



# A Company You Use Got Breached — What to Do Now

The calm steps to take now

————— An Extended Guide · No. 1653 · PASSWORDS & SECURITY —————

**Tech Made Simple. Service Made Personal.**

**Bill Davis — Bill's Home Tech**

(330) 200-8042 · [bill@billshometech.com](mailto:bill@billshometech.com) · Atwater, Ohio

**Book a visit — [billshometech.com/book](https://billshometech.com/book)**

# What's Inside

*Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.*

|                                                                  |    |
|------------------------------------------------------------------|----|
| 1. A breach notice is manageable . . . . .                       | 4  |
| 2. First question: is the notice even real? . . . . .            | 4  |
| 3. Telling a real notice from a fake one . . . . .               | 5  |
| 4. How to verify a notice yourself . . . . .                     | 6  |
| 5. The calm response, step by step . . . . .                     | 6  |
| 6. Step one: change that password . . . . .                      | 7  |
| 7. Step two: fix the password everywhere you reused it . . . . . | 7  |
| 8. Step three: turn on two-factor . . . . .                      | 8  |
| 9. Step four: watch your statements . . . . .                    | 9  |
| 10. Step five: consider a credit freeze . . . . .                | 9  |
| 11. Free credit monitoring offers . . . . .                      | 10 |
| 12. What kind of data leaked matters . . . . .                   | 10 |
| 13. When it crosses into identity theft . . . . .                | 11 |
| 14. identitytheft.gov: the one place to start . . . . .          | 12 |
| 15. Freezing and fraud alerts for theft . . . . .                | 12 |
| 16. Don't let the notice rush you . . . . .                      | 13 |
| 17. After a well-known breach in the news . . . . .              | 13 |
| 18. Checking what else may have leaked . . . . .                 | 14 |
| 19. Why unique passwords soften every breach . . . . .           | 14 |
| 20. Helping a spouse or parent respond . . . . .                 | 15 |
| 21. What a breach does not mean . . . . .                        | 16 |

|                                                     |    |
|-----------------------------------------------------|----|
| 22. Keeping records, just in case . . . . .         | 16 |
| 23. A gentle version for the computer-shy . . . . . | 17 |
| 24. Breaches at your bank or card issuer . . . . .  | 17 |
| 25. Breaches at email or tech accounts . . . . .    | 18 |
| 26. Watch for follow-on scams . . . . .             | 19 |
| 27. Staying calm the next time, too . . . . .       | 19 |
| 28. Putting it all together . . . . .               | 20 |
| Your Breach-Response Cheat Sheet . . . . .          | 20 |
| Plain-English Word List . . . . .                   | 21 |
| A Picture to Follow Along . . . . .                 | 23 |
| A Second Look . . . . .                             | 24 |
| A Note From Bill . . . . .                          | 24 |
| Your Visit — and My Promise . . . . .               | 25 |

## 1. A breach notice is manageable

*Unsettling to receive, but there's a clear path through it.*

A letter or email arrives saying a company you do business with has suffered a data breach, and some of your information may have been exposed. It's a jolt — your mind jumps to the worst. Take a breath. A breach notice is common, it's rarely your fault, and there's a short, clear set of steps that handles it calmly.

The companies most of us use — stores, airlines, insurers, service providers — hold our information, and from time to time one of them gets broken into. When that happens, they're generally required to tell the people affected. So a notice, unwelcome as it is, is the system working the way it should: you're being warned so you can protect yourself.

### GOOD TO KNOW

Getting a breach notice doesn't mean you've been robbed or that your identity is stolen. It means information was exposed and you should take a few sensible steps. Acting promptly is what keeps a scare from becoming a problem.

This guide does two things. First, it helps you tell a genuine notice from a scam dressed up to look like one — because that's the first trap. Then it walks you through the calm response, in order, so you know exactly what to do and what you can safely skip.

## 2. First question: is the notice even real?

*Scammers send fake breach notices to cause exactly this panic.*

Before you do anything a notice tells you to, pause on one question: is this notice genuine? Scammers know that a 'your data was breached' message makes people anxious and quick to click. So a favorite trick is to send a fake breach notice — by email or text — that imitates a real company, with a link to 'secure your account.' The link leads to a copycat page built to steal your password.

