

Global Visual Hacking Study Reveals Alarming Data Privacy Risks for Business Travelers

Concern for displaying sensitive company information on screens is rising due to GDPR, high-tech visual hacking gadgets and costly data breaches

Most business travelers consider visual hacking a threat, yet less than half say they are equipped to stop it. That's one of the key findings of the 2019 Global Visual Hacking Study conducted by SMS Research for 3M.

For this new study, more than 1,000 business travelers in Germany, India, Japan, the United Kingdom and the United States were asked about their attitudes toward data privacy and the actions they take to protect sensitive company information when they travel.

"The study reveals that 8 out of 10 business travelers consider visual hacking a threat," said Jessica Walton, global business manager, 3M. "What's more alarming is that business travelers recognize the risk but aren't leveraging effective safeguards against it. As a result, unprotected screens can be the weak link in a company's IT security efforts."

Over three-quarters of business travelers surveyed admit displaying company information on their screen in airplanes or on a train, while over two-thirds admit displaying company information on their screen while riding the bus or subway. This behavior might explain why business travelers surveyed believe nearly 1 in 3 data breaches occur because of visual hacking.

Data breaches have become commonplace, but many workers say they are not prepared to prevent them from occurring. According to the 3M study, two out of three business travelers have noticed someone looking at their screen. Despite this threat, more than 30 percent of business travelers say their organization has not educated them on how to protect sensitive information displayed on their screen.

For more information about how to help prevent visual hacking, visit www.3Mscreens.com/visualhacking

At a Glance: The 2019 Global Visual Hacking Study, sponsored by 3M:

Visual hacking is a threat.

Key Finding: Visual hacking is seen as a threat to business travelers – and concern is growing.

8 out of 10 business travelers consider visual hacking a threat.

More than two-thirds of business travelers are more concerned about visual hacking this year than last year.

Key Finding: Sensitive company information is at-risk for business travelers, most frequently on airplanes and trains.

Over three-quarters of business travelers surveyed admit displaying company information on their screen in airplanes and/or on a train.

Over two-thirds of business travelers surveyed admit displaying company information on their screen while riding the bus and/or using the subway.

Key Finding: Public transportation is considered the riskiest place to view sensitive information on-screen.

Half of business travelers say that public transportation is the riskiest place to view sensitive information on their screen.

Business travelers say the top four riskiest places to view sensitive information on their screens include public

transportation, cafés, airports and hotel lobbies.

Business travelers are visually hacked.

Key Finding: Visual hacking is rampant and a majority of business travelers have noticed someone looking at their screen.

Two out of three business travelers have noticed someone looking at their screen.

Key Finding: Business travelers risk revealing sensitive data on their screens.

Over 1 in 3 business travelers have seen business information on exposed screens when traveling. An equal number of business travelers have seen personally identifiable information on exposed screens when traveling.

Business travelers and their employers have a role in preventing visual hacking.

Key Finding: Business travelers try to prevent visual hacking, but most are not equipped to do so.

Less than half of business travelers say they are equipped to stop a visual hacker.

8 in 10 business travelers who say they are equipped to stop a visual hacker have a privacy filter.

1 in 3 business travelers say their company has not educated them on how to protect sensitive information on their screen.

Key Finding: More than half of business travelers have changed how they protect their screens in the past year – most often driven by data breaches and high-tech visual hacking gadgets.

Over half of business travelers have changed how they protect sensitive information displayed on their screen in the past year.

Nearly half of respondents who have changed how they protect information did so because of the increasing number of data breaches.

More than 4 in 10 business travelers who have changed how they protect information did so because of high-tech visual hacking gadgets.

4 in 10 business travelers who have changed how they protect information did so because of GDPR.

Visual hacking impacts business traveler productivity.

Key Finding: Very few people confront their visual hackers. Instead, travelers tend to move their screen or close their laptop.

Nearly half of those who have noticed someone looking at their screen moved the screen so the person couldn't see.

Over 1 in 3 of those who have noticed someone looking at their screen closed their laptop.

8 out of 10 business travelers try to prevent people from seeing their screen.

Visual hacking may lead to costly data breaches

Key Finding: Travelers link data breaches to visual hacking.

Business travelers believe that almost 1 in 3 company data breaches occur because of visual hacking.

About this Study:

The survey was executed in January 2019 by SMS Research. This study is based on responses from 1,007 business travelers in Germany, India, Japan, the United Kingdom and the United States who take a minimum of six business trips per year. Margin of error: +/-2.41% at a 95% confidence level for the total sample.

About 3M Display Materials and Systems Division

3M Display Materials and Systems Division is committed to bringing top-of-the-line, innovative privacy solutions to market. Privacy Filters from 3M help secure personal and confidential data displayed on screens by blacking out content from unauthorized side views, allowing workers to remain compliant with the company privacy policies. As experts in screen privacy, 3M offers one of the industry's most complete lines of screen privacy filters, available for most of today's high-resolution monitors, laptops, tablets and smartphones. Privacy Products from 3M help organizations protect information displayed on screens, wherever their employees might access it. For more information, visit www.3Mscreens.com/visualhacking.

About 3M

At 3M, we apply science in collaborative ways to improve lives daily. With \$33 billion in sales, our 93,000 employees connect with customers all around the world. Learn more about 3M's creative solutions to the world's problems at www.3M.com or on Twitter @3M or @3MNews.

3M is a trademark of 3M Company.

Contact:

Heidi Wight

Padilla

612-455-1795

Heidi.Wight@PadillaCo.com

<https://news.3m.com/2019-06-17-Global-Visual-Hacking-Study-Reveals-Alarming-Data-Privacy-Risks-for-Business-Travelers>