BLACKCLOAK™

What to Do When You Are Impacted By a Data Breach

Data breaches can cause a great deal of headaches for victims, and even though the aftermath of a breach may seem stressful, it doesn't mean all hope is lost. There are steps you can take to minimize the risk you face following an incident. This guide will explain what you should do if your information is compromised in a breach.

First Steps

Find Out What Information Was Affected:

When a data breach is disclosed, the affected entity will likely inform victims what data points were compromised in the breach. By knowing what information was caught up in the incident, you'll know the next steps you'll have to take.

Don't Waste Time:

Once you know what data points have been exposed, you'll want to move as soon as possible, to protect yourself. Cybercriminals may try and use the data they've stolen as soon as possible.

Now, let's cover what you should do when certain pieces of data are compromised in a data breach:

Passwords:

When your password is exposed in a data breach, you should change it as soon as possible. Make sure the password is unique and is not easy to guess. Consider using a passphrase that contains an appropriate amount of symbols and letters. If you have used the compromised password for other accounts, be sure to change all of them as soon as possible. To learn more, watch our webinar on password management best practices.

Social Security Numbers:

In the event your Social Security number is compromised, make sure to contact the Social Security Administration and report instances of identity theft and fraud to the FTC and SSA Office of the Inspector General respectively. Be sure to also place a credit freeze and fraud alert with the major credit reporting agencies, Experian, Equifax and TransUnion. To learn how to do these tasks, read our client guides on SSN compromise and what to do if you are a victim of identity theft.

Payment Card Information:

Cancel any cards that may have been compromised in a breach. To limit future risk, consider paying with a virtual payment card when making any purchases online.

Here are some additional steps you should take when you are a victim of a data breach:

Contact Law Enforcement and Report the Crime:

Report the crime to local law enforcement and any relevant federal agency if you fall victim to a data breach.

Record Details of the Incident:

Before reporting the crime, make sure you record as many details about the breach as possible, including what information was stolen, when it was stolen and from where. This can potentially help law enforcement track down any fraudulent activity you may see.

Enroll in Credit Monitoring and Watch Accounts for Fraudulent Activity:

Make sure you enroll in any credit monitoring services, especially if they are offered to you free of charge. In addition to placing credit freezes and fraud alerts on your accounts, keep an eye out for any suspicious activity and report anything out of the ordinary when you spot it.

Enable Dual Factor Authentication:

Set up dual factor authentication on your accounts whenever you can. This will make it harder for cybercriminals to access your account should they obtain your password.

Of course, it's important to remember you can't count on the aftermath of a data breach to simply disappear. Stolen data may not always be used or sold right away. You may have to continue using these precautionary measures for extended periods of time to minimize your overall risk.