DIGITALLYUNDRESSED

FREETOOLKIT

Data Breach Response Kit

What to do in the first 24 hours when your data appears in a breach

Estimated time: 20 minutes

From the book Why Am I the Only One Naked?

thedreamerai.com/digitally-undressed

Share this guide freely. Privacy is not a privilege.

Why This Matters Right Now

In March 2026 alone: ShinyHunters breached approximately 100 companies through Salesforce misconfigurations. Conduent exposed 25 million people. TriZetto leaked 3.4 million health records. LexisNexis - a data broker that holds information on hundreds of millions of people - confirmed their own servers were compromised.

11 breaches are publicly disclosed every day. The average breach takes 241 days to detect. By the time you receive a notification letter, your data may have been circulating on the dark web for months. This guide tells you exactly what to do.

> **CRITICAL**
> You cannot delete your Social Security number. You cannot change your date of birth. You cannot rotate your medical history. When permanent identifiers are breached, the damage is lifelong. Speed matters.

[Step 1] Confirm the Breach Is Real

Check HaveIBeenPwned.com: Enter your email address. This free service (run by security researcher Troy Hunt) cross-references your email against every known public breach. It will tell you which breaches included your data and what was exposed.

Verify the notification: If you received a breach letter, confirm it is from the actual company - not a phishing attempt. Go to the company's website directly (do not click links in the email) and check their security notices page.

Check the scope: Was it just email addresses? Or was it SSN, financial data, medical records? The response changes based on what was exposed.

[Step 2] Immediate Actions (First Hour)

Change the password on the breached account immediately. Then change it on any other account where you used the same password. Yes, every single one.

Enable two-factor authentication on the breached account and on your email account. Your email is the skeleton key - if attackers get in there, they can reset every other password you have.

Check for unauthorized activity: Log into the breached account and review recent activity, login history, connected devices, and any changes to account settings (email, phone number, recovery options).

IMPORTANT

Attackers try stolen credentials on other sites within hours of a breach. This is called credential stuffing. If you reuse passwords, assume every account with that password is compromised.

[Step 3] If Financial Data Was Exposed

Freeze your credit at all three bureaus. This is free and prevents anyone from opening new accounts in your name. Equifax: equifax.com/personal/credit-report-services. Experian: experian.com/freeze. TransUnion: transunion.com/credit-freeze.

Set up fraud alerts: Contact one bureau and they notify the other two. A fraud alert requires creditors to verify your identity before issuing new credit.

Monitor bank statements weekly for the next 90 days. Set up transaction alerts for any charge over $1.

[Step 4] If Medical Data Was Exposed

Request your medical records from your providers and review them for entries you do not recognize. Medical identity theft can result in incorrect information in your health records - which can affect treatment decisions.

Contact your health insurer and request an Explanation of Benefits (EOB) for the past 12 months. Look for claims you did not file.

[Step 5] If SSN Was Exposed

File an Identity Theft Report at IdentityTheft.gov (FTC). This creates a formal record you can use with creditors, banks, and law enforcement.

Request an IRS Identity Protection PIN at irs.gov/ippin. This prevents someone from filing a tax return in your name.

Consider identity monitoring services. Many breach notifications offer free monitoring. Accept it - it is the bare minimum the company owes you.

> **PRO TIP**
> If the breached company offers free credit monitoring, take it. But understand that monitoring only tells you AFTER someone uses your data. A credit freeze PREVENTS them from using it. Do both.

[Step 6] Long-Term Protection

Switch to a password manager (Bitwarden or 1Password). Generate unique passwords for every account. Never reuse a password again.

Set a quarterly reminder to check HaveIBeenPwned, review your credit report (annualcreditreport.com), and audit your account permissions.

Reduce your surface area. Delete accounts you no longer use. Every dormant account is a breach waiting to happen with data you forgot you shared.
