A privacy breach or sometimes known as a data breach is the misuse of your information. In other words, it is a cyber threat to your device. As the name 'privacy' breach suggests, it is the access to your private information without permission.

## Privacy Risks

Your privacy is very critical, and all your information is valuable. However, your information is spread over places like government agencies, financial institutions, health care agencies, and many other organisations. If this gets in the hand of the wrong people, then you can be in great danger. Hackers can use this information to commit crimes under your name. They can also sell this information on the dark web that gives access to further criminals.

## How it Works

The first step in this cyber threat is a security breach. Your device’s entire security system becomes null, and the hacker can penetrate your device. Thus, now all your data is open to the hacker. A technical problem in your device, human error, or inadequate policies can lead to cyber threats like privacy breaches. Sometimes, a mistake on your part like an email sent to the wrong person or a lost USB can also cause a privacy breach.

## Ways to Protect your Privacy

If a privacy breach takes place then there is not much you can do. However, you can take precautionary measures before time. Hence, it’s very important to follow these precautionary measures:

### Strong Password

Emphasis is always made on the use of strong passwords to prevent cyber threats. A password is the most common and greatest barrier against hackers. You should always use a strong, impeccable, and unique password for your device, system, and applications. If you feel that it is hard to remember strong passwords, you can use a reliable password manager.

### Monitor your Accounts

If a hacker gets access to your information then your accounts are at risk. You should always keep a regular check on your accounts for any suspicious activity. In case of any unfamiliar and doubtful activity, block your accounts to prevent more loss.

### Website Security

Don't just browse blindly on the internet. We enter a lot of information on the internet in the form of usernames and passwords. Thus, always check the website security before providing your credentials. A secure URL is one that begins with 'HTTPS' instead of 'HTTP.' Especially when you are accessing a website where you have to enter your credit card details, check the URL.

## Key Takeaway

Cyber threats always bring a heap of disaster with them so always ensure your online security. Take the necessary precautions to protect your personal information.

To know more about how you can keep your online experience secure, book a consultation with Aardwolf Security today!