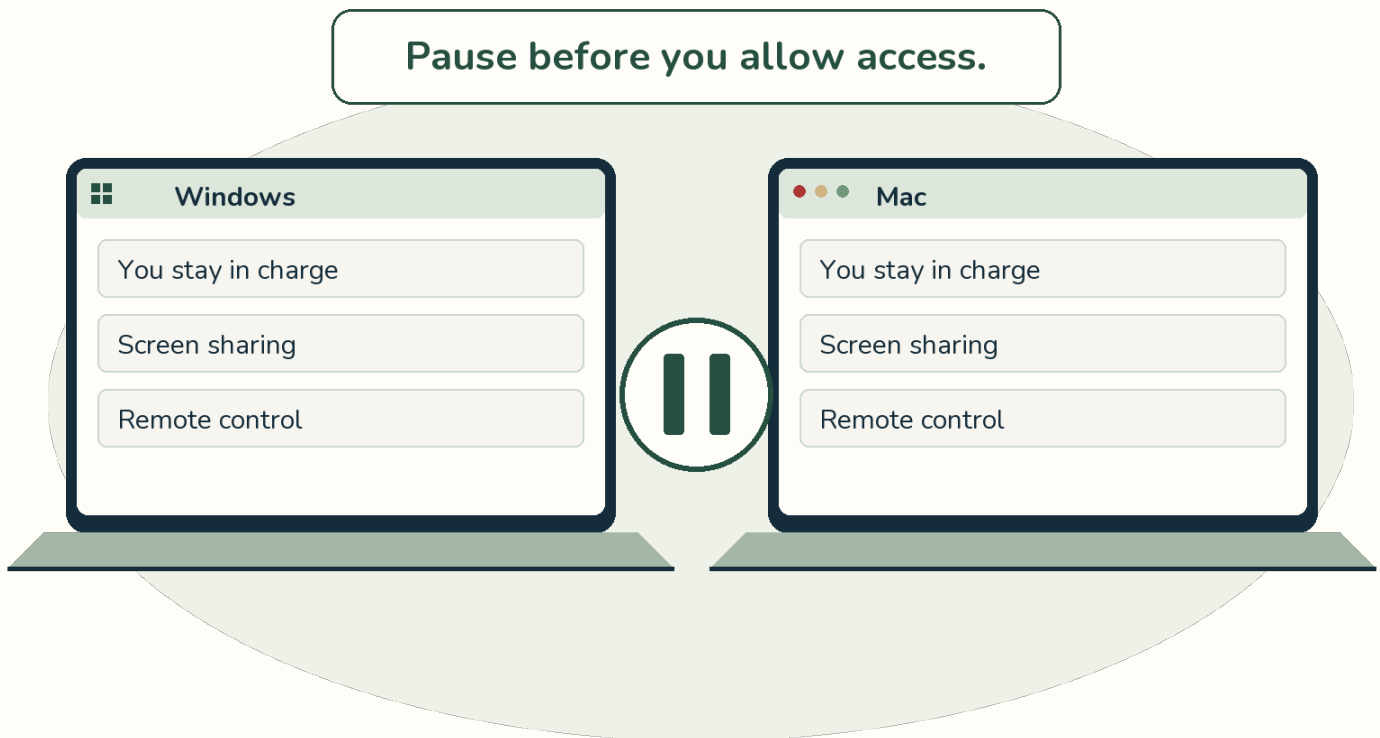




Before You Let Someone Connect to Your Computer

Windows & Mac • Pause. Verify. Stay in control.



Remote help can let someone see your screen or control your computer.
You choose whether to allow it.

Before connecting: pages 2–3

Ending the session: page 4

Suspicious access already happened? Start on page 5.

Print at Actual Size / 100%. You can pause and ask for help.



Before you allow a connection

Unexpected contact? Do not grant access. Confirm with a helper you know.

1 Check your appointment.

Step 1 of 18

Ask: “Did I arrange this visit?”

If not, do not allow access.

Next: Step 2.

