## What is Tailgating?

Tailgating is a social engineering attack. In simple words, tailgating is when an unauthorised person gets access to a restricted area by following an authorised person. People also refer to it as 'piggybacking.' It is a simple and common way to get crucial information.

In this social engineering attack, the hacker impersonates as a delivery person, repairman, or other workers. The basic way to fool people is to enter behind them as they open the door to enter an authorised section.

Many people refer to this social engineering attack as ‘a bug in human hardware.’ The human nature of courtesy plays the role of a bug here which the imposter exploits. Some people feel that it is rude and blunt to inquire from a person about why they are going somewhere.

## How to Avoid It?

People tend to believe that it is hard to avoid tailgating because it requires them to set aside some social norms. However, there we can avoid this social engineering attack by taking simple precautions.

### Training

The first and foremost step to avoid tailgating is by training your employees. You need to make your employees understand the harsh effects of tailgating. Thus, employees should keep notice of their surroundings and report in times of malicious activity. Your employees can play the role of stakeholders when it comes to the security of your organization.

### Smart Card and Badges

Large businesses become a target of tailgating more often than others. Large organisations typically have several employees working on different floors in the building. Thus, not everyone is aware of who works in the building. There is a need to provide some identity to your employees for verification, such as smart cards and badges.

### Visitor’s badge

Just like smart card and badges for your employees, you will also need badges for visitors. Imposters make their way in the building and start impersonating your employees. Thus, you cannot distinguish them. However, a badge will highlight the visitors, and you will know that you cannot allow them to access everywhere.

### Biometrics

Technology can help you everywhere in your life. Biometrics enhances the security of your organisation and prevents social engineering attacks like tailgating. It is best if you install biometric verifications at every level of the restricted area. Thus, only some employees can enter after verification.

## Conclusion

You will need information protection online as well as in your offices. Hackers and imposters can go to any level to get your data. Hence, vigilancy and pro-active approach can help us protect our data.