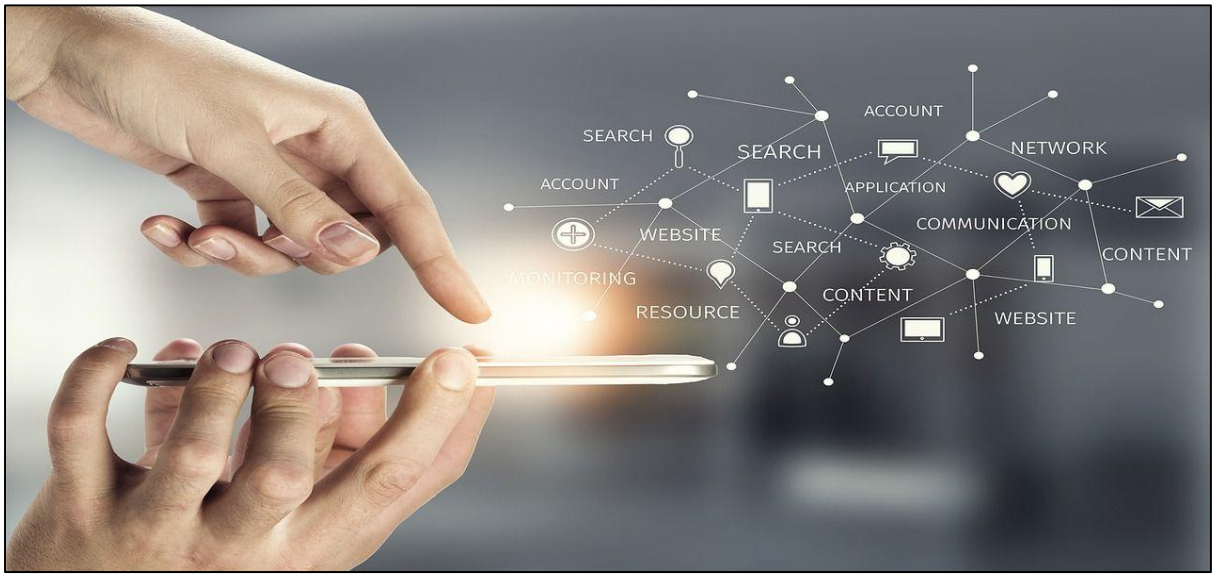
What is a Data Breach? Tips for Data Breach victims

A data breach occurs when someone gains unauthorized access to a computer system's sensitive, protected, confidential information, and the data has been viewed, stolen, or used illegally. Data breaches can happen anywhere, and it's important to know what to do if you are affected by a data breach.



Definitions of Breach Terms

Before we continue discussing data breaches, we need to understand the different types of breaches and the various ways that these breaches can occur. Data breaches can be broken down into 5 categories:

1. **Business:** a breach that occurs within a business or organization (ex: grocery stores, retailers, etc.)
2. **Financial**: a breach that occurs within a financial corporation (ex: banks, credit card companies, etc.)
3. **Educational:** a breach that occurs within an educational institution (ex: universities, high schools, etc.)
4. **Government/military:** a breach that occurs within a government or military-based facility (ex: police departments, military bases, etc.)
5. **Medical/health care:** a breach that occurs within a medical institution or health care company (hospitals, pharmacies, etc.)

How do Data Breaches happen?

Data breaches can occur in various types of institutions in several ways:

- **Insider theft:** exposure of information because of theft orchestrated by an individual within the institution, such as an employee or staff member (either former or current)
- **Hacking:** exposure of information because of a targeted attack executed through unauthorized access of a computer or network

- **Data on the move:** exposure of information during transportation or movement of information and information containers (computers, folders, hard drives, etc.) from where they are normally kept
- **Third-party/subcontractor error:** unintended exposure of information because of a third party or subcontractor
- **Employee error:** unintended exposure of information because of an error made by an employee
- **Accidental internet exposure:** exposure of information because of unintended access to the Internet
- **Physical theft:** exposure of information due to physical theft of information and/or information containers (computers, folders, hard drives, etc.)

