BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Pop-Ups, Fake Virus Alerts & Notification Spam

Closing scare pages, stopping notification spam,
and what to do if one got through, in plain English

A plain-English guide to the first step of most tech-support scams

Closing a window can't hurt anything

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For Windows 11, Mac, iPhone, iPad & Android · facts current November 2026

What's Inside

This is your guide to scary pop-ups, fake virus alerts and the notifications that won't stop. Read it in any order. If a warning is on your screen right now, go straight to Part 2 for your device. Every step is slow and plain, and each one is safe: closing a window can't hurt your computer. It's written for Windows 11, recent Macs, iPhones and iPads, and Android phones including Samsung Galaxy; if a screen looks a little different on yours, the idea is still the same.

Part 1 — Understanding Scare Pop-Ups

1 A Note from Bill
2 Pop-Up, Alert or Notification? Knowing What's on Your Screen
3 Anatomy of a Fake Virus Alert
4 Why Real Warnings Never Look Like This
5 The Ten-Second Routine When One Appears

Part 2 — Closing a Scare Page Safely

6 Closing It on a Windows Computer
7 When the Browser Won't Close: Task Manager & Restart
8 Closing It on a Mac
9 Closing It on an iPhone or iPad
10 Closing It on an Android Phone or Tablet
11 After You Close It: Stopping It from Reopening

Part 3 — Stopping Notification Spam

12 How Notification Spam Gets In
13 Turning Off Notifications in Chrome on a Computer
14 Turning Off Notifications in Microsoft Edge
15 Turning Off Notifications in Safari on a Mac
16 Turning Off Notifications in Chrome on Android & Samsung Phones
17 Turning Off Notifications in Samsung Internet
18 iPhone & iPad: Web Apps and Calendar Spam

Part 4 — Cleaning Up a Hijacked Browser

19 Signs Your Browser Has Been Hijacked
20 Removing Bad Extensions
21 Resetting Chrome and Edge
22 Fixing Safari's Home Page, Search & Extensions on a Mac
23 Unwanted Programs: Checking Windows and Mac Apps

Part 5 — Turning On Built-In Protection

24 Browser Safety Settings Worth Turning On
25 Running a Real Virus Scan

Part 6 — If You Called the Number or Let Someone In

26 If You Called but Didn't Do Anything Else
27 If You Let Them onto Your Computer
28 If You Paid or Gave Out Personal Information
29 Reporting It

Part 7 — Keeping It from Happening Again

30 Everyday Habits That Keep Scare Pages Away
31 Helping a Parent or Loved One

Part 8 — When to Call Bill & Your Cheat-Sheet

32 When to Call Bill
33 Your Pop-Up Safety Cheat-Sheet

PART 1

Understanding Scare Pop-Ups

What is actually on your screen, how a fake virus alert is built, why real warnings never look like this, and the calm ten-second routine that beats every one of them.

CHAPTER 1

A Note from Bill

Hello, and welcome. If you've picked up this guide, there's a good chance a screen has already frightened you: a red warning, a siren sound, a message that your computer is "locked" and a phone number to call right now. Or maybe your phone keeps buzzing with alerts that your device is "infected" and you can't figure out where they're coming from. Either way, I want to start with the most important sentence in this whole guide.

A warning on your screen that tells you to call a phone number is not real. Not from Microsoft, not from Apple, not from your bank, not from anyone. It is a web page pretending to be a warning, and the person on the other end of that number is a scammer.

I'm Bill. With 30+ years of professional experience, I help folks here in Portage County feel at home and safe with their technology. I wrote this guide the way I'd explain it sitting beside you at the kitchen table: slowly, in plain English, one step at a time. Any word you might not know, I'll stop and explain right then.

What this guide covers

- **Spotting a scare page** in a couple of seconds, so it never gets its hooks in.
- **Closing it safely** on a Windows computer, a Mac, an iPhone or iPad, and an Android phone, even when it seems "stuck."
- **Stopping notification spam**, those pop-up alerts that keep appearing in the corner of your screen or on your phone.
- **Cleaning up a browser** that has had its search engine or home page changed behind your back.
- **What to do if you already called the number**, let someone onto your computer, or paid.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end, a scary pop-up will be an annoyance instead of an emergency. You'll know how to make it go away, how to keep it from coming back, and exactly who to call (and who never to call) if one gets through.

The big promise: closing a window can't hurt anything

A scare page wants you to believe that closing it will make things worse. It won't. Closing a browser tab, quitting a browser, or even restarting your computer is always safe. The worst that happens is you lose a half-finished web page. Nothing on your computer is harmed by walking away from a scam.

And you're never stuck alone. If something on your screen worries you, call me at **(330) 200-8042** before you call anyone else. There is no such thing as a silly question here.

— Bill

CHAPTER 2

Pop-Up, Alert or Notification? Knowing What's on Your Screen

People use the word "pop-up" for three different things. Knowing which one you're looking at tells you exactly how to get rid of it, so it's worth a minute to learn the difference.

What it is	Where it shows up	How it got there
A pop-up window or scare page	Inside your web browser (Chrome, Edge, Safari), often filling the whole screen	You visited a bad web page, usually by clicking an ad, a search result or a link
A website notification	In the corner of your computer screen or on your phone's lock screen, even when the browser is closed	At some point a website asked "Allow notifications?" and someone tapped **Allow**
A real system message	From Windows Security, macOS, iOS or Android itself	Your device is telling you something genuine, like an update being ready

Pop-ups and scare pages

A **pop-up** is a window or message a web page opens on top of what you were reading. Most are just ads. A **scare page** is a nasty kind of pop-up dressed up as a security warning. It lives entirely inside your web browser. Close the browser and it's gone.

Website notifications

A **notification** is a little message that slides in from the edge of the screen. Websites are allowed to send them, but only if you said yes first. Scam sites trick people into saying yes with messages like "Click Allow to confirm you're not a robot" or "Click Allow to play the video." After that, the alerts keep coming, even with the browser closed. They are covered in Part 3, starting with *How Notification Spam Gets In* (Chapter 12).

GOOD TO KNOW

Pop-up blockers don't stop notifications

Microsoft says it plainly on its Edge help page: unwanted pop-ups are not the same as website notifications. A pop-up blocker stops new windows from opening. It does nothing about a site you already allowed to send notifications. That takes a different setting, one per browser, and this guide walks you through each one.

Checked against Microsoft Support on November 13, 2026.

Real system messages

Your computer and phone do show real warnings now and then. The difference is in how they behave, which is the subject of *Why Real Warnings Never Look Like This* (Chapter 4). The short version: real warnings are calm, they never show a phone number, and they never demand payment.

CHAPTER 3

Anatomy of a Fake Virus Alert

Scare pages come in many costumes, but they're built from the same few parts. Once you can name the parts, you'll recognize the whole thing in a glance, the way you'd recognize a counterfeit bill that's printed on the wrong paper.

The usual ingredients

- **A famous logo.** Microsoft, Windows, Apple, McAfee, Norton, Geek Squad. The logo is copied; anyone can paste it onto a web page.
- **Alarming words.** "Your computer has been locked," "Trojan spyware detected," "Do not shut down," "Your files will be deleted."
- **A phone number.** Usually big, bold and repeated: "Call Microsoft Support immediately." This is the hook.
- **A countdown timer** to make you rush.
- **Sound.** A siren, a beeping alarm, or a recorded voice reading the warning out loud.
- **A page that seems frozen.** It fills the screen, the mouse seems not to work, and boxes keep reappearing when you try to close them.