This is the cruel twist of breaches: the notice itself might be the attack. The fear a real breach would cause is exactly what the fake one manufactures, to rush you past your good judgment. So the first skill is telling the two apart, which, happily, follows consistent patterns.

**WATCH OUT**

Never act on a breach notice by clicking a link inside it. If the message says to change your password or verify your account, do it by going to the company's site yourself — typing the address — not through the message.

The rest of this guide assumes you've confirmed the notice is real, or that you're responding by going directly to the company yourself. Let's look at how to spot the genuine article.

### 3. Telling a real notice from a fake one

*The tells are consistent once you know them.*

Real breach notices and phishing fakes have different personalities, and once you've seen the contrast you'll spot it quickly. A genuine notice tends to inform and advise; a fake one pressures and rushes. Here's what to weigh.

- A real notice usually explains what happened and what information was involved.
- A real notice advises steps but doesn't need you to click a link to take them.
- A fake one is vague about details but loud about urgency — 'act now or lose access.'
- A fake one pushes a 'click here to secure your account' link as the only option.
- No real company asks you to confirm or enter your current password in a breach email.

When something feels off — the urgency, the demand to click, the request for a password — trust that feeling. The safe move is always the same: ignore the message's links and go to the company directly, by typing its web address or calling the number on your card or statement.

**TIP**

My guide on spotting a fake login page goes deeper on the copycat sites these links lead to. The two skills pair well: recognizing the fake message, and recognizing the fake page it would send you to.

## 4. How to verify a notice yourself

*Go to the source — don't let the message lead you.*

If you're unsure whether a notice is real, you can confirm it without touching anything in the message. The principle is to reach the company through a path you control, so that even if the notice was a fake, you end up in the genuine place.

- 1 Don't click any link or call any number in the message itself.
- 2 Open your browser and type the company's web address yourself, then sign in.
- 3 Look for any security notice or alert inside your account.
- 4 Or call the company using the number on your card, bill, or official site.
- 5 Ask them plainly whether there was a breach and what they advise.

A real breach is usually easy to confirm this way — the company will have posted about it, or their support line will know. If you reach the genuine company and they've no record of any breach or any message to you, then what you received was a scam, and you can delete it with confidence.

### WATCH OUT

The phone number in a suspicious message can be part of the scam, connecting you to the crooks themselves. Always use a number you find independently — on the back of your card or a statement — not one the message provides.

## 5. The calm response, step by step

*A short routine, done in order, closes the risk.*

Once you know the breach is real, the response is a short, orderly routine. You're not reacting in fear — you're working through a checklist. Doing these in order means each step builds on the last, and by the end the exposed information can't be used against you.

- 1 Change the password for the breached account to a new, strong, unique one.
- 2 Change that password anywhere else you used it.
- 3 Turn on two-factor sign-in for the account if it isn't already.
- 4 Watch your bank and card statements for charges you don't recognize.
- 5 If sensitive data was exposed, consider freezing your credit.

That's the heart of the whole guide. The first three steps lock down the account itself; the fourth catches any misuse early; the fifth protects the bigger picture when the breach involved more than a password. We'll take each in turn so you know exactly what it involves.

**GOOD TO KNOW**

You don't always need every step. A breach that exposed only an email address needs little more than awareness. One that exposed passwords or financial details deserves the full routine. The notice usually tells you which you're dealing with.

## 6. Step one: change that password

*The first and most important move.*

The moment you know an account was breached, change its password. This is the single most effective step, because it makes any exposed password worthless. Choose a new password that's long, strong, and unlike any you use elsewhere. A password manager can generate and remember one for you, which is the easiest way to get a good one.

- 1 Go to the company's site by typing its address yourself, and sign in.
- 2 Find the security or account settings and choose to change your password.
- 3 Set a new, long, unique password — let your manager create it if you have one.
- 4 Save the new password so you don't have to memorize it.

If you can't sign in because the breach involved your account being tampered with, use the company's 'forgot password' or account-recovery process, or call their support line. Getting back in and setting a fresh password is the priority.

**TIP**

Make the new password genuinely different, not a small tweak of the old one. Adding a number to the end of a leaked password barely helps. A fresh, unrelated password is what actually closes the door.

