Beware the Open Road: Unsecured Wi-Fi Risks for Travelers

The Fourth of July holiday weekend presents a historically opportune time for cyberattacks. A recent travel survey found that while physical theft remains a concern affecting 10% of surveyed travelers, cybercrime is rapidly catching up. A significant 7% of travelers reported falling victim to hacking or digital scams on their holidays, with American travelers experiencing a slightly higher rate. Public Wi-Fi snooping, where hackers steal data transmitted over unsecured networks, affected a concerning 33% of respondents. This highlights the importance of secure internet access while traveling. Social media account hacks and phishing scams were equally common, impacting 33% of cybercrime victims each. Identity theft emerged as another significant threat, affecting 29% of travelers targeted by cybercriminals. The survey also revealed that malware infections (26%) and ransomware attacks (20%) pose real threats to travelers, highlighting the diverse landscape of cybercrime targeting this vulnerable group.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.