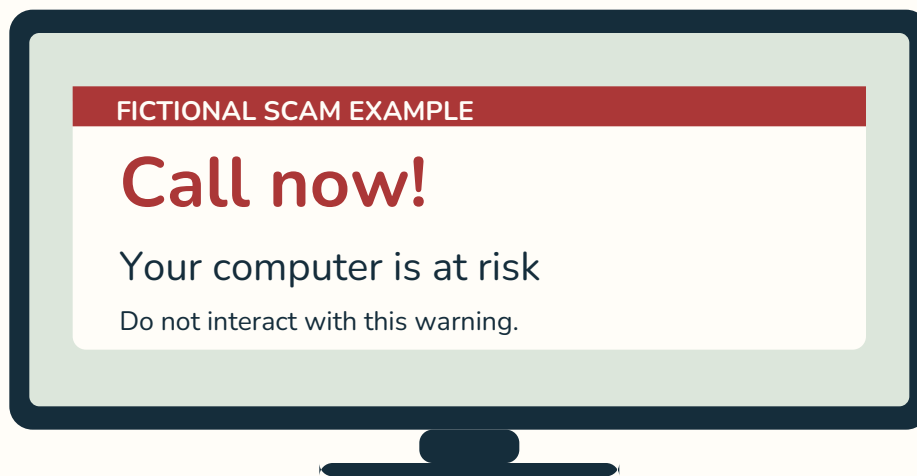




Close a Suspicious Pop-up Windows & Mac

A calm guide to closing a browser warning
and choosing your next step safely.



Pause. Do not call its number.

Choose your route

Everyone: page 2. Windows: pages 3–5.

Mac with Safari: pages 6–7. Already responded: page 8.

Closing may lose unsaved browser work. If a stranger already has access,
or you shared money or passwords, use the recovery page promptly.



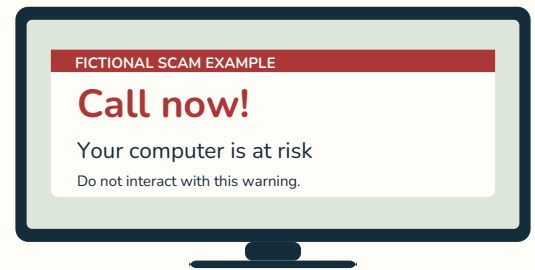
Before you close it

All computers • Start with these three safety checks

Step 1 of 3

1 Leave the message alone.

Do not click its buttons,
links, or download offers.

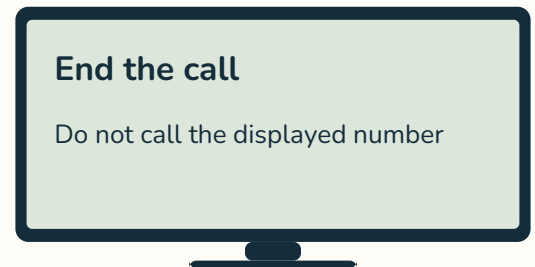


Pause. Do not call its number.

Step 2 of 3

2 Leave its number alone.

Do not call the number shown.
End a pressure-filled call.

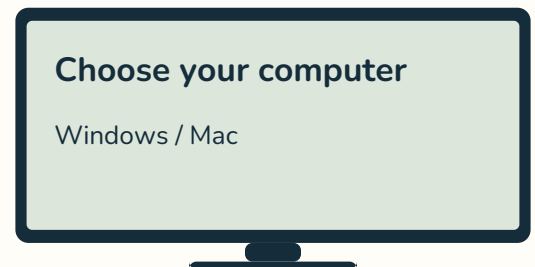


Do not use the warning's number.

Step 3 of 3

3 Choose your computer.

Windows: continue on page 3.
Mac with Safari: go to page 6.



One calm step at a time.

Already paid or allowed access? Go to page 8.



