Identity theft risk increases when traveling

Preventive steps lessen vulnerability caused by reliance on electronics

Written by Nancy Trejos - Gannett

The last time John Sileo took his daughter to DisneyWorld, it ended up costing much more than he expected.

When he returned to his hotel after a day at the theme park, his bank notified him that his credit card had been shut down because someone had gone on a $3,000 online shopping spree. He suspects the person used a smartphone to snap a picture of his card number at the theme park's electronic ticket booth.

Ironically, Sileo, an identity theft and fraud expert in Denver, had traveled to Orlando to give a speech to the Treasury Department on avoiding identity theft. But given that Sileo spends more than 50 days a year traveling for work, even he faces particular challenges to protecting his personal information.
"Data theft goes through the roof on the road," said Sileo, a spokesman for CSID, an identity protection provider.

Identity theft can be a rude awakening for many business travelers. Last year, identity theft made up 19 percent of the 1.3 million complaints stored in the Consumer Sentinel Network, a secure online database available to law-enforcement agencies.

Experts say business travelers are especially vulnerable because they increasingly rely on electronic devices that easily can be lost or hacked. Credant Technologies, a data-protection company, found that travelers have lost 11,000 mobile devices at the busiest U.S. airports this year, 37.5 percent of them laptops and 37.2 percent tablets or smartphones.

Hotels also are prime targets for people looking to steal financial data. In a study of 200 data-breach cases, Trustwave's SpiderLabs, the online security company's research arm, found 38 percent occurred at hotels or resorts.

"You are 15 times more likely to have your identity stolen than to have your car broken into," said Todd Davis, chairman and CEO of LifeLock, an identity-theft protection company.

Two key challenges for travelers involve the use of unsecured wireless networks at hotels, airports and other public venues and the infiltration of smartphones through Bluetooth technology.

A couple of years ago, Marshall Goldsmith, a buyer and restorer of antiques in Las Vegas, discovered that a stranger had opened credit card accounts and a home equity line of credit in his name. His information was likely compromised while using the Wi-Fi network at an airport. Now his computer is set up so he can gain access to it only with an eToken, a device that authenticates passwords.

"It costs more for the extra security, but I think that it's worth it," he said.

Many companies have taken measures to protect employees and sensitive corporate information, the Global Business Travel Association said. Many require their traveling employees to access company files through a secure virtual private network, or VPN. Others have invested in smartphones that can have their contents remotely erased.

But experts say workers must take responsibility for their own safety.

"If you take the appropriate precautions, you reduce your risk dramatically because the criminals will move to easier prey," Davis said.