Malwarebytes

Your data breach checklist

It seems every few months we're reading about another big company getting hit with a data breach. Customers' credit card info, logins, and passwords are stolen—but it's mostly the company's pain that makes the headlines. So after the dust has settled and the news cycle moves onto the next breaking story, you the consumer are left wondering, "Okay, what can I do to protect myself?"

Here's your data breach toolkit, courtesy of your friends at Malwarebytes, with steps you can take to clean up and stay safe when the next data breach happens.

1. Reset your password now.

Change your password for any compromised accounts. Go ahead and do it now, we'll wait here for you. Now that that's out of the way, you should consider enabling **multi-factor authentication**. With multi-factor authentication in place, even if cybercriminals steal your login credentials, they still won't be able to access your account without at least one other authentication mechanism, like your phone for example.

2. Monitor your credit accounts.

Look for any suspicious activity. Remember you get a free credit report, one from each of the three major credit bureaus, every year at **annualcreditreport.com**. This is the only U.S. Federal Trade Commission-authorized site for obtaining free credit reports.

3. Consider freezing your credit.

A credit freeze makes it harder to open up a line of credit under your name by restricting access to your credit report. You can lift or stop the freeze at any time. The only hassle is that you must contact each credit bureau individually to enact or remove a freeze.

4. Watch your inbox carefully.

Opportunistic cybercriminals know that millions of victims of any given data breach are expecting some kind of communication regarding hacked accounts. These scammers will take the opportunity to send out phishing emails spoofed to look like they're coming from those hacked accounts in an attempt to get you to give up personal information. Read our tips on **how to spot a phishing email.**

* Bonus tip: credit monitoring services.

Should you sign up? Often times, after a data breach, affected companies and organizations will offer victims free identity theft monitoring services. It's worth noting, services like LifeLock, et al. will notify you if someone opens up a line of credit in your name, but they can't protect your data from being stolen in the first place. Bottom line—if the service is free, go ahead and sign up. Otherwise, think twice.

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. **Learn more at www.malwarebytes.com.**