2 Call your trusted helper.

Step 2 of 18

Use a number you already know.

Do not use a pop-up’s number.

Next: Step 3.

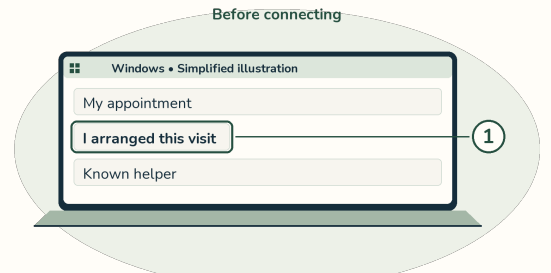
3 Ask about the access.

Step 3 of 18

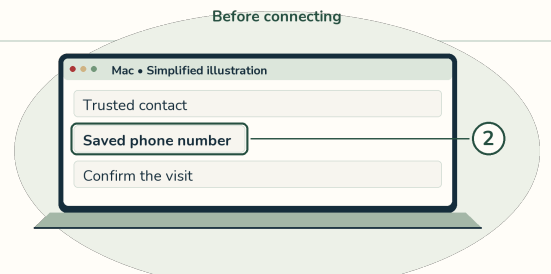
Ask what they will see or control.

Wait until you understand.

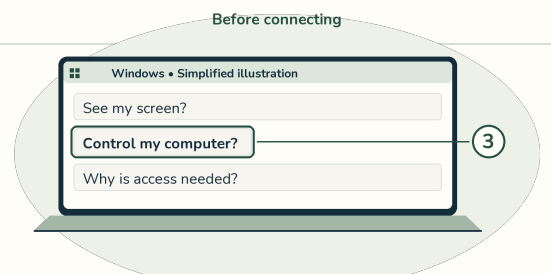
Next: Prepare to share.



I arranged this visit



Saved phone number



Control my computer?



Prepare for an arranged session

A verified helper's connection code is different from your account sign-in code.

4 Close private windows.

Step 4 of 18

Close banking, email and private documents before sharing.

Next: Step 5.

5 Keep your secrets private.

Step 5 of 18

Do not read out passwords or account sign-in codes.

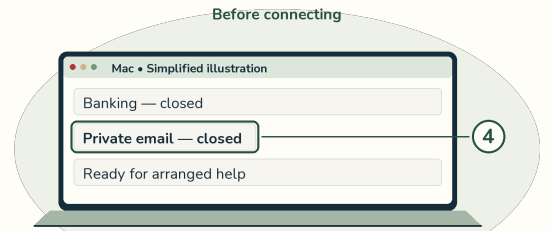
Next: Step 6.

6 Stay at the computer.

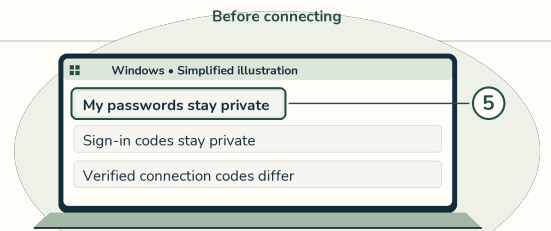
Step 6 of 18

Watch the session as it happens.
Stop if anything feels wrong.

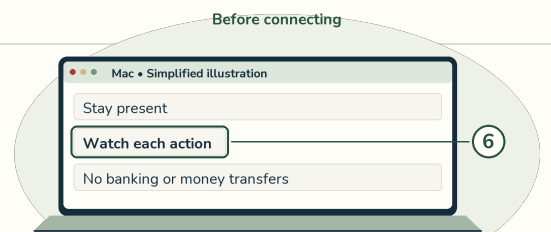
Next: Learn how to stop.



Private email — closed



My passwords stay private



Watch each action



End the session yourself

Quick Assist: Cancel control does not end sharing. Other apps may use Disconnect.

7 Windows: choose Leave.

Step 7 of 18

In Quick Assist, click Leave when the session is finished.

Mac users: Steps 8–9.

