Another Data Breach?  
Don't Get Data Breach Fatigue.

Spend a moment thinking about how many entities have your personal identifying information. You likely provided it to them for a legitimate need, like a loan or credit card application or a medical claim. These organizations have data on millions of individuals, and we trust them to maintain the security needed to protect it for us. If you add to the list of companies those that only have your name, email and home address, and credit card information, that’s essentially every website from which you’ve ever made an online purchase. 

The list just got a lot longer, and the security of small retail websites is typically more lax than that of large medical or financial ones. Hackers spend their lives searching for a way in, using sophisticated techniques to get through cyber security measures and steal valuable information from entities of all types.

Now, think about the last time you received an email that started something like this: “We are writing to you because of an incident involving access to information…” It probably wasn’t very long ago. We might even receive so many notifications or hear so many news reports regarding breaches that could affect us that we’re becoming apathetic.

“It’s just part of life now,” we might say. Or “It’s a risk of being online in 2023.” However, we can do more than cross our fingers and hope ours isn’t the next information that gets sold to the highest bidder. 

A quick web search for “data breach” reveals countless recent hits detailing major data breaches. In fact, during June 2023,[the Oregon DMV experienced a data breach](https://www.oregon.gov/odot/dmv/pages/data_breach.aspx#:~:text=This%20data%20contains%20personal%20information,about%20the%20MOVEit%20Transfer%20breach.) and the information of more than 3.5 million Oregonians was compromised. You might have even been affected by a data breach or received a notification from a retailer or other organization that your personal information could have been compromised. What did you do next? Did you feel helpless, or did you know how to safeguard your data after the fact? 

[The National Association of Attorneys General](https://www.naag.org/issues/consumer-protection/consumer-protection-101/privacy/data-breaches/) defines a data breach as the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

What is considered personal information depends on state law but typically includes an individual’s first name (or initial) and last name plus one or more of the following:

* Social Security number
* Driver’s license number or state-issued ID card number
* Account number, credit or debit card number, combined with any security code, access code, PIN, or password needed to access an account

One of the biggest risks following a data breach is that scammers could use your stolen personal information to open a loan or a line of credit in your name, potentially damaging your credit score or leaving you to pay for the fraudulent charges.

[This article from IBM](https://www.ibm.com/reports/data-breach?mhsrc=ibmsearch_a&mhq=data%20breach%202022) summarizes data breach research from 2022, stating that the average data breach cost the affected U.S. company $9.44 million last year. While losses to companies are huge, potential losses to individuals are not to be ignored. When a data breach leads to identity theft, the cost can be staggering. Therefore, it is important that you know what to do *when (not if)* you receive a data breach notification and also that you take steps to help protect yourself as much as possible in the future.

Immediately after receiving a data breach notification in your inbox or hearing about a retailer breach that might affect you, it’s important that you act quickly to take a few precautionary steps.

1. **Change your passwords right away.**Even if the company has not stated that passwords were affected, immediately change not only your password for the involved company but for any other businesses where you’ve used a similar password (we’ve all done it). Look into using a password manager that will help you create unique passwords—and you won’t have to memorize them.
2. **Identify any compromised information.**Look further into what information was exposed so that you can take the appropriate action.[IdentityTheft.gov/databreach](https://www.identitytheft.gov/#/Info-Lost-or-Stolen) has information on what to do to help protect yourself in each case.
3. [**Report the data breach**](https://www.identitytheft.gov/#/assistant) to the Federal Trade Commission.

To help protect yourself in the case of future data breaches, the following actions can help you save time and money for the inevitable next time:

1. **Don’t reuse passwords.**  
   Even if the data breach notification you receive is for an account you don’t use anymore, so it doesn’t have your current credit card information, you might have used a password that you’re still using on other sites. Hackers know there’s a good chance you’re using the same password on multiple platforms. If they access your old gaming password from college, they might also be able to use it to log in to your current financial accounts.
2. **Turn on**[**multi-factor authentication (MFA)**](https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA)**whenever it is available.**  
   Accounts that offer MFA provide extra security by requiring additional forms of identification beyond a password to log in to an account, such as a passcode or secret key obtained via text or email. This will help keep your account secure even if your password is compromised.
3. **Keep a close eye on your credit report.**It can often take months for a company to find out that their customers’ data has been stolen and then communicate the information to their users. By then, your personal information could have already been sold on the dark web and used to open lines of credit before you have even been notified of the risk. Federal law entitles you to a free copy of your own credit report at least once every 12 months from each of the three main consumer credit reporting agencies: Equifax, TransUnion, and Experian. Reports can be requested at[annualcreditreport.com](http://annualcreditreport.com/) or by calling 1-877-322-8228.
4. **Consider placing a fraud alert.**If you’ve been impacted by a data breach, you may also consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. Additional information is available at [http://www.annualcreditreport.com](http://www.annualcreditreport.com/).

Next time you receive a notification about a possible data breach, follow the steps above, both to put a stop to harm that may have already begun and to make it much more difficult for them to impact you in the future.