While some breaches are purely accidental, it doesn't change the fact that your information could be at risk after a breach. Let's take a closer look at four of the most common ways that data breaches occur:

Employee Error

Breaches can be accidents. In the case of employee error, the data breach may not have any specific motivation but occurs when an employee is tricked into unknowingly allowing access to a company's secured data through phishing emails or deceptive websites. Employees may accidentally provide sensitive information about the company's data servers on a fraudulent website or download malware that intercepts data entered or stored on the computer.

Hacking

A company's data system is like a gold mine for hackers. Hackers find vulnerable areas of a specific computer system or network to gain access to its information. Personally identifiable information (PII) can be more valuable than money and can be sold on the black market for a high price. Hackers can also use your PII to create credit card accounts, apply for jobs and receive tax refunds. Learn more about identity theft and identity fraud.

Third-Party Errors

Sometimes a breach can occur due to an error of a company's supplier, again purely accidental, when sensitive data is inappropriately processed or shipped. This can result in the exposure of this information to unauthorized sources. Information can also be at risk when vendors do not properly delete user information.

Theft and Loss

Data breaches can also happen by merely leaving a phone on a table in a restaurant, or a thief breaking into a car and stealing a laptop. Exposure of confidential information can happen simply by theft and loss of PCs, tablets, laptops, USB storage devices, and smartphones that store sensitive information.

Can you prevent a Data Breach?

Unfortunately, there is no way that you or anyone else can prevent a data breach from happening. However, you can decrease the chance of your information being misused by knowing what to do if your data is involved in a data breach.

What should I do if a Data Breach happens?

Let's look at a few steps you should take if you think you've been affected by a data breach:

- **Stay updated.** It's important to know which company was affected, what type of information was compromised and how many people were affected and the time of the breach (if pertinent). Knowing this information can help determine whether your information is at risk.

- **Check for breach notifications.** Companies are required to notify consumers that could have been affected by a data breach in most states. Watch for letters, emails, or other types of notifications alerting you that your information may have been compromised.
- **Monitor your credit/debit cards closely.** If there is a chance that your credit or debit card information was stolen, keep an eye on your bank statements for unauthorized activity.
- **Communicate with your bank.** If you notice any unauthorized activity on your cards, call your bank to file a claim for fraud.
- **Consider Identity Theft Protection.** With Bitdefender Identity Theft Protection, you have access to a Certified Resolution Specialist that will help secure your information and work with you if your information becomes compromised by a data breach.

Tips for Data Breach Victims

You can take these steps to reduce further cyber fraud and best protect your identity when a data breach happens to a company that has your personal and financial information (PII).

R ACCESS

1. **Change Your Passwords on Other Accounts**. Change your exposed account credentials immediately and then update any other accounts that use the same or similar password. Moving forward, use unique passwords or passphrases for every account to avoid credential stuffing.
2. **Adopt Multi-factor Authentication (MFA)**. More secure than a password, multi-factor authentication requires at least two inputs to verify who is accessing an account — such as a one-time code sent via text message and your password. The extra step can prevent identity thieves from accessing your accounts when they only have a compromised password.
3. **Freeze Your Credit Report**. A credit freeze prevents unauthorized viewing of and access to your credit report by new creditors, background check companies, and potential thieves. Credit freezes must be set (and removed) at each of the three bureaus. Credit freezes are free in all 50 states.
4. **Secure Your Device**. Make sure you have enabled the lock screen of your mobile device with a PIN or biometric passcode. Turn on the “Find My” device feature, so you can disable the device or delete your information if it’s lost or stolen. Use Bitdefender’s Anti-Theft feature on Android smartphones & tablets to be prepared for data wipe if needed.
5. **Don’t Overshare**. Cybercriminals use personal information posted on social media to impersonate you when creating or accessing accounts. Make sure you only share personal details with people you trust.

