk/reporting-a-fraud/>

[3] NCSC - Shopping and paying safely online

<https://www.ncsc.gov.uk/guidance/shopping-online-securely>

[4] NCSC - Recovering a hacked account

<https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account>

[5] Ofcom - guidance for parents and children's online safety

<https://www.ofcom.org.uk/parents>

[6] NCSC - Smart devices: using them safely in your home

<https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home>

[7] Report Fraud - Individual cyber protection

<https://www.reportfraud.police.uk/individual-protection/>

[8] NCSC - Cyber security advice for you and your family

<https://www.ncsc.gov.uk/section/advice-guidance/you-your-family>

## Key UK contacts

Report Fraud: [reportfraud.police.uk](https://reportfraud.police.uk) or 0300 123 2040 (England, Wales and Northern Ireland).

Scotland: Police Scotland on 101 for fraud and cyber crime.

Immediate danger: 999.

Suspicious email: [report@phishing.gov.uk](mailto:report@phishing.gov.uk).

Suspicious text: forward to 7726.

Banking scam: contact your bank through a verified route; 159 connects to many UK banks.

Childline: 0800 1111.

## Publication note

Published September 2026 by United Kingdom Cyber-Safe. Information and reporting routes were checked on 2 September 2026. Services and guidance can change; verify current details through the linked official sources.

Copyright 2026 United Kingdom Cyber-Safe. This guide may be shared in its complete, unaltered form with attribution. It is not legal, financial, medical or emergency advice.