Windows | Try this first

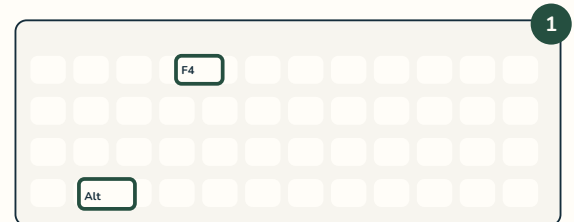
Keep the browser with the warning as the front window.

1 Close the browser window.

Hold **Alt**, press **F4**,
then release both keys.

Some laptops also require the Fn key.

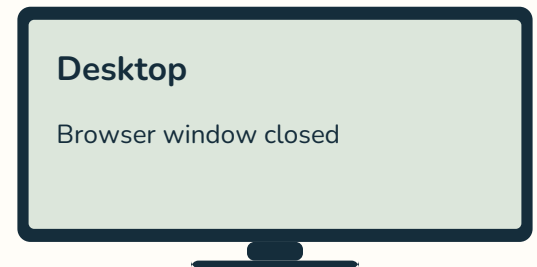
Step 1 of 3



Step 2 of 3

2 Check the result.

If the warning disappeared,
continue on page 5.



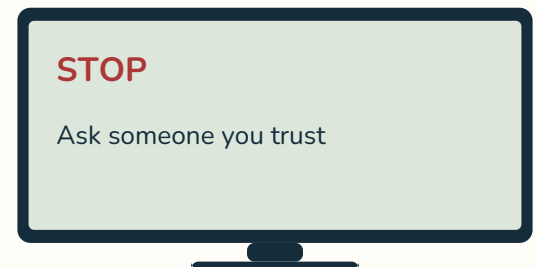
One calm step at a time.

3 Stop if it stays open.

Use page 4 only if the
browser will not close.

Do not click a fake Close button inside the warning.

Step 3 of 3



One calm step at a time.



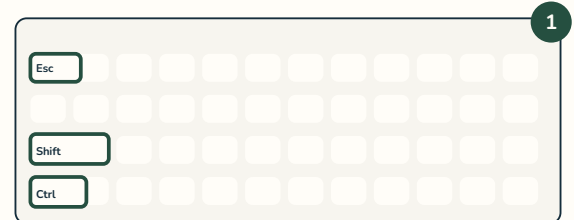
Windows | If it is stuck

Optional • Skip this page if the warning already closed.

Step 1 of 3

1 Open Task Manager.

Hold **Ctrl** and **Shift**,
then press **Esc**.



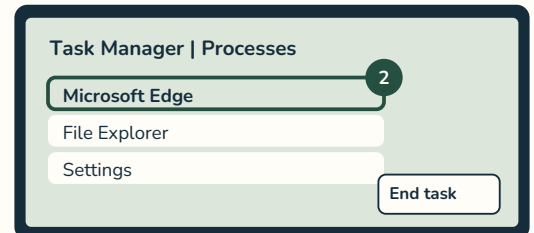
1
Ctrl + Shift + Esc

Step 2 of 3

2 Select your browser.

In Processes or Apps, choose
the browser you were using.

If needed, choose Processes. Do not pick system tasks.



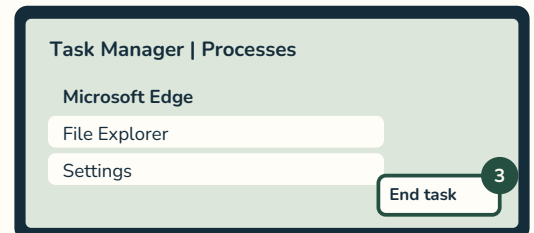
2
Microsoft Edge

Step 3 of 3

3 Click End task.

This closes that browser.
Then continue on page 5.

If it still will not close, stop and get trusted help.