GOOD TO KNOW

Why it seems locked

Scare pages use a normal browser feature called **full-screen mode** to hide the address bar and the close button, and they use tricks to keep reopening a little box every time you click. Your computer isn't actually locked. The browser is just being bossed around by one bad web page. Microsoft describes these pages exactly: they "may appear to block access to your machine so that you can't close them and may even use alarming sounds or recorded voices."

Checked against Microsoft Support on November 13, 2026.

Other versions you may see

- **"Your antivirus has expired"** with a Renew button. Real antivirus programs remind you inside the program, not on random web pages.
- **"Your phone is infected, tap to clean"** on an iPhone or Android. Web pages can't scan your phone.
- **A fake browser update**: "Chrome needs an update to continue." Microsoft warns that criminals disguise malware as browser updates.

- **A fake renewal invoice** in email: "You were charged $399.99 for Geek Squad / Norton / McAfee. Call within 24 hours to cancel." The FTC describes this exact scheme.

SCAM ALERT

The phone number is the whole scam

Everything on a scare page exists to get you to call. On the phone, a friendly-sounding "technician" asks to connect to your computer, pretends to find viruses, and then charges you to "fix" them, often by gift card, wire transfer, payment app or cryptocurrency. The FTC says scammers prefer those because "once you pay, it's hard to get your money back." No call, no scam.

Checked against the FTC's consumer advice on November 13, 2026.

CHAPTER 4

Why Real Warnings Never Look Like This

The single best defense is knowing what real warnings look like, so a fake one feels wrong right away. Here are the rules, straight from the companies scammers pretend to be.

Three rules that never bend

1. **Real warnings never give you a phone number to call.** Microsoft: "real error messages from Microsoft, or other big tech companies, never include phone numbers." The FTC: "Real security pop-up warnings and messages will never ask you to call a phone number."
2. **Real companies don't call or text you out of the blue** about a problem with your computer. Microsoft says it won't call you to offer tech support unless you contacted it first.
3. **Real help never asks for gift cards, wire transfers, cryptocurrency or a payment app.** Anyone who wants to be paid that way is a scammer.

Checked against Microsoft Support and the FTC's consumer advice on November 13, 2026.

What genuine warnings look like

Genuine	Fake
Comes from the program itself (Windows Security, your Mac, your phone's Settings)	Comes from a web page in your browser
Calm, plain wording	Shouting, sirens, countdowns
Offers a button that opens your own settings	Offers a phone number or a download
Goes away when you close it	Keeps reopening, fills the screen
Never asks for payment	Asks for payment, a card number, or a "support fee"

TIP

A quick test you can always use

Ask yourself: *is this inside my web browser?* If you can see a browser tab, an address bar, or the Chrome, Edge or Safari window around it, it's a web page, not your computer talking. Web pages can't see viruses on your computer.

FROM BILL

When you're not sure, ask first

If anything on your screen gives you pause, close it and call someone you trust: a family member, a friend, or me at (330) 200-8042. The FTC gives the same advice: talking it over with someone can help you see it's a scam. Never call a number the warning gives you.

CHAPTER 5

The Ten-Second Routine When One Appears

When a scare page pops up, your heart will race. That's normal, and it's exactly what the page is designed to do. Here is a routine short enough to remember in the moment. Read it now, while you're calm.

Stop, don't touch, close

1. **Stop.** Take a breath. Nothing bad is happening to your computer right now.
2. **Don't call, don't click inside it, don't type anything.** Not even on a button that says "Close" or "Cancel" inside the warning. Apple warns that some pop-ups have fake close buttons.
3. **Close the browser** using the steps for your device in Part 2: *Windows* (Chapter 6), *Mac* (Chapter 8), *iPhone or iPad* (Chapter 9), or *Android* (Chapter 10).
4. **If it won't close, restart the device.** Microsoft's own advice: close the browser, and if you can't, restart your computer.
5. **When it reopens**, don't restore the old tabs. *After You Close It: Stopping It from Reopening* (Chapter 11) shows how.

Checked against Apple Support and Microsoft Support on November 13, 2026.

STAY SAFE

Turn the sound down if it's blaring

The siren is just a sound file. Press the mute key on your keyboard or turn your speaker volume down so you can think. It has no connection to anything happening on your computer.

What you do NOT need to do

- You don't need to call anyone, including Microsoft or Apple.
- You don't need to buy anything or "renew" anything.
- You don't need to unplug your internet or throw the computer away.
- You don't need to be embarrassed. These pages fool careful, intelligent people every day.

GOOD TO KNOW

If it happened once, it's usually just the page

A single scare page that goes away after you close the browser was almost always caused by a bad web page or ad, not a virus. If they keep coming back on their own, or you see notifications in the corner of the screen, something else is going on, and Parts 3 and 4 cover that.

PART 2

Closing a Scare Page Safely

Step-by-step ways to close a full-screen, noisy, "locked" browser on Windows, Mac, iPhone, iPad and Android, and how to make sure it doesn't reopen.

CHAPTER 6

Closing It on a Windows Computer

Try these in order. Most of the time the first or second one does the job. Each step is safe.

Step 1: get out of full screen

Scare pages often switch the browser to full screen so you can't see the close button. Press the **Esc** key (top left of the keyboard) once or twice. If that doesn't do it, press **F11**, which switches full screen on and off in Chrome and Edge. On some laptops you need to hold the **Fn** key while pressing F11. When the browser's frame and tabs reappear, close the tab or the whole window with the **X** at the top right.

Step 2: the close-the-window keys

Hold down the **Alt** key and press **F4**. This closes whatever window is in front, which should be the browser. Microsoft recommends exactly this: "try pressing ALT+F4 if you can't do it with your mouse." If a little box pops up asking "Leave site?" or "Close tabs?", that one is from your browser itself, and choosing **Leave** or **Close** is fine. If you're not sure whether a box is from the browser or the scam, just press Alt+F4 again.

Checked against Microsoft Support on November 13, 2026.

Step 3: if nothing responds

Use Task Manager to end the browser (the next chapter, *When the Browser Won't Close: Task Manager & Restart* (Chapter 7)) or simply restart the computer. Restarting is always safe.

HEADS UP

Don't click inside the scam page to close it

Buttons painted on the page itself, like "OK," "Cancel," "Scan now" or even an X inside the warning, can be part of the trick. Use the keyboard or the browser's own close button at the very top of the window.

TIP

Practice once, when it isn't scary

Open your browser, press F11 to go full screen, then press F11 again to come back. Then press Alt+F4 to close it. Doing it once on a calm day makes it automatic on a bad one.

CHAPTER 7

When the Browser Won't Close: Task Manager & Restart

Task Manager is a built-in Windows tool that lists every program running and lets you shut any of them down. It's the "off switch" for a browser that won't listen.

End the browser with Task Manager

1. Press **Ctrl** + **Shift** + **Esc** together. Task Manager opens. (You can also right-click the **Start** button and choose **Task Manager**.)
2. If you see a small window with only a few names, click **More details** at the bottom.
3. On the **Processes** page, find your browser: **Google Chrome**, **Microsoft Edge** or **Firefox**.
4. Click it once to select it, then click **End task**.
5. The browser closes, scare page and all. Close Task Manager.