## 7. Step two: fix the password everywhere you reused it

*This is where a single breach quietly spreads — or doesn't.*

Here's the step people skip, and it's the most important one after changing the breached password itself. If you used that same password on any other account, those accounts are now at risk too, because criminals take a breached password and try it on many other sites. So change the password anywhere you reused it.

Think through where that password might have traveled — your email, your bank, your shopping accounts. Change each one to its own unique password. This is tedious if you reused a password widely, which is precisely the argument for giving every account a

unique one going forward, so a future breach can never spread like this again.

- List the accounts where you might have used the same password.
- Change each to its own new, unique password.
- Prioritize email and financial accounts — those matter most.
- Going forward, let a manager give every account a unique password.

#### WATCH OUT

If the breached password was also your email password, treat that as urgent. Your email is the master key — whoever controls it can reset your other accounts. Change it first and turn on two-factor there.

## 8. Step three: turn on two-factor

*A second lock so a stolen password can't be used.*

After changing the password, turn on two-factor sign-in for the account if you haven't already. With it on, getting in needs your password plus a second step — a code, a tap, or a key. That means even if the new password were somehow exposed in a future breach, a criminal still couldn't get in without that second factor.

This step turns a one-time fix into lasting protection. It's especially worth doing on the accounts that matter most: your email, your bank, and your password manager. Any form of two-factor is far better than none, so if the choice feels overwhelming, just pick one and turn it on.

- Look under the account's Security or Sign-in settings for 'two-factor' or '2-step.'
- An authenticator app or a tap-to-approve is sturdier than a texted code.
- Save any backup codes it gives you in a safe place.

#### GOOD TO KNOW

My guide on two-factor the simple way compares the app, text, and email methods in plain terms. And my guide on recovery codes covers saving the backup codes two-factor gives you, so you're never locked out.

## 9. Step four: watch your statements

*Early eyes catch misuse while it's small.*

For a few weeks and months after a breach, keep a closer eye on your bank and credit-card statements. If exposed information is going to be misused, unfamiliar charges are often the first visible sign. Catching one early — even a tiny test charge — lets you stop the problem before it grows.

- 1 Review your bank and card statements more carefully than usual.
- 2 Turn on free transaction alerts in your banking and card apps.
- 3 Question even small, odd charges — thieves often test with tiny ones.
- 4 Report anything you don't recognize to your bank or card issuer right away.

Free transaction alerts are the easiest way to do this without effort — your bank texts or emails you when a charge posts, so you don't have to remember to check. Report anything unfamiliar promptly; card issuers are used to this and will reverse fraudulent charges and reissue the card.

### WATCH OUT

A small, strange charge you don't recognize is worth a call even if it seems trivial. Thieves often test a card with a tiny purchase before attempting a large one. Spotting the test stops the rest.

## 10. Step five: consider a credit freeze

*When sensitive data leaked, this is the strongest shield.*

If the breach exposed more than a password — a Social Security number, a date of birth, financial account details — the concern widens from that one account to your identity itself. The strongest protection against someone opening new accounts in your name is a credit freeze, and it's free by law at all three credit bureaus.

A freeze locks your credit file so new lenders can't see it, which blocks the main thing an identity thief wants to do. It doesn't affect your existing accounts or your credit score, and you can lift it briefly whenever you apply for credit yourself. For the kind of breach that exposes sensitive data, it's the single best move.

- Freeze at all three bureaus — Equifax, Experian, and TransUnion.
- It's free, by law, and doesn't hurt your credit score.
- Lift it briefly, for free, the few times a year you apply for credit.

**GOOD TO KNOW**

My guide on freezing your credit at all three bureaus walks through it step by step. For a breach involving a Social Security number or financial details, it's the most valuable thing you can do.

## 11. Free credit monitoring offers

*Companies often offer it after a breach — usually worth taking.*

After a breach, the company responsible often offers affected customers free credit monitoring for a stretch of time. This service watches your credit file and alerts you to new activity, like a new account being opened. It's generally worth accepting, because it's free and it's an extra set of eyes — but understand what it does and doesn't do.

