Courtesy of
Chittenden Group

CYBERRISKS&LIABILITIES_

Tailgating and Piggybacking Explained

Tailgating and piggybacking are low-tech tactics used by malicious actors to access restricted areas. They occur when an unauthorized individual gains physical access to a location with sensitive information or vulnerable IT equipment, which can have significant financial and reputational impacts on businesses.

This article provides more information about tailgating and piggybacking, their potential impacts and tips on how businesses can prevent these security breaches.

Understanding Tailgating and Piggybacking
Tailgating and piggybacking present a significant risk to cybersecurity. Although resources are often devoted to complex digital hacking methods, businesses should not overlook the threats of tailgating and piggybacking. They are relatively simpler methods employed by cyber intruders to gain access to a business' secure data or equipment.

Tailgating can occur when a malicious actor sneaks in by following an authorized employee into a secured area. On the other hand, piggybacking is a type of social engineering tactic that occurs when the malicious actor tricks the authorized individual into letting them into a secure area. Here are examples of tailgating and piggybacking:

- An intruder disguises themself as a delivery person or contractor, so an authorized employee allows them to enter the premises.
- An authorized individual holds the door open for the unauthorized person behind them.
- A malicious actor pretends to be an employee who has forgotten or lost their credentials.
- An intruder carries a bulky item in their hands, making them appear too full to open the door, or they pretend to be distracted while talking on the phone and follow someone inside.
- A trespasser acts as if they are an invited guest and may even use specific names of people in the office to appear legitimate.
- An unauthorized individual follows an authorized individual through a slowly closing door before the door shuts and locks.

Once the perpetrator gains access to a restricted area, the business faces several risks. The intruder can steal or view sensitive data, upload malware, take property or damage devices. These occurrences can lead to significant data breaches, creating compliance violations and reputational damage. Security breaches can erode the trust of vendors and clients, leading to costly fines and penalties.

Preventing Tailgating and Piggybacking Attacks
As part of a comprehensive approach to cybersecurity, businesses should implement measures to prevent tailgating and piggybacking attacks. Consider the following actions:

- **Implement access control systems.** Devices (e.g., badge readers, alarms, sensors and biometric scanners) can help prevent unauthorized individuals from entering secure areas. Entrances requiring multifactor identification can also discourage intruders.
- **Utilize surveillance cameras and video analytics.** Closed-circuit television and security cameras can help monitor who enters the premises and act as a visual deterrent. Advanced systems can also use artificial intelligence and video analytics to help identify unauthorized individuals.

CHITTENDEN GROUP
INSURANCE

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

- **Train employees on physical security awareness.** Businesses can help reduce risks by educating employees on physical security threats and training them to prevent them. Instructing employees to ensure doors close behind them and to report suspicious activity can also help mitigate exposures.
- **Use visitor management systems for tracking and authorizing visitors.** Visitor management systems provide a record of who has entered an area. Whether the system involves an employee working at the front desk, a security guard or a digital system checking in visitors, it can provide a layer of security to confidential areas.
- **Install physical barriers.** Turnstiles and security gates can provide a low-tech way to secure areas and provide a perceptible obstacle to potential intruders.
- **Maintain clear security policies and procedures.** Comprehensive security policies and procedures that address physical threats are essential. It's also critical to regularly update the policies and procedures and communicate any changes effectively.
- **Conduct regular security audits to identify vulnerabilities.** Testing and auditing security systems can help identify and remedy weaknesses. Additionally, they can provide insight into which methods are effective.

Conclusion

Physical breaches, such as tailgating and piggybacking, threaten confidential data and vulnerable equipment. Taking steps to understand and prevent these events can help reduce the risk of them occurring and offer financial and reputational protection. For more information and risk management solutions, contact us today.