Checked against Microsoft Edge's scareware blocker help on November 13, 2026.

Or simply restart

If Task Manager won't open either, restart the computer. Click **Start**, then the **Power** button, then **Restart**. If you can't reach the Start menu, press **Ctrl** + **Alt** + **Delete** and use the power button at the bottom right of that screen. As a last resort, hold the computer's physical power button for about ten seconds until it turns off, wait a moment, and turn it back on.

GOOD TO KNOW

Holding the power button is safe here

Forcing the computer off isn't something to do every day, because you can lose unsaved work. But when a scam page has taken over, it's perfectly fine. The scare page won't survive a restart unless your browser reopens your old tabs, and the next chapter shows how to stop that.

TIP

Edge may close it for you

Microsoft Edge has a **Scareware blocker** that watches for full-screen scam pages. When it spots one, Edge exits full screen, silences the audio and shows a warning so you can close the page. See *Browser Safety Settings Worth Turning On* (Chapter 24) to make sure it's on.

CHAPTER 8

Closing It on a Mac

Macs get scare pages too, usually pretending to be from Apple. They're just as fake, and just as easy to close once you know the keys.

Step 1: leave full screen and close the tab

Press **Esc**. If the window is still full screen, press **Control** + **Command** + **F** to switch full screen off. Then close the tab with **Command** + **W**, or quit the whole browser with **Command** + **Q**.

Step 2: Force Quit

If the browser won't respond, force it to quit:

1. Press **Option** + **Command** + **Esc** together. (Or click the Apple menu at the top left of the screen and choose **Force Quit**.)
2. In the Force Quit window, click **Safari** (or Chrome, or whichever browser it is).
3. Click **Force Quit**, then confirm.

Checked against Apple Support on November 13, 2026.

Step 3: reopen Safari without the old tabs

Safari likes to reopen the windows you had before, which can bring the scare page right back. Apple's tip: quit Safari, then **press and hold the Shift key while you open Safari**. Holding Shift stops it from reopening any windows or tabs that were open.

Checked against Apple Support on November 13, 2026.

> **GOOD TO KNOW**
>
> **A restart is safe on a Mac, too**
>
> If all else fails, choose Apple menu > **Restart**. When the box appears asking whether to reopen windows when you log back in, uncheck that option. Apple also notes that macOS includes a built-in tool that removes known malware when restarting.

Checked against Apple Support on November 13, 2026.

CHAPTER 9

Closing It on an iPhone or iPad

On an iPhone or iPad, a scare page is always just a Safari (or Chrome) tab. Phones can't be "locked" or "infected" by a web page the way the message claims. Closing the tab ends it.

Close the tab in Safari

1. Don't tap anything on the warning itself.
2. Tap the **Tabs** button (two overlapping squares) at the bottom or top of Safari. If you don't see Safari's buttons, tap the very top or bottom edge of the screen to bring them back.
3. Find the scary tab and tap the small **X** on its corner, or swipe it away to the left.
4. Or, Apple's suggestion: tap the search field and type a new web address or search, which moves you away from the page.

Checked against Apple Support on November 13, 2026.

If Safari itself seems stuck

1. Swipe up from the bottom of the screen and pause in the middle to see your open apps. (On an iPhone with a Home button, press it twice.)
2. Swipe the Safari card up and off the screen. This closes Safari.
3. Open Safari again. If the bad tab is still there, close it from the Tabs view as above.

SCAM ALERT

"Your iPhone has 4 viruses" is always fake

A web page cannot scan your iPhone. Messages like "Your iPhone is damaged by viruses, tap here to clean" or "Apple Security Alert, call now" are ads designed to make you install something or call a number. Close the tab. You don't need to install any "cleaner" app.

TIP

Keep two protections switched on

Apple's help page lists two settings worth checking: **Settings** > **Apps** > **Safari**, then turn on **Block Pop-ups** and **Fraudulent Website Warning**. More in *Browser Safety Settings Worth Turning On* (Chapter 24).

Checked against Apple Support on November 13, 2026.

CHAPTER 10

Closing It on an Android Phone or Tablet

On Android phones, including Samsung Galaxy phones, scare pages show up in Chrome or Samsung Internet. Closing the tab ends them.

Close the tab

1. Don't tap the warning.
2. Tap the **tabs** button at the top or bottom of the browser (in Chrome it's a small square with a number in it).
3. Close the scary tab with its **X**, or swipe it away.

If the browser seems stuck

1. Open your recent apps: swipe up from the bottom and hold, or tap the **Recents** button (three lines) on phones that have navigation buttons.
2. Swipe the browser card up and away to close it.
3. Reopen the browser and close the bad tab if it's still there.
4. Still stuck? Hold the power button (on Samsung phones, the side key and volume down together) and choose **Restart**.

HEADS UP

Don't install anything a pop-up offers

Android pop-ups often say "Your battery is damaged" or "Install this cleaner to remove viruses" and send you to an app download. Close the tab instead. If you want real protection, it's already built in, and *Browser Safety Settings Worth Turning On* (Chapter 24) shows where.

GOOD TO KNOW

Notifications are a different problem

If the scary messages appear in your phone's notification shade (the list you see when you swipe down from the top), they're website notifications, not pop-ups. They need to be turned off in settings: see *Turning Off Notifications in Chrome on Android & Samsung Phones* (Chapter 16) for Chrome and *Turning Off Notifications in Samsung Internet* (Chapter 17) for Samsung Internet.

CHAPTER 11

After You Close It: Stopping It from Reopening

Sometimes the scare page comes right back the moment you reopen the browser. That's usually because the browser is helpfully "restoring" your last session. Here's how to start fresh.

Chrome and Edge

- When the browser reopens and offers **Restore** pages, don't click it. Close that little message.
- If the scam tab reopens anyway, close it right away with its X.
- If it reopens every single time, check what your browser is set to open on startup. In Chrome, go to **Settings** > **On startup**; in Edge, **Settings** > **Start, home, and new tabs**. Choose to open the New Tab page.

Safari on a Mac

Hold the **Shift** key while opening Safari, as in *Closing It on a Mac* (Chapter 8). That opens Safari with no old windows.

When it keeps coming back no matter what

If scare pages keep appearing on their own, even on sites you trust, you may have picked up an unwanted browser extension or program. Part 4 walks through finding and removing it, starting with *Signs Your Browser Has Been Hijacked* (Chapter 19).

TIP

Clear the browsing history if you like

Clearing your recent history keeps the scam address from popping up as a suggestion when you type. It isn't required, but it's tidy. In Chrome or Edge, press **Ctrl** + **Shift** + **Delete** on Windows (on a Mac, **Command** + **Shift** + **Delete**) and choose a time range like "Last hour."

WHAT THIS DOES FOR YOU

What this does for you

Once you know you can always close the window, restart, and start fresh, a scare page loses its power. It's just a page you didn't want to read.

PART 3

Stopping Notification Spam

Those "virus detected" alerts that slide in from the corner of the screen or land on your phone's lock screen. Where they come from, and how to switch them off in every major browser.

CHAPTER 12

How Notification Spam Gets In

If you're seeing alerts like "Your PC is infected!" or "McAfee: subscription expired" popping up in the corner of your screen, even when your browser is closed, you're almost certainly dealing with **website notification spam**. The good news is that it's easy to switch off.