8 Mac: open sharing menu.

Step 8 of 18

For FaceTime, click the screen-sharing button in the menu bar.

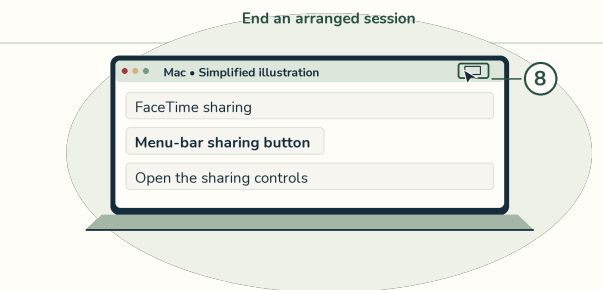
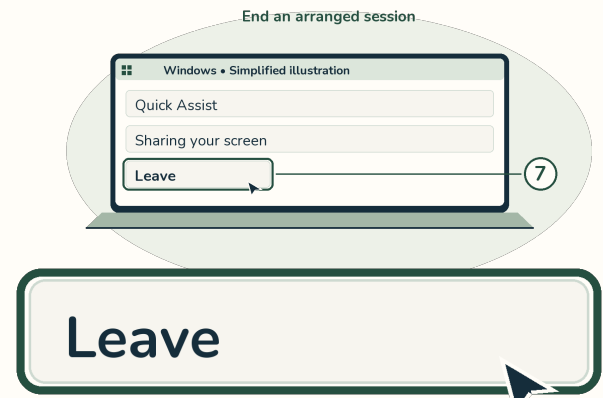
Next: Step 9.

9 Mac: click Stop Sharing.

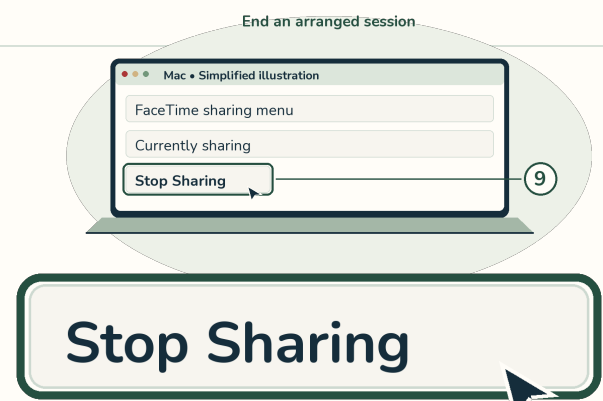
Step 9 of 18

Choose Stop Sharing in the menu.
Check that sharing has ended.

Check: Sharing has ended.



Screen-sharing menu





Suspicious access? Act now.

Cannot stop it? Shut down. Hanging up the phone alone does not end access.

10 Disconnect the internet.

Step 10 of 18

Turn off Wi-Fi and unplug any network cable on this computer.

Next: Step 11.

11 Call someone you trust.

Step 11 of 18

Use another trusted phone or computer to ask for help.

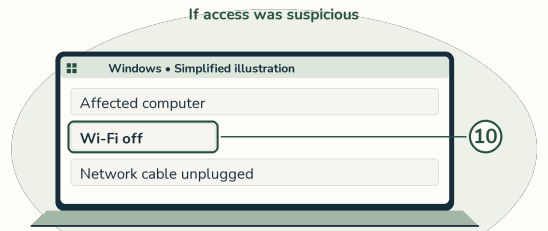
Next: Step 12.

12 Contact your bank now.

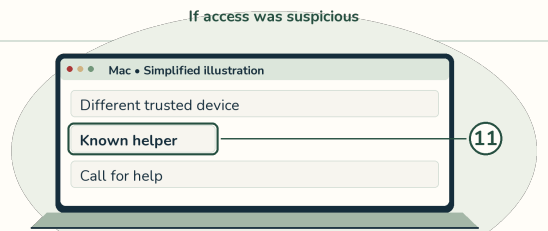
Step 12 of 18

If money or bank details were exposed, call its official number.