3
End task



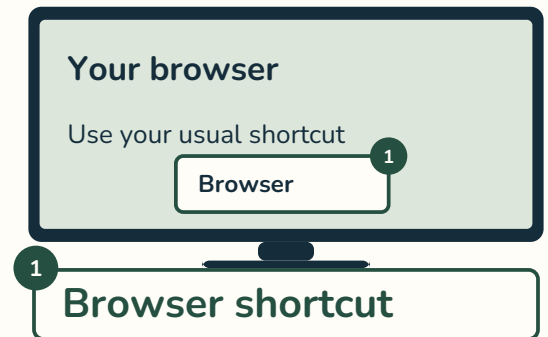
Windows | Reopen safely

The suspicious browser window must already be closed.

1 Open your browser.

Use its usual Start menu
or taskbar shortcut.

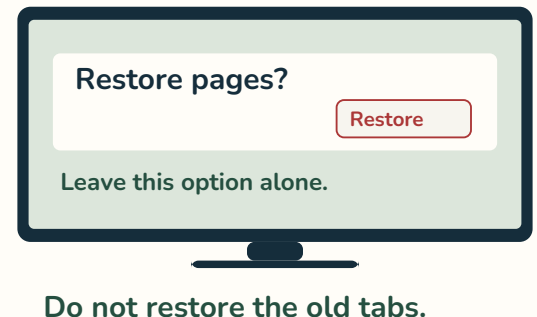
Step 1 of 3



2 Leave Restore alone.

Do not choose Restore pages
or Reopen previous tabs.

Step 2 of 3



If the warning returns by itself, stop and get help.

3 Type a known address.

Use the address bar to enter
a website you already trust.

Step 3 of 3



Do not return to the suspicious link.



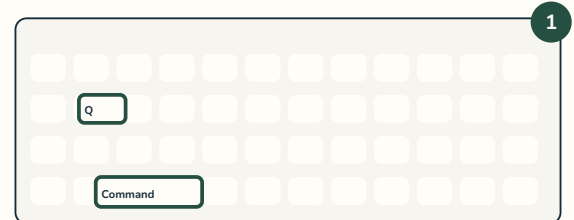
Mac | Try this first

Safari example • Keep Safari as the current app.

1 Quit Safari.

Hold **Command**, press **Q**,
then release both keys.

Step 1 of 3

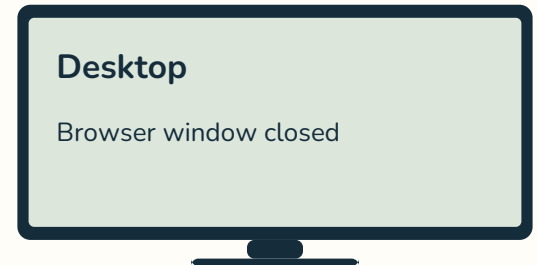


1
Command + Q

Step 2 of 3

2 Check the result.

If the warning is still there,
use page 7 before continuing.



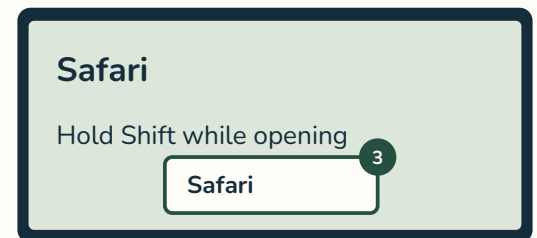
One calm step at a time.

Step 3 of 3

3 Reopen Safari with Shift.

Hold **Shift** while opening
Safari from its usual icon.

If the warning returns, stop. Do not interact with it.



3
Shift + Safari



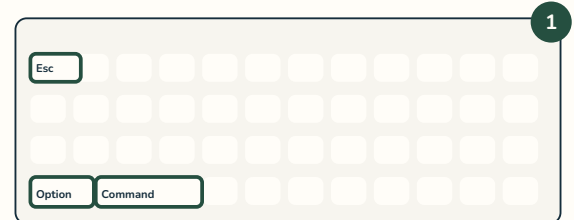
Mac | If Safari is stuck

Optional • Unsaved Safari work may be lost.