How it starts

Every modern browser lets websites ask, "Can we send you notifications?" Plenty of honest sites use this for news headlines or appointment reminders. Scam sites abuse it. They show a message like:

- "Click **Allow** to confirm that you are not a robot."
- "Click **Allow** to watch the video."
- "Press **Allow** to continue."

Clicking Allow doesn't prove anything or play anything. It gives that website permission to send notifications to your computer or phone from then on. The site then sends fake virus warnings, fake prize messages and ads, each one linking to another scam page.

GOOD TO KNOW

They're not a virus

Notification spam is annoying and the messages are lies, but the notifications themselves are just a permission you can take back. Removing the permission stops them. You don't need to buy any software. Edge's help page notes that once a site has permission, its notifications "will still appear even if Microsoft Edge is closed," which is why they seem to come from nowhere.

Checked against Microsoft Support on November 13, 2026.

How to tell which browser is sending them

- **On Windows**, the notification usually names the browser at the top: "Google Chrome" or "Microsoft Edge," followed by the website's address.
- **On a Mac**, it shows the website's name and often a small Safari or Chrome icon.
- **On Android**, swipe down from the top. The notification shows the browser (Chrome or Samsung Internet) and the site.

- **On iPhone**, ordinary websites can't send notifications. If you see them, it's from a web app saved to your Home Screen, a real app, or calendar spam. See *iPhone & iPad: Web Apps and Calendar Spam* (Chapter 18).

TIP

Write down the website name

Before you dismiss one, note the web address it shows, like *news-alert-24.example*. When you open the notification settings in the chapters ahead, you'll know exactly which entry to block.

Your browser	Go to
Chrome on a computer	*Turning Off Notifications in Chrome on a Computer* (Chapter 13)
Microsoft Edge	*Turning Off Notifications in Microsoft Edge* (Chapter 14)
Safari on a Mac	*Turning Off Notifications in Safari on a Mac* (Chapter 15)
Chrome on Android or Samsung	*Turning Off Notifications in Chrome on Android & Samsung Phones* (Chapter 16)
Samsung Internet	*Turning Off Notifications in Samsung Internet* (Chapter 17)
iPhone or iPad	*iPhone & iPad: Web Apps and Calendar Spam* (Chapter 18)

CHAPTER 13

Turning Off Notifications in Chrome on a Computer

These steps work for Google Chrome on Windows and Mac. Google's own help page uses the same path.

Remove or block the spammy site

1. Open **Chrome**.
2. Click the three dots at the top right (**More**), then **Settings**.
3. Click **Privacy and security**, then **Site settings**, then **Notifications**.
4. Scroll to the list headed **Allowed to send notifications**. Look for any site you don't recognize or don't want.
5. Click the three dots next to that site and choose **Block** (or **Remove**). Do this for each unwanted site.

Checked against Google Chrome Help on November 13, 2026.

Stop sites from asking at all

On the same Notifications page, choose the option that **doesn't allow sites to send notifications**. Google also offers a middle ground, **Use quieter messaging**, which hides the "Allow notifications?" pop-up and shows only a small bell icon next to the address. For most people I'd simply turn them off. You can always allow one particular site later.

Checked against Google Chrome Help on November 13, 2026.

GOOD TO KNOW

Chrome is already watching for abuse

Google says that when you visit sites with intrusive or misleading notifications, Chrome automatically blocks them, and it may remove permission from sites you haven't visited in a while. Chrome's **Safety Check** (in **Settings** > **Privacy and security**) lists any permissions it removed.

Checked against Google Chrome Help on November 13, 2026.

TIP

The quickest fix while you're on the site

If you happen to be on the site, click the small icon just left of the web address (Google calls it **View site information**) and switch **Notifications** off.

HEADS UP

Removed but it came back?

If a site you blocked reappears in the allowed list by itself, something on the computer is changing your settings. That's a job for Part 4, starting with *Removing Bad Extensions* (Chapter 20).

CHAPTER 14

Turning Off Notifications in Microsoft Edge

Edge is the browser that comes with Windows 11, so it's the one I see notification spam in most often. Microsoft's help page gives two ways to stop it.

From Edge's settings

1. In Edge, click the three dots at the top right (**Settings and more**).
2. Click **Settings**, then **Privacy, search, and services**, then **Site permissions**, then **All sites**.
3. Click the website that's sending the notifications.
4. Find **Notifications** and choose **Block** from the drop-down menu.
5. Repeat for any other site you don't want.

Checked against Microsoft Support on November 13, 2026.

From the address bar

1. Go to the website.
2. Click **View site information** (the small icon to the left of the address).
3. Under **Permissions for this site**, set **Notifications** to **Block**.

Checked against Microsoft Support on November 13, 2026.

> GOOD TO KNOW
> **Menus move around**
> Microsoft has rearranged Edge's settings more than once. If you don't see **Privacy, search, and services**, type **notifications** into the search box at the top of Edge's Settings page and it will take you there.

Silencing Edge in Windows itself

Windows also has its own on/off switch for each app's notifications. Open **Start** > **Settings** > **System** > **Notifications**, find **Microsoft Edge** (or Google Chrome), and switch it off. This silences *every* notification from that browser, good and bad, so use it as a quick stopgap while you clean up the site permissions above.

TIP

Edge also blocks scam pages

While you're in Edge's settings, check that **Scareware blocker** is on. See *Browser Safety Settings Worth Turning On* (Chapter 24).

CHAPTER 15

Turning Off Notifications in Safari on a Mac

On a Mac, website notifications are managed in two places: System Settings (to switch off a site) and Safari's own settings (to remove it and stop new requests). These steps follow Apple's current Safari User Guide.

Stop one website's notifications

1. Click the Apple menu at the top left of the screen and choose **System Settings**.
2. Click **Notifications** in the sidebar. You may need to scroll down.
3. Under **Application Notifications**, click the website's name.
4. Turn off **Allow Notifications**.

Checked against Apple's Safari User Guide on November 13, 2026.

Remove the site and stop new requests

1. Open **Safari**.
2. From the menu bar, choose **Safari** > **Settings**.
3. Click **Websites**, then click **Notifications** in the list on the left.
4. Select any unwanted website and set it to **Deny**.
5. At the bottom, uncheck **Allow websites to ask for permission to send notifications**. From now on, sites won't even ask.

Checked against Apple's Safari User Guide on November 13, 2026.

GOOD TO KNOW

Why the site stays in the list

Apple notes that after you turn a site off in System Settings, it still appears in the Notifications list. To remove it from that list, deny it in Safari's Websites settings as shown above.

TIP

Using Chrome on your Mac?

Chrome's notification settings are the same on a Mac as on Windows. Follow *Turning Off Notifications in Chrome on a Computer* (Chapter 13).

CHAPTER 16

Turning Off Notifications in Chrome on Android & Samsung Phones

On Android phones, spammy website notifications land in the notification shade with everything else, so they can look very official. Here's how to shut them off in Chrome. Google's help page uses these exact steps.

Turn off notifications for all sites

1. Open **Chrome**.
2. Tap the three dots to the right of the address bar (**More**), then **Settings**.
3. Tap **Site settings**, then **Notifications**.
4. Turn the switch at the top off. Or leave it on and tap any unwanted site in the list below to block it.