SET UP ALERTS

6. **Set Up Credit Report Monitoring**. Credit monitoring services can spot the opening of potentially fraudulent new accounts or even misuse of your existing accounts. Many also have the advantage of sending you updates based on ongoing usage, rather than relying on you to check in with them or only allowing you to get an update once a year. There are many monitoring options — some free and some paid — and you should select the type of monitoring with which you are the most comfortable.
7. **Place Fraud Alerts on Your Credit Report**. A fraud alert advises those making an inquiry into your credit report to be more cautious when using it (both for existing and new account activity), typically requiring them to take additional steps to verify the applicant's identity.
8. **Protect Your Mobile Device**. Set up monitoring on your mobile devices to detect malware, spyware, and other exploitable weaknesses. Look for an identity theft protection plan with mobile cybersecurity, such as Bitdefender Ultimate Security and Bitdefender Ultimate Security Plus.
9. **Enable Multi-Account Activity Alerts**. Receiving mobile or other text alerts to detect possible fraudulent activity is even more important after a breach. Adjust these to strike the right balance of alert activity for your needs.
10. **Activate Alerts for Credit and Debit Card Accounts**. Notifications for suspicious transactions (e.g., unusual login attempts, contact information change) can quickly detect suspicious activity on your credit or debit card. Many banks support text messages, email, or in-app alerts.
11. **Set Alerts for or Lock Online Card Transactions**. Typically, card data stolen in an online merchant breach can only be used for fraudulent purchases online as well. Setting up alerts for online transactions can help quickly detect suspicious activity without creating unnecessary alerts for purchases at physical stores. By locking your card and only unlocking it when you make purchases, you limit the opportunities for anyone else to use your account.

BE ON THE LOOKOUT

12. **Scan Criminal Marketplaces**. Identify where your personal data is already available. It could be combined with your breached information to conduct fraud in your name. The Account Privacy feature in Bitdefender Mobile Security for iOS and Android as well as free services, including Firefox Monitor and Have I Been Pwned? can scan where personal data is available online.
13. **Monitor Your Social Media Accounts**. Imposter accounts and account takeovers through social media can lead to fraudsters scraping personal information, targeting you or your connections through social engineering, then buying and selling your personal information on the Dark Web.
14. **Beware of Social Engineering**. When your contact information is exposed (e.g., phone number, email, or street address), you're likely to be contacted by

criminals pretending to be a trusted authority to obtain even more private data to commit more targeted fraud.

15. **Monitor for Suspicious Email Account Activity**. If your email provider supports alerts, set up notifications for unusual login attempts, changes to contact information, or other suspicious activity so you can quickly detect fraud.
16. **Review Your Records with the Medical Insurance Bureau (MIB)**. Just like your credit reports, consumers are legally entitled to annual access to their records with the Medical Insurance Bureau (MIB). Your MIB consumer file can be requested digitally here.

MAKE CONTACT

17. **Order Free Copies of Your Credit Reports**. Regularly review your credit reports to identify inaccuracies and spot potentially fraudulent activity. The three nationwide credit reporting agencies — TransUnion, Equifax, and Experian — are required to provide you with access to your reports once a year. And now, each of the agencies is providing reports once per week.
18. **See If You Need a Replacement Card**. If they don't replace it automatically, contact your financial institution to see if you need a replacement card. Security features (e.g., alerts and card controls) may reduce your risk without the inconvenience of replacing the potentially compromised card.
19. **Activate USPS Informed Delivery**. The Informed Delivery service allows you to digitally view mail and packages that are set to be delivered to your address, so you know when to expect important mail (like replacement cards), reducing the risk of mail theft. Find out more at the post office's website.
20. **Notify the DMV of Your Stolen Driver's License**. Alert state agencies and law enforcement of the theft of your driver's license number or physical license so they're aware someone might impersonate you. Better yet, ask the DMV to change your driver's license number to protect you against impersonation.
21. **Contact the Social Security Administration**. Request your wage earnings report to verify that your Social Security number is not being used fraudulently, which could result in your owing taxes for wages earned by someone using your stolen information.