1 Open Force Quit.

Hold **Option** and **Command**,
then press **Esc**.

Step 1 of 3

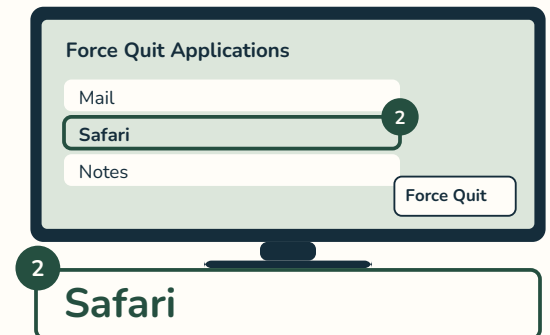


1
Option + Command + Esc

2 Select Safari.

Choose **Safari** in the
Force Quit Applications list.

Step 2 of 3



2
Safari

3 Click Force Quit.

If asked to confirm, click
Force Quit again.

Step 3 of 3



3
Force Quit

Return to page 6, step 3. If stuck, get trusted help.



If you already responded

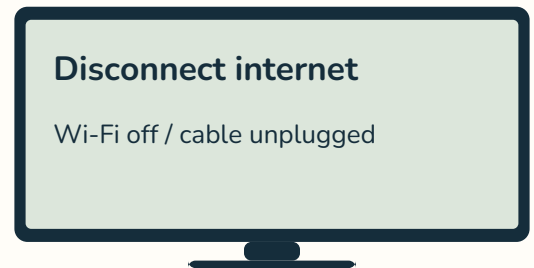
Closing a pop-up is not the same as securing accounts.

Step 1 of 3

1 Disconnect if access remains.

If a stranger may still control the device, disconnect internet.

Turn off Wi-Fi or unplug the network cable.

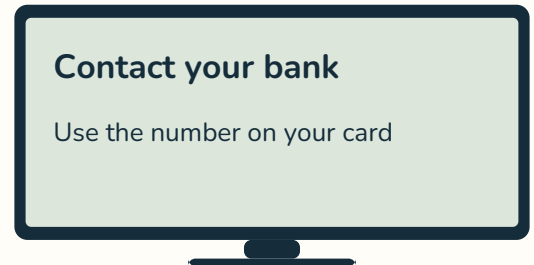


One calm step at a time.

Step 2 of 3

2 Call your payment provider.

If you paid or shared card details, use the number on your card.



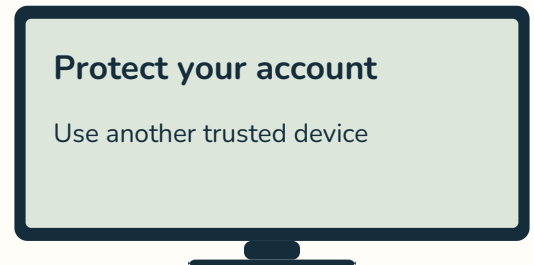
One calm step at a time.

Step 3 of 3

3 Secure an exposed account.

On a trusted device, change any password you shared.

For identity misuse, visit IdentityTheft.gov.



One calm step at a time.



Keep trusted help nearby

If a warning keeps returning, stop and get help. A closed browser is not proof that no software or account was affected.

For ongoing protection

Use the normal system and browser settings for updates. Ask for help checking pop-up blocking and deceptive-site protection. Do not install updates offered by an alarming webpage.

Reporting and recovery

Report scams at ReportFraud.ftc.gov.

For exposed identity information, visit IdentityTheft.gov.

Keep receipts and relevant messages if money was involved.

Microsoft: scams and closing the browser

Microsoft: Windows keyboard shortcuts

Apple: keyboard shortcuts

Apple: Force Quit

Apple: pop-ups and safe Safari reopening

FTC: recovery after a scam

Sources reviewed October 23, 2026. Illustrations are not actual screenshots.