Checked against Google Chrome Help on November 13, 2026.

Straight from the notification

On many phones you can swipe down to see the notification and tap **Unsubscribe** right on it. Chrome may also show its own warning when it thinks a notification is deceptive. When it does, tap **Unsubscribe**, then **Report spam to Chrome**.

Checked against Google Chrome Help on November 13, 2026.

Using Android's own settings

Samsung's support page describes another route that works for Chrome and Samsung Internet: open **Settings** > **Notifications**, tap the browser the notification came from, and under the list of sites, switch off the website. You can also press and hold (or slide) the notification itself and tap the settings gear to jump to the right place.

Checked against Samsung Support on November 13, 2026.

> **TIP**
>
> **Turn off pop-ups while you're there**
>
> In Chrome on Android: **More** > **Settings** > **Permissions** > **Pop-ups and redirects**, and turn it off so sites can't open new windows.

Checked against Google Chrome Help on November 13, 2026.

CHAPTER 17

Turning Off Notifications in Samsung Internet

Samsung Galaxy phones come with their own browser, **Samsung Internet** (a purple planet icon). It has its own notification list, separate from Chrome's.

Quickest way: from the notification

1. Swipe down from the top of the screen to see your notifications.
2. Slide the website notification slightly to the side (don't swipe it all the way off), then tap the **Settings** gear.
3. You'll land in the notification settings with that website highlighted. Switch it off.

Checked against Samsung Support on November 13, 2026.

From Android Settings

If you already dismissed the notification: open **Settings** > **Notifications**, tap **Samsung Internet**, and under Sites, switch off each website you don't want. Samsung notes that menus can vary by model and software version.

Checked against Samsung Support on November 13, 2026.

Inside Samsung Internet

Samsung Internet also has its own list of sites allowed to notify you. Open the app, tap the menu (three lines), tap **Settings**, and look for **Notifications** (on many versions it's under **Sites and downloads**). Block any site you don't recognize.

GOOD TO KNOW

Menu names vary

Samsung updates its browser often, and different guides describe slightly different menu names. If you can't find the browser's own list, the Android Settings route above always works.

CHAPTER 18

iPhone & iPad: Web Apps and Calendar Spam

iPhones and iPads handle website notifications differently. An ordinary web page in Safari can't send you notifications. So if you're getting unwanted alerts on an iPhone, it's usually one of three things.

1. A web app saved to the Home Screen

Since iOS 16.4, a website that's been added to your Home Screen can ask to send notifications. If you see alerts from one you don't want, open **Settings** > **Notifications**, scroll down to find the web app's name, and turn off **Allow Notifications**. Better still, press and hold its icon on the Home Screen and delete it.

2. Calendar spam

This one catches a lot of iPhone owners. Strange events appear in the Calendar app, like "Your iPhone may be infected, tap to clean" or "You won a prize," and they send alerts. They come from tapping a link that **subscribed** your calendar to a spam calendar, or from junk invitations. Don't tap links inside them.

Delete a single spam event

1. In the **Calendar** app, tap the unwanted event.
2. Tap **Delete Event**, then **Delete Event** again.
3. If it's an invitation from someone you don't know, tap **Report Junk**, then **Delete and Report Junk** instead.

Checked against Apple Support on November 13, 2026.

Remove a whole spam calendar

1. In the **Calendar** app, tap the **Calendars** button.
2. Find the calendar you don't recognize and tap the info button (the small **i**) next to it.
3. Tap **Delete Calendar** or **Unsubscribe**, then tap it again to confirm.

Checked against Apple Support on November 13, 2026.

> **TIP**
>
> **If it won't delete, hide it**
>
> Apple says some calendars can't be removed. You can hide any calendar by tapping **Calendars** and tapping to remove the checkmark next to it.

Checked against Apple Support on November 13, 2026.

3. An app you installed

If the alerts name a real app (a "cleaner," a "VPN" or a game), open **Settings** > **Notifications**, tap that app and turn notifications off, or delete the app. Any app that installed itself through a scary pop-up is best deleted.

SCAM ALERT

No app needs to "clean" your iPhone

Messages telling you to download an app to remove viruses from an iPhone are scams. Keep your iPhone updated and download apps only from the App Store, as Apple recommends.

PART 4

Cleaning Up a Hijacked Browser

When your search engine, home page or new-tab page has changed by itself, or scare pages keep returning. How to find the unwanted extension or program and put things back.

CHAPTER 19

Signs Your Browser Has Been Hijacked

A **hijacked** browser is one whose settings were changed without your say-so, usually by an **extension** (a small add-on program that lives inside the browser) or by a program that came bundled with something you downloaded. It's more annoying than dangerous, but it's worth cleaning up, because these add-ons often lead you to more scam pages.

Common signs

- Your searches suddenly go to an unfamiliar search site instead of Google or Bing.
- Your home page or new-tab page is a strange site covered in ads.
- Scare pages or pop-ups appear even on websites you trust.
- New toolbars or icons appear next to the address bar that you don't remember adding.
- A message says your browser is "managed by your organization" on a home computer.
- Settings you change keep changing back.

> **GOOD TO KNOW**
>
> **Browsers try to protect you**
>
> Google says Chrome checks every time it starts whether programs have changed your settings without your knowledge, and if something isn't right, it can reset your search engine, home page, startup pages, pinned tabs and extensions automatically.

Checked against Google Chrome Help on November 13, 2026.

The clean-up order

1. Remove any extension you don't recognize: *Removing Bad Extensions* (Chapter 20).
2. Reset the browser's settings: *Resetting Chrome and Edge* (Chapter 21) (Chrome and Edge) or *Fixing Safari's Home Page, Search & Extensions on a Mac* (Chapter 22) (Safari).
3. Look for unwanted programs on the computer: *Unwanted Programs: Checking Windows and Mac Apps* (Chapter 23).
4. Run a security scan: *Running a Real Virus Scan* (Chapter 25).

FROM BILL

"Managed by your organization" on a home computer

On a work laptop, that message is normal. On your own home computer, it can mean an unwanted program has put rules in place that a simple reset won't undo. That's a good time to call me at (330) 200-8042 rather than wrestle with it.

CHAPTER 20

Removing Bad Extensions

Extensions can be wonderful: password managers, ad blockers, a coupon helper you chose on purpose. The trouble comes from ones that sneak in. Google notes that sometimes when you install an application on Windows or Mac, it also installs a Chrome extension along with it.

Checked against Chrome Web Store Help on November 13, 2026.

In Chrome

1. Open Chrome, click the three dots (**More**) at the top right, then **Extensions** > **Manage extensions**.
2. Look through the list. For any you don't recognize or don't use, click **Remove**, then **Remove** again to confirm.
3. Not sure about one? Switch it off with its toggle instead. If the problems stop, remove it.

Checked against Chrome Web Store Help on November 13, 2026.

In Edge

1. Click the three dots (**Settings and more**), then **Extensions** > **Manage extensions**.
2. Turn each extension off. Microsoft suggests this test: if the pop-ups stop, turn them back on one at a time to find the culprit.
3. Click **Remove** under any you don't want.

Checked against Microsoft Support on November 13, 2026.

In Safari on a Mac

Choose **Safari** > **Settings**, then click **Extensions**. Uncheck any extension you don't want, or select it and click **Uninstall**. Apple specifically suggests checking this list if pop-ups won't go away.

