

[Cybersecurity 101: The Fundamentals of Cybersecurity](#) > [What is a Cyberattack?](#) > [What are Tailgating and Piggybacking Attacks?](#)

WHAT ARE TAILGATING AND PIGGYBACKING ATTACKS?

Thuy Nguyen - June 25, 2025

Threat actors use digital tailgating — also known as piggybacking — to gain unauthorized system access, steal data, abuse privileges, or compromise infrastructure. Stolen credentials and hijacked user sessions are common digital tailgating techniques threat actors use to bypass security controls and exploit systems.

The terms “tailgating” and “piggybacking” originate from social engineering techniques used to breach physical locations. Now, these tactics are used within a digital context. The ramifications of digital tailgating can be just as severe as those of **other common cyberattacks**, including malware and insider threats.

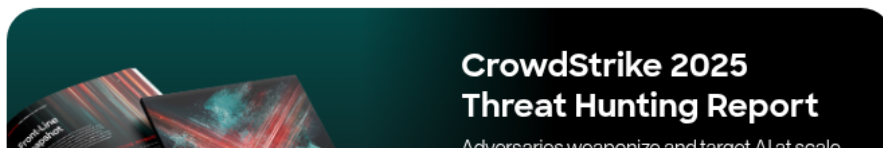
This article explores digital tailgating in depth, including its associated risks and effective defense strategies organizations can use to enhance their security posture.

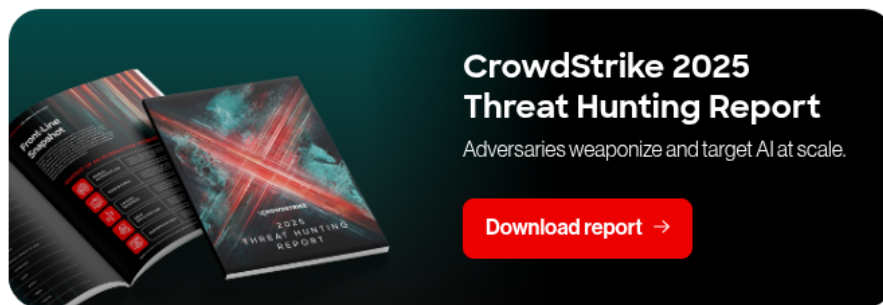
I Understanding tailgating in the modern digital world

In a physical tailgating or piggybacking attack, attackers use stealth or manipulation to access secure or restricted areas. Think of a credentialed employee using their personnel badge to swipe into a restricted office, only to have someone sneak in behind them before the door locks.

Digital tailgating applies the same principle to the digital world. It involves attackers exploiting the access of an authorized user to infiltrate networks or computer systems. Common methods threat actors use to digitally piggyback include:

- Session hijacking
- **Cross-site scripting (XSS)**
- Exploiting unattended and unlocked smart devices
- **Phishing** for credentials





I How tailgating works

When an attacker intends to tailgate their way into a network or computer system, they might use session hijacking, social engineering, or the system's flawed logout procedures. These methods are effective because they exploit human behavior and system vulnerabilities that IT security teams may overlook.

Session hijacking

Session hijacking (or cookie hijacking) is when attackers obtain a user session ID by sniffing network traffic using tools like Wireshark or by using an XSS attack to obtain the session cookie in the web browser. For example, if you're connected to your organization's network using an unencrypted Wi-Fi network, you leave yourself susceptible to tailgating via session hijacking.

Social engineering

Social engineering is another method attackers employ — one that relies on deception and manipulation — to tailgate into a network. An example is a phishing email that appears to come from your organization's IT department asking you to confirm your password as part of routine IT maintenance. If you fall for this and divulge your username and password, the attacker can gain access to your organization's network.

Flawed logout procedures

Flawed logout procedures occur when a system's logout mechanism fails to terminate the user's session properly after the user logs out or becomes inactive. As a result, the user's session remains active even when the user is not, creating a potential vulnerability that attackers can exploit to tailgate into the system.

LEARN MORE

See how you can quickly monitor for vulnerabilities with the systems and applications in your organization.

Watch: Using Falcon Spotlight for Vulnerability Management >

I Why tailgating is increasing in prevalence

The rise of remote work is driving an increase in digital tailgating. Remote workers often use personal devices without strong security controls, opt out of multi-factor authentication (MFA), or connect to their organizations' systems over an insecure network (such as unencrypted public Wi-Fi). Insecure networks are particularly risky because attackers can sniff the network using a

I Why tailgating is increasing in prevalence

The rise of remote work is driving an increase in digital tailgating. Remote workers often use personal devices without strong security controls, opt out of multi-factor authentication (MFA), or connect to their organizations' systems over an insecure network (such as unencrypted public Wi-Fi). Insecure networks are particularly risky because attackers can sniff the network using a packet sniffing tool and potentially steal session cookies.