Monitoring is reactive: it tells you after something happens. A credit freeze is preventive: it helps stop the thing from happening at all. So take the free monitoring if offered, but don't let it replace a freeze if sensitive data was exposed. The two work well together — the freeze blocks, the monitoring watches.

- Free monitoring after a breach is usually worth accepting.
- Enroll through the company directly, not through a link in a suspicious message.
- Monitoring alerts you after the fact; a freeze helps prevent it — use both.
- When the free period ends, you're not obliged to start paying for it.

**WATCH OUT**

Sign up for the offered monitoring by going to the company's official site yourself. Scammers send fake 'claim your free monitoring' messages after well-known breaches to harvest your details. Verify before you enroll.

## 12. What kind of data leaked matters

*The right response depends on what was exposed.*

Not all breaches are equal, and matching your response to what actually leaked saves you from both under- and over-reacting. The notice usually spells out what information was involved. Here's how to read it.

- Email address only — low risk. Be alert for more phishing, but little to do.
- Password — change it, and change it anywhere you reused it.
- Credit-card number — watch statements; your bank may reissue the card.

- Social Security number or birth date — consider a credit freeze; this is the serious tier.
- Full identity details together — treat as possible identity theft (next chapters).

The pattern is that the more permanent and personal the exposed information, the stronger your response should be. A password can be changed in a minute; a Social Security number can't be changed at all, which is exactly why a freeze matters when one is exposed.

#### GOOD TO KNOW

If the notice is vague about what leaked, treat it on the cautious side and go to the company to ask. It's reasonable to want a plain answer about what of yours was involved.

## 13. When it crosses into identity theft

*The signs that this is more than a password change.*

Sometimes a breach is the prelude to actual identity theft — someone using your information to impersonate you. It helps to know the signs, so you can escalate from 'tidy up a password' to 'treat this as theft' at the right moment. None of these means panic, but each means it's time for the fuller response.

- A bill or account statement arrives for something you never opened.
- You're denied credit for a reason you don't recognize.
- The bureaus or your bank flag activity you didn't do.
- You can't log into an account because someone changed the password.
- The IRS says a tax return was already filed in your name.

Any one of these suggests your stolen information is being actively used, not just exposed. That's the point to move to the dedicated recovery path, which exists precisely for this and makes it far less overwhelming than facing it alone.

#### WATCH OUT

In the stressful aftermath of a breach, scammers may call pretending to be your bank's 'fraud department' offering to help. Hang up and call the number on the back of your card yourself. Real help never needs your password or a gift card.

## 14. identitytheft.gov: the one place to start

*A free, official site that builds your recovery plan.*

If you believe your identity has actually been stolen, there is one best starting point: identitytheft.gov. It's run by the Federal Trade Commission, it's completely free, and instead of leaving you to figure out the steps alone, it asks what happened and generates a personalized, step-by-step recovery plan — including the letters and forms you'll need.

- 1 Type identitytheft.gov into your browser yourself.
- 2 Answer its questions about what happened to you.
- 3 Follow the personalized recovery plan it builds for you.
- 4 Use the pre-filled letters and checklists it provides.

This single site replaces a confusing scramble of phone calls with an orderly plan. It walks you through contacting the bureaus, placing fraud alerts or freezes, disputing fraudulent accounts, and keeping records. For something that feels overwhelming, it's a remarkably calm, capable guide.

### GOOD TO KNOW

identitytheft.gov is the official government site — reach it by typing the address yourself. Beware of imitators with similar names that charge for what this site does for free.

## 15. Freezing and fraud alerts for theft

*Two free tools that stop misuse of your credit.*

When identity theft is involved, your credit file is the battleground, and you have two free tools to defend it. A credit freeze locks the file so no new accounts can be opened. A fraud alert is a lighter flag that asks lenders to verify it's really you first. Victims are entitled to both for free, and to an extended, longer-lasting fraud alert.

- A freeze is the stronger tool — it blocks new credit entirely until you lift it.
- A fraud alert is lighter — credit can still be opened, but lenders must verify you.
- Victims are entitled to a free extended fraud alert lasting several years.
- You can have a freeze and an alert at the same time.