Checked against Apple Support on November 13, 2026.

HEADS UP

Names can be misleading

Unwanted extensions often have friendly names like "Search Plus," "PDF Converter" or "Weather Now." The question isn't whether the name sounds nice, it's whether *you* installed it on purpose and still use it.

TIP

Add extensions only from the official store

Get Chrome extensions from the Chrome Web Store, Edge add-ons from Microsoft's add-ons site, and Safari extensions from the Mac App Store, and only ones you went looking for. Never install one because a pop-up told you to.

CHAPTER 21

Resetting Chrome and Edge

Resetting a browser puts its settings back the way they were when it was new, while keeping the things you care about most. It's a good second step after removing bad extensions.

Reset Chrome

1. Open Chrome, click the three dots (**More**) at the top right, then **Settings**.
2. Click **Reset settings**.
3. Click **Restore settings to their original defaults**, then **Reset settings**.

Checked against Google Chrome Help on November 13, 2026.

Google lists what goes back to the default:

- Your default search engine, home page and startup tabs, and the new-tab page.
- Pinned tabs.
- Content settings, like which sites may show pop-ups.
- Cookies and site data, so you'll be signed out of many websites.
- Extensions and themes are turned off (not deleted).

GOOD TO KNOW

What a Chrome reset keeps

Google says your saved bookmarks and passwords won't be deleted or changed. Because you'll be signed out of websites, make sure you know your important passwords (or have them in a password manager) first.

Checked against Google Chrome Help on November 13, 2026.

Reset Edge

1. Click the three dots (**Settings and more**), then **Settings**.
2. Click **Reset settings** in the menu on the left. (If you don't see it, type **reset** in the Settings search box.)
3. Click **Restore settings to their default values**, then **Reset**.

Like Chrome, an Edge reset sets your startup page, new-tab page, search engine and pinned tabs back to normal, turns off extensions and clears cookies, while keeping your favorites, history and saved passwords.

TIP

Set your search engine back on purpose

After a reset, do a quick search to make sure it goes to the search site you like. In Chrome it's under **Settings** > **Search engine**.

CHAPTER 22

Fixing Safari's Home Page, Search & Extensions on a Mac

Safari doesn't have a single reset button, but its key settings are easy to check one at a time.

Check four places

1. **Extensions: Safari** > **Settings** > **Extensions**. Uninstall anything you don't recognize (see *Removing Bad Extensions* (Chapter 20)).
2. **Home page: Safari** > **Settings** > **General**. Look at the **Homepage** box and type the address you want, or leave it blank.
3. **Search engine: Safari** > **Settings** > **Search**, and choose your preferred search engine.
4. **Notifications and pop-ups: Safari** > **Settings** > **Websites**. Check **Notifications** and **Pop-up Windows** in the list on the left (see *Turning Off Notifications in Safari on a Mac* (Chapter 15)).

GOOD TO KNOW

Apple's advice when pop-ups won't go away

Apple's help page for persistent pop-ups on a Mac recommends three things: update to the latest version of macOS (or restart if you're already up to date, since macOS removes known malware when restarting), check your Applications folder for apps you don't expect, and check Safari's Extensions list.

Checked against Apple Support on November 13, 2026.

HEADS UP

Look out for "profiles"

On a Mac, some unwanted programs install a configuration profile that controls Safari's settings. If your home page or search engine changes back no matter what you do, open **System Settings** and search for **Profiles**. If you see a profile you don't recognize on your personal Mac, that's worth a call before you remove anything.

CHAPTER 23

Unwanted Programs: Checking Windows and Mac Apps

If scare pages keep returning after you've cleaned up the browser, a program on the computer itself may be behind it. These usually arrive bundled with free downloads, or because a pop-up talked someone into installing a "cleaner" or "driver updater."

On Windows 11

1. Click **Start** > **Settings** > **Apps** > **Installed apps**.
2. Change the sort order to **Date installed** so the newest programs are at the top.
3. Look for anything installed around the time the trouble started that you don't recognize: "PC Cleaner," "Driver Booster," an odd search toolbar, or a remote-control program you didn't ask for.
4. Click the three dots next to it and choose **Uninstall**.

On a Mac

Open **Finder** and click **Applications**. Apple suggests checking this folder for apps you don't expect and deleting or uninstalling them. Drag an unwanted app to the Trash, then empty the Trash.

Checked against Apple Support on November 13, 2026.

HEADS UP

Don't uninstall things you're unsure about

Your computer has many programs with technical names that it needs, like drivers from your computer's maker or Microsoft runtime components. If you're not sure what something is, leave it and ask. Removing the wrong thing can cause more trouble than the pop-ups.

STAY SAFE

Remote-control programs need special attention

If you find a program like AnyDesk, TeamViewer, UltraViewer, ScreenConnect or LogMeIn that you didn't install for a reason you understand, a scammer may have used it to reach your computer. Uninstall it, and go straight to *If You Let Them onto Your Computer* (Chapter 27).

PART 5

Turning On Built-In Protection

Every major browser and computer already includes good, no-cost protection against scam pages. Here's where to find it and make sure it's switched on.

CHAPTER 24

Browser Safety Settings Worth Turning On

You don't need to buy anything to be well protected against scare pages. These built-in settings are free and take a minute each.

Microsoft Edge: Scareware blocker

Edge's **Scareware blocker** watches for pages that take over the screen with fake alerts, alarms or locked pages. Microsoft says that when a page matches known scam patterns, Edge exits full screen, silences the audio and shows a warning, giving you the option to close the page. It's on by default for most Windows and Mac computers with enough memory; on lower-powered computers you may need to turn it on, and on very low-powered ones the option may not appear.

1. In Edge, open **Settings**.
2. Click **Privacy, search, and services**, then **Security**.
3. Make sure **Scareware blocker** is switched on.

Checked against Microsoft's Edge scareware blocker page on November 13, 2026.

Microsoft Edge: pop-up blocker

Edge's pop-up blocker is on by default. To check: **Settings** > **Privacy, search, and services** > **Site permissions**, then under **Content** choose **Pop-ups and redirects** and make sure **Blocked (recommended)** is on.

Checked against Microsoft Support on November 13, 2026.

Google Chrome: Safe Browsing

Chrome's **Safe Browsing** warns you about dangerous sites, downloads and extensions. **Standard protection** is on by default. **Enhanced protection** also warns about new dangers Google didn't know about before, at the cost of sending more browsing information to Google for security checks.

1. In Chrome, open **Settings**.
2. Click **Privacy and security**, then **Security**.
3. Choose **Enhanced protection** or **Standard protection**. Never choose **No protection**.

Checked against Google Chrome Help on November 13, 2026.

Safari on iPhone, iPad and Mac

- **iPhone or iPad: Settings** > **Apps** > **Safari**. Turn on **Block Pop-ups** and **Fraudulent Website Warning**.
- **Mac: Safari** > **Settings**. In the **Security** tab, turn on the warning for fraudulent websites. In the **Websites** tab, set **Pop-up Windows** to block.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

Ads that look like pop-ups

Microsoft points out that some ads are drawn right into the web page to look like pop-ups, and a pop-up blocker can't stop those. That's why the habit in *The Ten-Second Routine When One Appears* (Chapter 5) matters more than any setting.

Checked against Microsoft Support on November 13, 2026.

