



Data Breach First Aid

What to Do Before and After a Breach

It can feel like we hear about a new security incident every day. Banks, schools, government agencies, and even the retailer shipping your gourmet coffee may hold personal, financial, or login information that attackers want. A breach means information was exposed; it does not always mean identity theft has already happened.

Before a breach, limit your exposure. Think carefully about who receives your data and why. Skip accounts created only for a one-time discount. When you stop using an app or service, delete the account, not merely the app.

Protect every account. Use a long, unique password for each one, store passwords in a password manager, and turn on multifactor authentication for important accounts. Do not change passwords just because the calendar says so. Change them when they are exposed, reused, or compromised.^{1,2}

After a breach, verify what happened. Do not automatically trust links or phone numbers in a breach notice. Navigate independently to the organization's official website or use a number you already know is legitimate. Find out what was exposed, what help is available, and which recovery steps are recommended.³

Secure what was exposed. If payment information was involved, contact your bank or card issuer using a trusted number. They may recommend locking or replacing a card, closing an affected account, or changing login credentials. Keep reviewing transactions for activity you do not recognize.³

Preparing now lowers your risk. If a breach happens anyway, quick and deliberate action can keep exposed data from becoming a larger emergency.

Received a breach notice? Verify it independently before you click a link, call a number, or sign in.

First-aid principle: A breach means information was exposed. It does not always mean identity theft has happened.

Find out what was exposed, then match your response to the data at risk.



Who Needs to Know?

Who you contact depends on the information exposed and whether anyone has already misused it.

- 1 The breached organization:** Confirm what was exposed and what help is available.
- 2 Your bank or card issuer:** Act if payment or account information may be compromised.
- 3 Your employer or IT team:** Report work credentials, devices, email, or company data.
- 4 Friends and family:** Warn them if an account takeover could enable impersonation.
- 5 Credit bureaus or identity-theft authorities:** Contact them if sensitive identity data was exposed or misused.

THREE FAST MOVES

VERIFY

SECURE

MONITOR

Card Lock or Credit Freeze?

Card lock or replacement: helps stop new purchases on one specific card. Contact the bank or card issuer if payment information was exposed.

Credit freeze: restricts access to your credit reports, making it harder to open new accounts in your name. In the U.S., contact Equifax, Experian, and TransUnion separately. It is free, remains until you lift it, and does not block existing-account activity.

If both card data and identity information were exposed, you may need both.⁴



LOCK OR FREEZE?

MATCH THE TOOL TO THE RISK