For most people facing theft, the freeze does the heavy lifting and the fraud alert is a useful companion. identitytheft.gov will fold both into your recovery plan at the right moment, so you don't have to decide in the abstract.

**GOOD TO KNOW**

My guide on freezing your credit at all three bureaus covers the freeze in full detail, including how to lift it briefly when you need to apply for credit yourself.

## 16. Don't let the notice rush you

*Urgency is the scammer's tool — and your own panic's.*

The single most protective habit across this whole subject is refusing to be rushed. Both the fake notices and your own understandable alarm push toward hasty action — clicking the link, calling the number, handing over a password to 'fix it fast.' Slowing down by even a minute is often all it takes to see a scam for what it is.

A real breach gives you time. Nothing genuine requires you to act within the hour. The company's advice will still be valid tomorrow, and your careful response — going to the site yourself, changing the password calmly — loses nothing by being unhurried. Speed helps only the scammer.

**WATCH OUT**

Any message about a breach that creates urgency — 'act within 24 hours,' 'your account will be closed' — should raise your guard, not your pulse. Real notices inform; they don't threaten. Slow down and verify on your own.

When something feels pressured, that pressure is the signal to stop. Ask someone you trust, or give me a call. Checking before you act is always free, and it's never the wrong choice.

## 17. After a well-known breach in the news

*When a big breach is reported, here's the measured response.*

Sometimes you'll hear about a large breach on the news rather than from a letter — a major company whose systems were broken into, affecting many customers. If you're one of their customers, the response is the same calm routine, with one extra note: the company will usually set up an official page explaining what happened and what to do.

- Go to the company's official site yourself to read their guidance.
- Change your password there, and anywhere you reused it.
- Check whether your information was involved using any tool they provide.

- If they offer free monitoring, enroll through their official site.

A well-known breach is also prime time for scammers, who flood inboxes with fake 'were you affected?' messages riding on the real news. So the caution is doubled: get your information only from the company directly or from trustworthy news, never from a message that arrives in the wake of the headlines.

#### WATCH OUT

The bigger and more newsworthy a breach, the more fake messages will reference it. Treat any email or text about a famous breach as suspect, and go to the source yourself.

## 18. Checking what else may have leaked

*A breach notice is a good moment for a wider look.*

A breach notice is a natural prompt to check your broader exposure, not just the one account. You can run your email address through a free, trusted site called Have I Been Pwned to see which known breaches it has appeared in, and let your phone's or password manager's built-in checkup flag any passwords that are weak, reused, or already leaked.

This turns an unwelcome notice into a useful nudge: a quick audit of your passwords while the subject is on your mind. Fix anything flagged, starting with your most important accounts, and you come out the other side more secure than before the notice arrived.

- Type haveibeenpwned.com yourself and check your email addresses.
- Open your phone's or manager's password checkup and read the flags.
- Fix anything compromised or reused, email and bank first.

#### GOOD TO KNOW

My guide on checking whether your passwords have leaked covers these tools in full — where to find them, what the warnings mean, and how to act on each.

## 19. Why unique passwords soften every breach

*The habit that keeps one breach from becoming many.*

Step back and a pattern emerges from all these steps. The reason a breach is frightening is the fear that the exposed password opens other doors too. Remove that fear — by giving every account its own unique password — and a breach shrinks to a single contained event: you change that one password, and nothing else is touched.

That's the quiet goal behind the whole response. A password manager that creates a different strong password for every account means future breach notices become minor errands rather than scares. You'll still change the breached password, but it can never cascade, because it was never shared.

- Unique passwords keep one breach from spreading to your other accounts.
- A manager makes unique passwords effortless — it remembers them for you.
- This single habit defuses most of what makes a breach dangerous.

**TIP**

My guides on your first password manager and on strong passwords you can actually remember show you how to get to one-unique-password-per-account without it feeling like a chore.

## 20. Helping a spouse or parent respond

*A calm task to walk through together.*

If you help a spouse or an aging parent manage their accounts, a breach notice is a moment they may find especially alarming, and your steady presence makes all the difference. Sit down together, confirm the notice is real, and work through the same calm routine side by side.