TIP

Keep everything updated

Apple and Microsoft both stress installing the latest updates. Many updates include security fixes that help control pop-ups. Turn on automatic updates for your computer, phone and browser.

CHAPTER 25

Running a Real Virus Scan

If you're worried something unwanted got onto your computer, run a scan with the security software you already have. The FTC's advice when you think there may be a problem is simple: update your security software and run a scan.

Checked against the FTC's consumer advice on November 13, 2026.

On Windows 11: Windows Security

Windows 11 includes **Microsoft Defender Antivirus** in the **Windows Security** app. It's on by default unless you've installed another antivirus program.

1. Click **Start**, type **Windows Security**, and open it.
2. Click **Virus & threat protection**.
3. Click **Quick scan** for a fast check. For a deeper look, click **Scan options**.
4. If you suspect something stubborn, choose **Microsoft Defender Offline scan** in Scan options and click **Scan now**. Your computer restarts, scans, and restarts again, so save your work first.
5. Afterward, see results under **Protection history**.

Checked against Microsoft Support on November 13, 2026.

On a Mac

Macs include built-in malware protection. Apple's advice for persistent pop-ups is to update to the latest macOS, and if you're already up to date, restart, because macOS removes known malware when restarting.

Checked against Apple Support on November 13, 2026.

On a phone

Keep your iPhone or Android updated and install apps only from the App Store or Google Play. On Android, Google Play Protect is built in and checks apps for you. You don't need a "cleaner" app.

SCAM ALERT

Never run a scan someone on the phone tells you to

Scammers love to "show" you a scan that finds hundreds of problems. A real scan is one *you* start, from the security program already on your computer, with nobody else connected.

GOOD TO KNOW

Thinking about paid antivirus?

That's a fair question with an honest answer that depends on your situation. Our companion manual on antivirus and Windows Security covers Windows Security versus Norton and McAfee, renewals and fake renewal emails.

PART 6

If You Called the Number or Let Someone In

Calm, practical steps if you phoned a scammer, let them connect to your computer, paid, or gave out personal information. It's fixable, and the sooner you act, the better.

CHAPTER 26

If You Called but Didn't Do Anything Else

First, well done for stopping. If you called the number, talked to someone, then hung up without letting them onto your computer, paying, or giving out passwords or account numbers, you are in good shape.

What to do now

1. **Hang up and don't call back.** If they call you again, don't answer, or hang up as soon as you recognize them.
2. **Close the scare page** using Part 2.
3. **Think back carefully**: did you give them your name, address, email, date of birth, any part of your Social Security number, a card number, or a password? If so, go to *If You Paid or Gave Out Personal Information* (Chapter 28).
4. **Report it** to the FTC at **ReportFraud.ftc.gov**. See *Reporting It* (Chapter 29).

Checked against the FTC's consumer advice on November 13, 2026.

HEADS UP

Expect a follow-up call

Scammers who got your phone number may call back pretending to be a "refund department" or even a government agency offering to help. The FTC warns that tech support scammers sometimes hand you off to a fake government official who says your money is at risk. Someone who works for the government will never tell you to move your money to "protect it."

Checked against the FTC's consumer advice on November 13, 2026.

WHAT THIS DOES FOR YOU

You did the right thing

Calling a number in a moment of fright is human. Stopping before you gave them access or money is exactly what keeps people safe. Give yourself credit.

CHAPTER 27

If You Let Them onto Your Computer

If you let a "technician" connect to your computer, don't panic, but do act today. While connected, they may have installed a program that lets them get back in, looked at files, or watched you sign in to accounts.

Right away

1. **Disconnect**: if they're still connected, turn off your Wi-Fi or unplug the internet cable, or simply shut the computer down.
2. **From a different device** (your phone or another computer), **change the password for your email first**, then your bank, and any account you signed in to while they were connected. If you use the same password anywhere else, change it there too.
3. **Turn on two-step verification** (also called two-factor authentication) for email and banking.
4. **Call your bank and credit card companies** using the number on the back of your card if you signed in to banking or shared any card details while they were connected.

Checked against the FTC's consumer advice on November 13, 2026.

Then clean the computer

The FTC's steps if you gave a scammer access to your computer: update your security software (or install some), run a scan, delete anything it identifies as a problem, then change your passwords and turn on two-factor authentication.

Checked against the FTC's consumer advice on November 13, 2026.

- Uninstall any remote-control program they had you install (*Unwanted Programs: Checking Windows and Mac Apps* (Chapter 23)).
- Run a full scan, ideally a Microsoft Defender Offline scan on Windows (*Running a Real Virus Scan* (Chapter 25)).
- Check your browser for extensions you didn't add (*Removing Bad Extensions* (Chapter 20)).

FROM BILL

This is a good time to get help

Making sure a scammer has no way back in is fiddly work, and it's exactly what I help people with. I can check for remote-access programs, clean up the browser, run proper scans and help you change passwords in the right order. Call (330) 200-8042. My help is $49 remote · $99 in your home.

STAY SAFE

If they knew your bank login

Scammers sometimes "accidentally refund" too much and ask you to send the difference back. That's a trick: nothing was refunded; they moved your own money around. Never send money back to a "tech support" company.

CHAPTER 28

If You Paid or Gave Out Personal Information

If you paid a scammer, act quickly. The FTC says it's always worth asking the company you used to send the money if there's a way to get it back. How you paid decides who to call.

How you paid	Who to contact right away	Ask them to
Credit card	Your card company (number on the back of the card)	Reverse the charge and refund your money
Debit card	Your bank or credit union (number on the back of the card)	Reverse the charge and refund your money
Zelle or bank transfer	Your bank or credit union	Reverse the payment
Payment app (Venmo, Cash App, PayPal)	The payment app	Reverse the payment
Gift card	The gift card company (number on the back of the card)	Refund the money. Keep the card and receipt.
Wire transfer (Western Union, MoneyGram)	The wire transfer company	Refund the money; say a scammer tricked you
Cryptocurrency	The crypto exchange or ATM operator	Reverse the transaction
Cash by mail	U.S. Postal Inspection Service, 1-877-876-2455	Intercept the package (fee applies)

Checked against the FTC's consumer advice on November 13, 2026.

GOOD TO KNOW

Credit cards give you the most protection

The FTC notes that federal law protects you from unauthorized use of your credit and debit cards, while cryptocurrency payments don't have the same legal protections. Gift cards and wires are hard to recover, which is exactly why scammers ask for them.

Checked against the FTC's consumer advice on November 13, 2026.

If you gave out personal information

- **Your Social Security number**, and it was used: report it at **IdentityTheft.gov** to get a personalized recovery plan. If you're not sure it was used, follow the steps at **IdentityTheft.gov/databreach**.
- **A password**: change it right away, plus anywhere else you used it, and turn on two-factor authentication.

- **A card or bank account number**: call that bank or card company now.

Checked against the FTC's consumer advice on November 13, 2026.

SCAM ALERT

Watch out for "recovery" scams

After a scam, you may hear from someone offering to get your money back for a fee. Nobody legitimate charges you up front to recover money lost to a scam. Our companion manual on credit freezes and identity theft covers freezing your credit if your Social Security number was shared.

CHAPTER 29

Reporting It

Reporting doesn't usually bring money back by itself, but it helps stop scammers and protects your neighbors. The FTC says it uses reports to build cases, spot trends and warn the public.

