**A data leak may be disastrous for any business.**

A data breach reveals flaws in systems and failures in protecting the company's most sensitive information.

Despite being a disaster, the discovery of these flaws can be converted into a rewarding experience. It's an opportunity to improve your business operations in order to avoid a repeat of the situation.

Fortunately, there are a few basic steps you can take to protect your organisation from a data breach, preserving the company's reputation and avoiding a potentially significant charge.

**Here are the top 5 reasons for a data breach, as well as what to do if one occurs.**

1. **Human Error**

Unfortunately, one of the most common reasons of a data leak is human nature. As humans, we make mistakes, make poor decisions, and frequently fail to follow the procedures laid out in front of us. Human mistake is to blame in three major ways:

**Using Weak Passwords**

Hackers have a harder time cracking passwords that incorporate numbers, upper and lower case characters, and symbols, as difficult as they are to remember. Use dates and names that are difficult to read.

**Sharing Password Information**

Never give out your password to a coworker. While you would not want to suspect a coworker, giving anyone else access to your personal account is not a good idea.

**Scamming or opening phishing emails**

Emails or SMS messages that look shockingly realistic are one of the most common methods hackers gain access to networks. Responding to an email with personal or business information is never a good idea.

1. **Leaving security systems unpatched**

In the fight against a data breach, having a strong security system to protect your company's IT is critical. If you don't keep your security software up to date, you're leaving your firm vulnerable to hackers. Similarly, failing to update your website software to newer versions and keeping all relevant plugins up to date can invite a hacker in.

1. **Malware**

One of the most common reasons of a data breach is malware. Malicious software is a term that refers to any virus that is meant to assault, harm, or steal data from an IT equipment.

The following are the primary methods for avoiding malware:

* Use a strong antivirus programme.
* Keep an eye on the websites you visit at your place of business. During the working day, many companies limit the kind of websites you can access.
* Keep an eye on what you click on and what you open. If an email appears to be suspicious, report it to your IT department without opening any attachments.

Fortunately, malware rarely creates major problems for businesses, but the amount of malware in circulation is nevertheless a source of concern and a hazard that all employees should be aware of.

1. **When working remotely, be wary of insecure networks.**

Prior to the pandemic, approximately 14% of the workforce worked from home. In June 2020, 49% of workers said they had worked from home at some point.

Businesses have had to react rapidly to a shift in working locations, with working from home expected to continue for the foreseeable future. When the first lockdown began in March 2020, IT departments all across the world were forced to labour around the clock to guarantee that secure networks were in place to prevent data breaches while working remotely.

1. **Theft of a tangible object or document**

Have you ever forgotten something on a train, bus, or taxi? Many of us have done so. While the chances of the item being returned are small, you can take precautions such as encrypting passwords on computers and avoiding bringing printed documents home. To restrict access on mobile devices, sensitive documents should also be encrypted. Remember to shred any documents you no longer require to ensure that they are properly discarded. Don't forget about hard drive-containing gadgets. To prevent information from being accessed, hard drives can be securely shredded.

**After a data breach, what should you do?**

You may be tempted to panic if your company has been the target of a hacking effort. To operate properly and with integrity, follow these simple steps:

* Before you act, take a step back and think about what has transpired.
* Determine the specific problem and take steps to solve it. The way you react after the breach is remembered more than the breach itself.
* Communicate with your employees and customers, and be open and honest about what has occurred.
* Notify the ICO so that they can take appropriate action. A data breach must be reported within 72 hours of the occurrence.
* Learn from your data breach and reassure your customers that steps have been made to prevent a repeat occurrence.
* Staff should be informed and trained on the new procedures.

Recycle Pro can assist you in preventing data breaches now that you've recognised the major causes. Request a quote for our shredding services right now.