- First, confirm the notice is genuine by going to the company directly.
- Change the breached password and any reuse of it, together.
- Turn on two-factor for their important accounts.
- Set up free statement alerts so misuse is caught early.
- If sensitive data leaked, help them freeze their credit.

Doing it together also teaches them what a real response looks like, which makes them far less likely to be rushed by a fake notice later. Knowing the calm routine is itself a defense against the panic the scammers rely on.

**GOOD TO KNOW**

Seniors are heavily targeted for identity theft, so helping a parent respond well — and freeze their credit as a precaution — is one of the kindest protections you can set up for them.

## 21. What a breach does not mean

*Clearing up the worst-case fears.*

A lot of the distress around a breach comes from imagining it's worse than it is. So let's name what a breach notice does not mean, to put the real risk in proportion. Most breaches are exposures that a calm response handles well before any harm is done.

- It does not mean your own computer or phone was hacked — the company was breached.
- It does not mean money has already been taken from you.
- It does not mean your identity is stolen — that's a separate, less common step.
- It does not mean you did anything wrong.
- It does not require you to pay anyone to 'fix' it.

What it does mean is simple: information was exposed, and you should take a few sensible steps. Held in that light, a breach notice is a manageable chore, not a catastrophe. The steps in this guide are the whole of what's usually needed.

### WATCH OUT

Anyone who contacts you demanding payment to 'remove your data from the breach' or 'secure your account for a fee' is running a scam. Legitimate protections after a breach — changing passwords, freezing credit — are free.

## 22. Keeping records, just in case

*A little paperwork pays off if things escalate.*

For a serious breach — especially one involving sensitive data or any sign of misuse — it's worth keeping simple records of what you did and when. If the situation ever escalates to identity theft, having a tidy trail makes recovery faster and your case stronger. It needn't be fancy; a single sheet or note is plenty.

- Keep the original breach notice.
- Note the date you changed passwords and turned on two-factor.
- Save any confirmation of a credit freeze or fraud alert.
- Record any odd charges and your report of them to the bank.

Most of the time you'll never need these notes, and that's fine. But if a breach turns into something larger, you'll be glad to have a clear record rather than relying on memory. It's the same logic as keeping receipts for a warranty you hope never to use.

**GOOD TO KNOW**

If you report identity theft at [identitytheft.gov](https://www.identitytheft.gov), it helps you keep exactly these kinds of records as part of the recovery plan it builds, so you're not organizing it all from scratch.

## 23. A gentle version for the computer-shy

*The response is still for you — here's the unhurried path.*

If you don't spend much time on a computer, a breach notice can feel doubly frightening — scary in itself and daunting to respond to. It's more approachable than it looks, and you have options that don't require you to become an expert. The protection is just as real however you get there.

You can call the company by phone instead of using the website, and a person can help you change your password and set things right. You can ask a trusted family member, or me, to sit with you and walk through the steps the first time. And you can take it one step at a time — there's no need to do everything at once.

- Call the company's official number for help changing your password.
- Ask a trusted helper, or me, to go through the steps with you.
- Do the most important step — changing the password — first, and the rest after.

**TIP**

Responding to a breach is exactly the kind of thing I help folks with all the time, in person or over a screen-share. If a notice has you worried, a short call is often all it takes to sort it out calmly.

## 24. Breaches at your bank or card issuer

*When it's a financial company, a few extras apply.*

A breach at a bank, credit union, or card issuer deserves the same calm routine plus a little extra attention, because these companies hold money and financial details directly. The good news is that banks and card issuers are well practiced at this and have strong protections for you, including the right to dispute fraudulent charges.

- 1 Change your online banking password and turn on two-factor.
- 2 Turn on transaction alerts so you see every charge as it posts.
- 3 Watch for any charge you don't recognize and report it promptly.
- 4 Ask the bank whether they recommend reissuing your card or account number.

If fraudulent charges appear, report them quickly. By law and by policy, card issuers generally remove fraudulent charges and send you a new card, and banks have protections for unauthorized transfers. Acting promptly is the main thing that keeps you fully covered.

**WATCH OUT**

After a bank breach, expect a wave of scam calls and texts pretending to be 'your bank's fraud team.' Your real bank won't ask for your password, a code, or a transfer to a 'safe account.' Hang up and call the number on your card.

