# What is data leakage?

What is data breach? The following article will explain in detail for you and give advice on how to protect yourself from attacks like this in the future.

If you follow confidential news, you might hear people talking about big companies leaking data. And you might be worried about how these data breaches could affect you, as a user.

So what is data breach? The following article will explain in detail for you and give advice on how to protect yourself from attacks like this in the future.

## Learn about data leaks and precautions

1. What are the differences between security incidents, security breaches and data leaks?
2. Examples of some famous data leaks
3. How did data leaks occur?
4. Who is affected by the data leak and what to do if the data is leaked?
5. How can you protect yourself from data leakage?

## What are the differences between security incidents, security breaches and data leaks?

The common term for a company or organization that has been hacked or digitally attacked is called a security incident. This includes a range of issues such as malware infection, phishing, distributed denial of service (DDoS) attacks, and lost or stolen employee equipment.

A security incident may or may not result in the security of an organization being compromised. If attackers succeed in breaching an organization's security, that is called a security breach.

Data leakage is a specific type of security breach. This is where attackers successfully access data without their permission. Usually, the attacker will successfully carry out a security breach, and then steal the data resulting in a data leak.

But there could be many other types of data leaks. For example, an organization may accidentally place sensitive data in an insecure location. If people can access data that should not have been allowed, it is a data leak.

## Examples of some famous data leaks

One of the biggest data breaches in recent years was revealed in 2018. Hackers attacked Facebook and stole the information of about 30 million users. Hackers have made an attack through the Facebook developer's API (Application Programming Interface) and can obtain user information such as name, gender and identity.

Another well-known data leak happened with Equifax in 2017. Equifax is a major credit reporting company and holds data on a large number of Americans. Hackers gained initial access to the company's system, through a consumer complaint portal, with a well-known vulnerability.

They then use the web portal to access other parts of the network. Hackers find usernames and passwords stored in plain text (which is a huge security error). They then used these passwords to steal data such as name, address, social security number and date of birth. In total, this leak is likely to affect 145 million people.

Credit card company and Capital One bank also leaked data in 2019. Hackers stole names, addresses, credit points and social security numbers of more than 100 million customers.

The company misconfigured a web application firewall and hackers could exploit this to gain access to the system. The hacker in this case is a software engineer, who previously worked for Capital One's web hosting company, Amazon Web Services.

## How did data leaks occur?

There are many ways data leaks can occur. According to the Kastle Systems report, the most common cause of data leakage is hacking, followed by poor security. Hackers have used malware in nearly 50% of data breaches. They used social engineering in about a quarter of these attacks.

Hackers can 'introduce' malware to the target computer through techniques such as email spam. The email will trick the user into clicking the link to download malicious software onto the device. Another way to hack a system is through social engineering attacks like phishing. This is where hackers set up a fake website and trick users into entering their username and password into the site.

Hackers can then copy those usernames and passwords, then use them to access security systems.

Sometimes, affected organizations make mistakes that lead to data leaks. For example, an employee could lose or steal a company's computer. If cyber criminals have that computer, they can use it to gain access to company systems.

Or, as seen in the case of Equifax, an organization may have poor security practices such as storing passwords in plain text. That makes it easier for hackers to steal data.

## Who is affected by the data leak and what to do if the data is leaked?

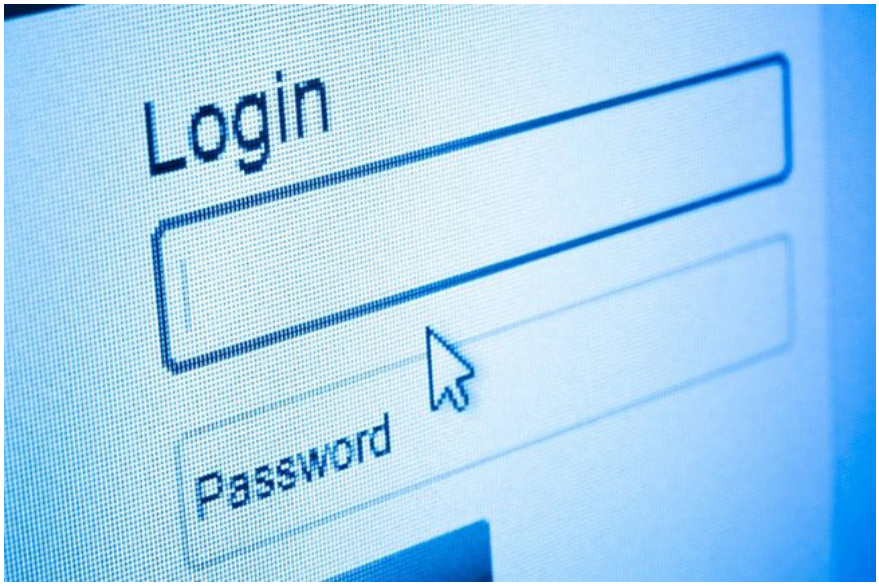
With so many companies leaking data, there's a good chance you could be affected as well. Therefore, a great resource to find out if your information is part of the leak is the **HaveIBeenPwned.com** website **.** You can enter your email address into this website to see if you are affected by the data leak.

If your information is affected by a data leak, don't panic! First, check which websites are responsible for this violation. Now, go to each website and change the password immediately. This measure is enough to protect you in most cases.

Sometimes, you will need to take more drastic action, for example if the breach affects your bank or it's very sensitive data like social security numbers. In these cases, you may want to freeze your credit, start using a credit monitoring service and / or check your credit report to make sure no one is doing anything suspicious in your name. yours.

If you believe someone else has opened an account in your name, contact that organization's fraud protection and let them know.

## How can you protect yourself from data leakage?




To protect yourself from data leaks, there are several steps you can take:

1. **Use strong passwords** : Ideal passwords are combinations of numbers, letters, and special characters. Also, you should never reuse the same password for multiple websites. Finally, never share your password with anyone.
2. **Use HTTPS when browsing the web** : Using HTTPS ensures you connect to websites securely. This makes it harder for hackers to get your data.
3. **Be wary of spam, phishing and other suspicious communications** : Be careful what you click, especially if you receive an unsolicited email or are browsing a less reputable website.
4. **Keep your device and software up to date** : Updating the operating system and other software can be an uncomfortable task. But it is an important way to protect you from attacks. When a security hole is revealed, companies will update their software to protect against it. If you do not update, you will leave a big hole in your security system.
5. **Check your credit report regularly** : If you think someone may have stolen your data, he can use it to withdraw money on your credit card in your name. Therefore, you should use a credit monitoring service. This service will send notice if suspicious activity is detected on your account.

With the information given, you may be ready to face a data leak. And by following the steps outlined above, you can make yourself less likely to become a victim of future data leakage.

If your job requires working with data, you should also consider how hackers can target your organization. To find out more, refer to 2 articles: 5 biggest mistakes in enterprise security and 6 enterprise security vulnerabilities

to be aware of.

You finished reading the article "**What is data leakage?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.