PHYSICAL SECURITY

What is Physical Security Testing?

Physical security testing simulates real-world scenarios where attackers combine social engineering and physical intrusion to bypass digital defenses. With remote work reducing on-site staff, physical access has become one of the easiest paths to compromise and the #1 added component to penetration tests in 2025.

This testing attempts to gain unauthorized access to restricted areas, evaluating whether an attacker could reach sensitive data through server rooms or network closets via lock circumvention, sensor manipulation, badge cloning, or social engineering.

Why conduct physical security testing?

Integration of Physical and Cybersecurity

Modern attackers combine both. A rogue device in your server room bypasses even the strongest firewall. Physical testing reveals vulnerabilities that render cyber defenses ineffective.

Awareness of Insider Threats

Physical assessments evaluate policies that mitigate tailgating, badge sharing, or unauthorized device usage—critical for organizations with employees and visitors who may unknowingly expose the organization to risk.

Regulatory Compliance

Many industries mandate physical security controls. Physical testing ensures compliance and aligns with industry best practices.

Could My Organization Benefit from Physical Security Testing?

Physical security is often a weak point in organizations, yet it's the least tested. If your organization has on-site infrastructure, remote access points, or compliance requirements, physical testing provides the integrated view of risk that technical testing alone cannot.

Why Use SEVN-X for Your Next Assessment?

SEVN-X combines physical intrusion testing with technical exploitation to show how attackers actually operate. Our assessments don't just test locks. We test whether your team can detect and respond to unauthorized access before it becomes a breach.

info@sevnx.com

484.989.0911

ACHIEVE BETTER CYBERSECURITY