## 25. Breaches at email or tech accounts

*The master-key accounts need the firmest response.*

A breach involving your email, Apple, Google, or Microsoft account is more serious than most, because these are the master keys to much of your digital life. Your email in particular can reset the passwords of nearly everything else, so if one of these is involved, give it the firmest, fastest response.

- Change the password at once, to something long and entirely new.
- Turn on two-factor sign-in immediately if it isn't already.
- Review the account's security settings for anything you didn't set.
- Check that recovery email and phone numbers are still yours.
- Sign out of all devices if the account offers that option.

These accounts usually have a security page showing sign-in activity and the devices that are signed in. Look it over for anything unfamiliar. If you see a strange device or location, signing out everywhere and changing the password cuts off an intruder cleanly.

**GOOD TO KNOW**

My guide on locking down your email as the master key, and my guides on securing your Google, Apple, and Microsoft accounts, go step by step through exactly these settings.

## 26. Watch for follow-on scams

*A breach often draws a second wave aimed at you directly.*

Here's a pattern worth knowing: a breach is often just the opening act. Once criminals have your email address and a sense of which companies you use, they follow up with targeted scams aimed squarely at you. These can feel convincing precisely because they reference the real breach and the real company, so your guard deserves to stay up for a good while afterward.

- Emails or calls 'about the breach' asking you to verify or pay something.
- Fake 'account recovery' or 'claim your settlement' messages.
- Callers who already know a detail about you, using it to sound legitimate.
- Messages urging you to move money to a 'safe account' for protection.

The defense is the same steady rule throughout this guide: don't act on incoming messages, go to companies yourself, and never let someone who contacted you walk you into a password, a code, or a payment. The fact that a caller knows your name or a recent purchase proves nothing — that's exactly what the breach leaked.

### TIP

A caller or message that knows real details about you is not therefore trustworthy — a breach is how they got those details. Legitimacy is about how you reached them, not how much they seem to know.

## 27. Staying calm the next time, too

*Once you know the routine, every future notice is easier.*

Here's a comforting truth: the first breach notice is the hardest, and every one after is easier. Once you've been through the routine — verify, change, protect, watch — it becomes a familiar checklist rather than a fright. Breaches are a fact of modern life, and the people who handle them best aren't the ones they never happen to; they're the ones who know the steps.

So the real goal of this guide isn't just this one notice — it's giving you a routine you carry forward. Keep the cheat sheet handy, remember that a notice is a to-do list and not a disaster, and each future breach becomes a few calm minutes rather than a sleepless night.

- The steps are the same every time — verify, change, protect, watch.

- Unique passwords and two-factor shrink every future breach in advance.
- Knowing the routine is itself what keeps panic — and scammers — at bay.

**TIP**

Pin the cheat sheet from this guide near your computer. When the next notice arrives, you'll have the whole calm routine in front of you, and it'll be a short errand rather than a scare.

## 28. Putting it all together

*The whole plan in one easy breath.*

Let's bring it home. When a company you use is breached, the response is a short, calm routine: first make sure the notice is real by going to the company yourself, then change that password, fix any reuse, turn on two-factor, and watch your statements. If sensitive data leaked, freeze your credit. If it becomes theft, start at [identitytheft.gov](https://www.identitytheft.gov).

- 1 Confirm the notice is genuine — never act through a link in the message.
- 2 Change the breached password, and change it anywhere you reused it.
- 3 Turn on two-factor sign-in for the account.
- 4 Watch your bank and card statements, and turn on free alerts.
- 5 Freeze your credit if a Social Security number or financial details leaked.
- 6 If your identity is being misused, go to [identitytheft.gov](https://www.identitytheft.gov).

That's the whole of it. A breach notice is unwelcome, but it isn't a catastrophe — it's a to-do list, handled in order, usually in well under an hour. Done calmly, you come out the other side more secure than you were before it arrived.

**GOOD TO KNOW**

If any single step here feels like one too many, you don't have to do it alone. Walking through exactly this, at your kitchen table or over a screen-share, is one of the most common things I help folks with.

**CHEAT SHEET**

## Your Breach-Response Cheat Sheet

Keep this page by the computer. It's the short version of what to check, what to do, and in what order, the day a breach notice arrives.

