Cybersecurity Digest
Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

DT:01.06.2026

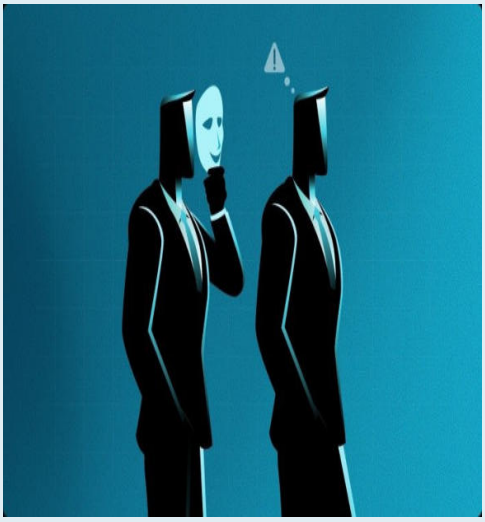
VOLUME 3 ISSUE 5

TAILGATING ATTACK

Tailgating is one of the most overlooked physical security threats in cybersecurity. A tailgating attack is a physical security breach where an unauthorized person gains access to a restricted area by closely following someone who has legitimate access credentials. Unlike technical cyber threats such as malware and phishing, tailgating exploits human behavior and lapses in physical security protocols to infiltrate organizations undetected. Attackers will often time their entry at doors, turnstiles, or lifts to slip past an organization's physical security measures. Once access is gained, the consequences can be severe as the attacker can try to steal sensitive information or devices or even install malware that creates a backdoor for future attacks. By understanding tailgating attacks, it is clear that organizations that fail to implement strong physical security controls are at high risk of breaches that could lead to other kinds of attacks.

What is a Digital Tailgating Attack?

While physical tailgating attacks involve unauthorized access to physical premises, a digital tailgating attack refers to unauthorized individuals gaining access to devices, systems, or networks due to negligence or security lapses. Unlike hacking attempts that exploit software vulnerabilities, digital tailgating relies on human errors and weak access controls.



Digital Tailgating Attack Examples

- **Stolen or Unattended Laptops**: Attackers may steal a logged-in laptop or access a device left unattended in a public space.
- **Shoulder Surfing**: Cybercriminals spy on employees entering passwords or accessing sensitive data in public areas like cafes, airports, or coworking spaces.
- **Accessing an Unlocked Workstation**: An unauthorized individual gains access to a company network by using a workstation that was left unlocked.
- **Exploiting Open Wi-Fi Networks**: Attackers intercept communications by connecting to unsecured public or corporate Wi-Fi networks.

Risks Associated with Digital Tailgating

Once an attacker gains digital access, they can:

- **Steal sensitive data**, such as customer records and intellectual property.
- **Inject malware, ransomware, or spyware** to compromise company systems.
- **Manipulate or delete critical files** to cause operational disruptions.
- **Use compromised credentials** to access internal databases or cloud applications.

Digital tailgating is often overlooked as a cybersecurity risk, but it can be just as damaging as a traditional cyberattack if not mitigated effectively.

Common Tailgating Methods Impersonation and Deception

Attackers use social engineering tactics to trick employees into granting them access to restricted areas. They may:

- Dress as security personnel, IT staff, or maintenance workers to gain trust.
- Claim to be a new employee who forgot their access card.
- Use emotional manipulation, such as pretending to be in distress or pretending to be a delivery driver and deliberately have their hands full when approaching a door to manipulate an em-

Risks and Consequences of Tailgating Attacks

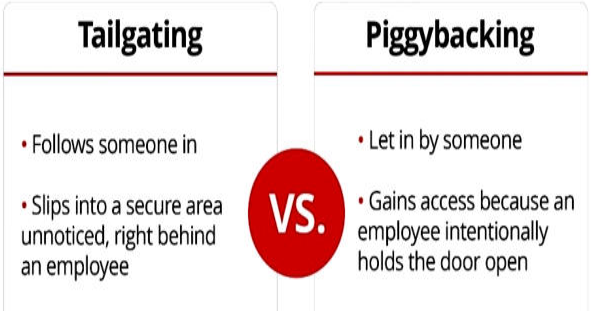
Data Theft and Security Breaches
Tailgating can lead to unauthorized access to sensitive data, resulting in financial losses, reputational damage, and legal liabilities.

Hardware Theft
Attackers may steal or tamper with company laptops, hard drives, or USB devices, potentially leading to the exposure of confidential data.

Malware Installation
Unauthorized individuals can physically or digitally introduce malware into a company's network, leading to system compromise, data loss, or ransomware attacks.

Sabotage
Tailgaters may damage or disrupt critical infrastructure, leading to downtime, financial losses, or operational failure.

Tailgating vs. Piggybacking
While both tailgating and piggybacking involve an individual gaining unauthorized access to an area but the key distinction lies in consent and awareness.
Tailgating occurs when an unauthorized person gains entry by closely following an authorized individual without their knowledge while Piggybacking happens when an authorized individual knowingly allows an attacker to enter a restricted area, often out of courtesy or without verifying credentials. This could involve an employee holding the door open for someone who appears to be a visitor or coworker, assuming they have permission to enter. Both tactics are used in social engineering and can be a serious security threat.



How to prevent Tailgating Attacks

Organizations can reduce the risk of tailgating attacks by implementing proactive security measures, such as:

Physical Security Measures

o **Implement Access Control Systems**: Implement the use of biometric authentication, keycards, and turnstiles to restrict unauthorized entry.

o **Use Security Guards and Checkpoints**: Ensure security personnel verify credentials before granting access to individuals.

Install Anti-Tailgating Doors: Deploy security doors that allow only one person to pass at a time.

Employee Training and Awareness

o **Conduct Security Awareness Training**: Educate employees on the dangers of tailgating and how to recognize social engineering tactics.

Promote a "Challenge Culture": Encourage employees to question and report unauthorized individuals.

Security Protocols and Policies

o **Enforce the "No Badge, No Entry" Policy**: Require all employees and visitors to display identification at all times.

Implement Zero Trust Security Measures: Regularly verify identity and access requests before granting entry.

Video Monitoring and Surveillance

o **Deploy CCTV Cameras and Motion Sensors**: Monitor high-risk entry points to detect suspicious activities.

o **AI-Powered Surveillance Systems**: Identify unusual behaviors and trigger security alerts in real time.

By implementing these security measures, organizations can strengthen their overall security measures against attackers using tailgating tactics to gain unlawful access to sensitive information.