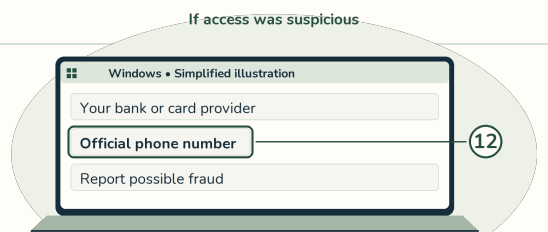
Next: Protect accounts.



Wi-Fi off



Known helper



Official phone number



Protect accounts and the computer

A trusted helper can reconnect for updates and review sign-ins and recovery details.

13 Change exposed passwords.

Step 13 of 18

Use another trusted device.
Start with your email account.

Next: Step 14.

14 Turn on two-factor sign-in.

Step 14 of 18

Use an extra sign-in check
where your accounts offer it.

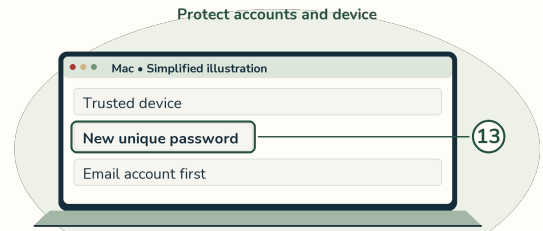
Next: Step 15.

15 Have the computer checked.

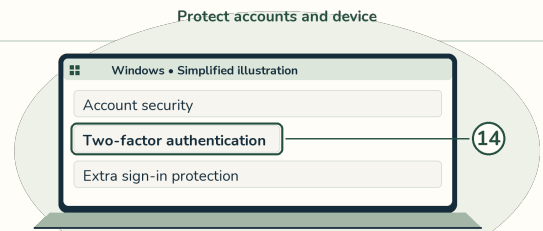
Step 15 of 18

Ask a trusted helper to review
security and remote-access apps.

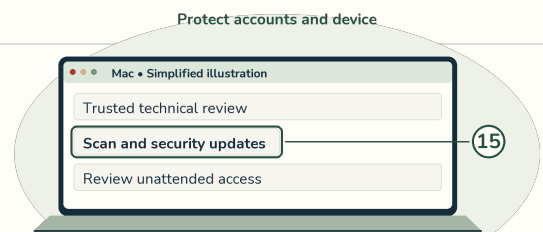
Next: Keep records.



New unique password



Two-factor authentication



Scan and security updates



Record, report and return safely

Do not pay a stranger who promises to recover your money. Keep using trusted contacts.

16 Keep a record.

Step 16 of 18

Write down dates, caller and app.
Save messages and receipts.

Next: Step 17.

17 Report the scam.

Step 17 of 18

On a trusted device, visit
ReportFraud.ftc.gov.

Next: Step 18.

18 Wait for a trusted review.

Step 18 of 18

Use the affected computer for
sensitive accounts only after review.

You can ask for help.

Record, report and return safely

Windows • Simplified Illustration

What happened?

Date • caller • app

Payments and messages

Date • caller • app

Record, report and return safely

Mac • Simplified Illustration

Report a scam

ReportFraud.ftc.gov

For identity misuse: IdentityTheft.gov

ReportFraud.ftc.gov

Record, report and return safely

Windows • Simplified Illustration

Before normal use

Trusted review completed

Sensitive accounts can wait

Trusted review completed



Keep this quick reminder

Before connecting

Expect the visit. Confirm the helper. Understand the access.

When finished

End the session and check the sharing indicator is gone. Review any unattended access with your trusted helper.

If access was suspicious

Disconnect the computer. Use another trusted device for help, banking calls and account protection.

Official references

Microsoft: Quick Assist

Apple: FaceTime screen sharing on Mac

FTC: Tech support scams

FTC: What to do if you were scammed

FTC: Disconnect an affected computer

Reviewed October 27, 2026 • Quick Assist and FaceTime examples.
For other apps, ask your trusted helper to show you how to end access.