### First, is the notice even real?

- Don't click links in the message. Go to the company by typing its address yourself.

- A real notice informs and advises; a fake one pressures and rushes.
- No real company asks you to confirm your password in a breach email.
- Unsure? Call the company using the number on your card or official site.

### The calm response, in order

- 1 Change the password for that account.
- 2 Change it anywhere else you used the same password.
- 3 Turn on two-factor sign-in for the account.
- 4 Watch your bank and card statements for anything odd.
- 5 Consider a credit freeze if sensitive data was exposed.

### If it looks like identity theft

- Go to [identitytheft.gov](https://www.identitytheft.gov) — the FTC's free, official recovery site.
- Freeze your credit at all three bureaus.
- Watch statements and report anything you don't recognize.

### Keep in mind

- Free credit monitoring offered after a breach is usually worth accepting.
- A breach is common and rarely your fault — a calm response handles it.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

### WORDS TO KNOW

## Plain-English Word List

**Data breach** — When a company's systems are broken into and the information it held about customers is stolen or exposed.

**Breach notice** — The letter or email a company sends to tell you your information may have been exposed, often required by law.

**Phishing** — A fake message designed to look official, meant to trick you into giving up a password or personal details, often by clicking a link.

**Credit freeze** — A free, legally protected lock on your credit file that stops anyone from opening new accounts in your name.

**Credit monitoring** — A service that watches your credit file and alerts you to new activity. Often offered free for a time after a breach.

**Identity theft** — When someone uses your stolen information to impersonate you — opening accounts, filing taxes, or making charges in your name.

**identitytheft.gov** — The U.S. government's free, official site that walks identity-theft victims through a step-by-step recovery plan.

**Two-factor (2FA)** — A second step at sign-in beyond your password, so a leaked password alone can't get anyone into your account.

**Reused password** — The same password used on more than one account. One breach then puts every account sharing it at risk.

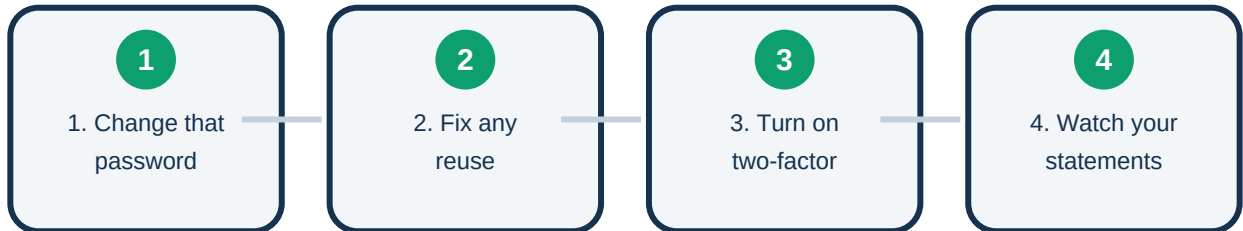
**Fraud alert** — A free flag on your credit file asking lenders to verify it's really you before opening new credit.

## AT A GLANCE

## A Picture to Follow Along

## The Calm Steps After a Breach Notice

A handful of minutes, in order, closes the risk.



**You're acting, not reacting - that's what keeps you safe.**

Illustration - a breach notice is a to-do list, done in order.

## AT A GLANCE

## A Second Look

## Real Notice vs. Phishing Pretending to Be One

Scammers mimic breach notices. The tells are consistent.

| A real notice                                                                                   | A phishing fake                                                                                  |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Explains what leaked<br>Says change your password<br>No link needed to act<br>No urgent threats | Vague but alarming<br>'Click here to secure'<br>Rushes you with a link<br>Asks for your password |

**When in doubt, go to the site yourself - never through the message.**

Illustration - a real notice informs; a fake one pressures.

## BEFORE YOU GO

## A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.



## HOW I CAN HELP

# Your Visit — and My Promise

**In-home visit — \$99 flat** for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

**Remote Support — \$49** for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

### GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full \$99. No questions, no awkwardness. That's how I'd want to be treated.

Call or text **(330) 200-8042** · Book a visit: **billshometech.com/book** · **bill@billshometech.com**

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.