Weak session management practices also create opportunities for tailgating attacks. For example, if tokens aren't rotated or invalidated quickly in OAuth-based sessions, they can stay active across multiple applications. This creates a wider window for attackers to intercept and exploit unrevoked tokens to gain unauthorized access.

I Risks associated with digital tailgating

Once an attacker successfully exploits one of these attack surfaces, they can operate in stealth mode because they have assumed the identity of a legitimate user. This creates business risks such as:

- Data compromise: Tailgaters may steal sensitive data, such as the target's personally identifiable information (PII) or corporate intellectual property (IP).
- Lateral movement: Once they have breached the perimeter, threat actors may move deeper into the organization's network.
- Malware installation: As a tailgater gains access to systems, they may install backdoors, ransomware, and other malware.

These attacks can have dire consequences for organizations, including financial losses, competitive disadvantages from stolen IP, and penalties for regulatory noncompliance.



EXPERT TIP

In this video CrowdStrike will illustrate Falcon using multiple detection capabilities to prevent script-based attacks.

[Watch: How Falcon Prevents Script-Based Attacks](#)

I Preventing tailgating in digital environments

Addressing common enablers of tailgating can significantly reduce the chances of a successful attack. Organizations can implement various techniques to mitigate digital tailgating risk.

Using MFA to deter unauthorized access

With MFA, organizations can strengthen their access security by requiring their users to verify their identity using multiple factors. MFA typically involves a combination of the user's password and at least one other factor, such as a code from an authenticator app or biometrics. Additional authentication factors make it harder for tailgaters to breach a system using a compromised password alone.

Strict session management policies

With MFA, organizations can strengthen their access security by requiring their users to verify their identity using multiple factors. MFA typically involves a combination of the user's password and at least one other factor, such as a code from an authenticator app or biometrics. Additional authentication factors make it harder for tailgaters to breach a system using a compromised password alone.

Strict session management policies

Session timeout and automatic logout are fundamental session management best practices. Implementing both helps reduce the risk of attackers compromising active sessions.

- Session timeout automatically terminates sessions and invalidates tokens after a period of inactivity, requiring a user to reauthenticate to continue using the system.
- Automatic logout is similar in that a user is automatically logged out after a period of inactivity.

User awareness and training on security risks

When users know the risks of digital tailgating and the security practices to reduce them, they will be more security-conscious. Training should emphasize the importance of locking devices when unattended and the risks of failing to do so. Additionally, users should know how to identify phishing attempts; this can be achieved with organized phishing simulations and training.

Device and network monitoring

After a digital tailgater compromises a session, they will eventually exhibit abnormal behavior that a legitimate user would not. With adequate device and network monitoring, organizations can detect this behavior and act immediately. For example, if an attacker gains access to a user account from an unexpected IP address, network monitoring tools can flag the unusual location.

I How CrowdStrike helps mitigate digital tailgating risks

Understanding digital tailgating can help keep your organization one step ahead of attackers, reducing the risk of downtime, reputational damage, and noncompliance fines. Given the complexity of mitigating tailgating risks, many organizations look to enterprise-grade solutions built to protect against these attacks.

CrowdStrike Falcon® Adversary Intelligence performs incident investigation by analyzing malicious activity and enhancing detection with threat intelligence. Its features include an advanced malware sandbox and attack surface reduction.

CrowdStrike Falcon® Identify Protection detects and prevents identity-based attacks in real time. It offers auto-classification of all accounts, zero-friction identity verification with flexible policies, and improved security posture with multi-factor authentication, among other features.

Explore CrowdStrike's solutions for proactive defense against tailgating threats. [Start your free trial of the CrowdStrike Falcon® platform today](#) and stay one step ahead of attackers.¹

¹ Terms and conditions might apply.



Thuy Nguyen is a Senior Product Marketing Manager at CrowdStrike focusing on Falcon OverWatch threat hunting service. Thuy previously held roles at Microsoft driving advancement and thought leadership in AI and machine learning, specifically on open source solutions and responsible AI. Thuy holds



Thuy Nguyen is a Senior Product Marketing Manager at CrowdStrike focusing on Falcon OverWatch threat hunting service. Thuy previously held roles at Microsoft, driving advancement and thought leadership in AI and machine learning, specifically on open source solutions and responsible AI. Thuy holds an MBA from University of Michigan, concentrating in technology and marketing. Thuy currently resides in Seattle, Washington.

Featured Articles

Common Cyber Attacks



Types of Cyberattacks

SQL Injection



SQL Injection (SQLi)

Vulnerability Management



Vulnerability Management

Try CrowdStrike free for 15 days

- Start free trial →
- Contact us →
- View pricing >



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			



Types of Cyberattacks



SQL Injection (SQLi)



Vulnerability Management

Try CrowdStrike free for 15 days

- Start free trial →
- Contact us →
- View pricing >



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			