Where to report

Who	When and how
FTC	**ReportFraud.ftc.gov**. For any tech support scam, whether you lost money or not.
Microsoft	**microsoft.com/reportascam**, if the scammer pretended to be Microsoft.
Your bank or card company	Right away, if money or account details were involved.
IdentityTheft.gov	If your Social Security number or identity was misused.
Local police	Especially if you lost money; your bank may ask for a report number.

Checked against the FTC's consumer advice and Microsoft Support on November 13, 2026.

TIP

Write things down while they're fresh

Note the phone number you called, the website address, the names they used, what you paid and how, and the time. A photo of the screen with your phone is handy, too. Reports and bank disputes go much faster with details.

STAY SAFE

Tell someone you trust

Scammers count on embarrassment to keep people quiet. Telling a family member or friend helps you think clearly, and it might stop the same scam from reaching them.

PART 7

Keeping It from Happening Again

A handful of everyday habits that keep scare pages and notification spam away, and how to set up a loved one's devices so they're protected too.

CHAPTER 30

Everyday Habits That Keep Scare Pages Away

Most scare pages arrive through the same few doors. Close those doors and you'll rarely see one.

Five habits

1. **Say no to "Allow notifications."** Unless it's a site you use every day and want alerts from, click **Block** or **Don't allow**. Never click Allow to "prove you're not a robot."
2. **Be careful with search ads.** The FTC warns that tech support scammers try to get their sites into search results and run their own ads. When looking for a company's help line, go to the company's own website by typing its address.
3. **Download software only from the source.** Apple says the safest place for apps is the App Store; otherwise get software directly from the developer, not through an ad or link. The same goes for Windows: get programs from the Microsoft Store or the maker's own site.
4. **Update the browser from its own menu.** Microsoft says that if you see an unusual notice that your browser needs an update, close it and go to the browser's **Help** > **About** page, which checks for real updates.
5. **Pause before you call.** If anything tells you to call a number, don't. Look up the company's real number yourself, or call someone you trust.

Checked against the FTC's consumer advice, Apple Support and Microsoft Support on November 13, 2026.

TIP

Bookmark the sites you use most

If you visit your bank, your email and your favorite news site from bookmarks instead of searching for them each time, you'll almost never land on a look-alike page.

GOOD TO KNOW

Fake renewal emails are the same trick

An email saying you were charged for a Norton, McAfee or Geek Squad renewal and must call within 24 hours is the inbox version of a scare page. The FTC's advice: don't use the number in the message. Check your card or bank statement. If there's no charge, it was a scam; delete it.

Checked against the FTC's consumer advice on November 13, 2026.

CHAPTER 31

Helping a Parent or Loved One

If you're the family member who gets the panicked phone call, here's how to set up a loved one's devices so the call happens less often, and what to say when it does.

A one-visit setup

- Turn off website notifications in every browser they use (Part 3), and turn off "sites can ask."
- Remove extensions and programs they don't need (Part 4).
- On Windows, make sure Edge's Scareware blocker and Windows Security are on; on iPhone, turn on Block Pop-ups and Fraudulent Website Warning (Part 5).
- Turn on automatic updates.
- Delete any spam calendars on their iPhone (*iPhone & iPad: Web Apps and Calendar Spam* (Chapter 18)).
- Put your number, or mine, on a sticky note by the computer with the words: **"Scary message? Don't call it. Call me."**

What to say on the phone

- "You haven't done anything wrong. It's a fake web page."
- "Don't call the number on the screen. Let's close it together."
- Walk them through the keys in Part 2 for their device, slowly.
- Ask gently whether they called the number, let anyone connect, or paid. If yes, go to Part 6 together.

STAY SAFE

Embarrassment is the scammer's best friend

People who've been fooled often hide it, which lets the scammer come back. Make it easy to tell you. A calm "thank you for telling me" does more good than any software.

FROM BILL

Happy to help with the setup

If you'd like me to go through a loved one's computer or phone and switch all of this on, I can do it remotely or in their home. $49 remote · $99 in your home. Call (330) 200-8042 or book at billshometech.com/book.

PART 8

When to Call Bill & Your Cheat-Sheet

When it's worth picking up the phone, and a one-page summary to keep by the computer.

CHAPTER 32

When to Call Bill

This guide gives you everything you need to handle a scare page yourself. But some situations are worth a second set of eyes, and I'd always rather hear from you before something goes wrong than after.

Call me when

- **You let someone connect to your computer**, or installed a program a caller asked you to.
- **You paid** a "tech support" company, or shared a card or bank number.
- **Pop-ups keep coming back** after you've followed Parts 3 and 4.
- **Your browser says it's "managed by your organization"** on a home computer.
- **You'd like everything set up properly** on your computer, phone or a loved one's devices.
- **Something just doesn't feel right.** Trust that feeling.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience, I help folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't rush and I don't talk down to anyone. Whether it's a two-minute "is this real?" call or a full clean-up, we'll handle it together. $49 remote · $99 in your home. Call **(330) 200-8042** or book a time at **billshometech.com/book**. My AI receptionist, Sophie, may answer when you call.

SCAM ALERT

The one number never to call

The number on a scary pop-up. Every time. Call someone you know instead.

Thank you for taking the time to learn this. You now know more about scare pages than most people ever will, and that makes you very hard to fool.

— Bill

CHAPTER 33

Your Pop-Up Safety Cheat-Sheet

Copy this onto a card and keep it by your computer.

The golden rule

A warning that tells you to call a phone number is always a scam. Real warnings never include a phone number.

When one appears

1. Stop. Don't call, click or type.
2. Close the browser (keys below).
3. Won't close? Restart.
4. Reopen without the old tabs.

The keys

Device	Leave full screen	Close it	Force it closed
Windows	Esc or F11	Alt + F4	Ctrl + Shift + Esc, End task
Mac	Esc or Control + Command + F	Command + Q	Option + Command + Esc
iPhone / iPad	-	Tabs button, X on the tab	Swipe Safari away
Android	-	Tabs button, X on the tab	Recents, swipe browser away

Stop notification spam

Browser	Where
Chrome (computer)	Settings > Privacy and security > Site settings > Notifications
Edge	Settings > Privacy, search, and services > Site permissions > All sites
Safari (Mac)	System Settings > Notifications; Safari > Settings > Websites > Notifications
Chrome (Android)	More > Settings > Site settings > Notifications
Samsung Internet	Settings > Notifications > Samsung Internet

Browser	Where
iPhone calendar spam	Calendar > Calendars > info button > Delete Calendar or Unsubscribe

If you called, let them in, or paid

- Disconnect the computer from the internet.
- From another device, change your email password first, then banking.
- Call your bank or card company (number on the back of the card).
- Run a scan with Windows Security, or update and restart your Mac.
- Report it: **ReportFraud.ftc.gov**.

Checked against the FTC's consumer advice, Microsoft Support, Google Chrome Help, Apple Support and Samsung Support on November 13, 2026.

WHAT THIS DOES FOR YOU

You're ready

A scare page is just a web page. You know how to close it, how to stop the notifications, how to clean up after it, and what to do if one ever gets further. That's real peace of mind.

Bill's Home Tech · Complete Manuals Series · (330) 200-8042 · billshometech.com · Portage County, Ohio