3M News Center

Study Identifies Visual Privacy as Weak Link in Data Security Practices

Two-Thirds of Employees Put Sensitive Information At Risk for a Visual Data Breach When Working Outside the Workplace

A recent study conducted by People Security and commissioned by 3M, the maker of privacy filters for computers and mobile devices, reveals two-thirds of employees expose sensitive data outside the workplace – some even exposing highly regulated and confidential information such as customer credit card and social security numbers. The *Visual Data Breach Risk Assessment Study* also found the majority of companies do not have policies or measures in place to protect sensitive information from computer screen snooping when employees are working in public places.

During RSA Conference, key findings from the Visual Data Breach Risk Assessment Study will be available at Booth 959 in the Expo Center, along with additional materials from 3M Privacy Filters.

“With the rise in mobile workers carrying confidential data with them outside the office, snooping is no longer a harmless hobby and may represent a weak link in corporate data security practices,” says Dr. Hugh Thompson, Chief Security Strategist of People Security. “Today’s latest smart phones now make it possible for a data thief to take a high-resolution picture of confidential information on a computer screen and retrieve readable data without any hacking necessary. Information revealed on mobile devices outside the workplace now creates a window into a corporation’s most confidential data – whether it is regulated or simply company secrets – and significantly raises the threat level of visual data breaches.”

“Companies know they need to protect confidential information, but the threat of a visual data breach has historically been low on the priority list,” said John Stoxen, 3M Director of Business Conduct and Compliance. “This study should convince companies to reassess their data security policies and tools to determine how to better protect against visual data breaches when employees are working outside the office. At 3M, we address the risk of visual privacy in our Electronic Resources policy by requiring employees to take appropriate measures to protect 3M confidential information in public places by using privacy filters.”

The study included a survey of 800 working professionals[1] and an experiment at a large IT conference where attendee computer usage habits and data security choices were observed[2]. The following key findings and implications outline some of the highlights from the whitepaper.

Key Study Findings:

Employees Putting Information at Risk of Visual Breach

The study revealed that two-thirds (67%) of working professionals surveyed had worked with some type of sensitive data outside the trusted confines of the office within the past year, including highly sensitive information such as customer credit card numbers (26%), customer social security numbers (24%), patient medical information (15%) and internal corporate financial information (42%).

Smart Phone Camera New Tool for Data Thieves

Fifty-five percent of working professionals surveyed worked on their laptop in a high-traffic public area at least 1 hour per week. IT analyst firm IDC estimates that nearly 73 percent of the US workforce has some level of mobility[3], and by 2013 this number will increase to more than 75 percent. Many of these workers will access corporate email/data in public areas through laptops and smart phones and the rise in quality smart phone cameras now makes it possible for a data thief to capture readable information as it is displayed on screen. Since the pictures can now be preserved for future use this increases the risk of a visual data breach.

Visual Privacy Under-Addressed by Corporate Policy

There is a significant gap between risk and corporate policy to prevent visual data breaches. Seventy percent of working professionals surveyed said their company had no explicit policy on working in public places and 79 percent reported no company policy on the use of privacy filters to prevent visual data breaches.

Employees Value Convenience Over Privacy.

Eighty percent of working professionals surveyed thought that prying eyes posed a risk to their companies. Yet a majority (65%) of kiosk users chose one without a privacy filter. These findings illustrate that some employees are careless with corporate data by choosing convenience over security.

Protection against visual data breaches last to be addressed by corporations.

Data security practices such as VPN access (46%), disk encryption software (38%) two-factor authentication (19%) were all more commonly used to protect against breaches compared to the use of privacy filters (13%).

Opportunity to Increase Productivity.

Fifty-seven percent of working professionals surveyed said they have stopped working on their laptops because of privacy concerns in a public place and 70 percent said they would be more productive in public places if they thought no one else could see their screen. By addressing the issue of visual privacy in corporate policies, as well as giving employees the necessary tools to protect the data they are accessing in public, companies can make their mobile workforce even more productive when working outside the office.

For more information or to download the study whitepaper, go to http://www.3MPrivacyFilters.com/whitepapers.

About 3M
3M captures the spark of new ideas and transforms them into thousands of ingenious products. Our culture of creative collaboration inspires a never-ending stream of powerful technologies that make life better. 3M is the innovation company that never stops inventing. With $27 billion in sales, 3M employs about 80,000 people worldwide and has operations in more than 65 countries. For more information, visit www.3M.com or follow @3MNews on Twitter.

[1] Luth Research conducted the survey of 800 working professionals who were employed either part-time or full-time at the time of the survey and used a computer for at least a portion of the day from August 30 to September 13, 2010. The margin of error is +/- 3.5 percentage points.

[2] Conference included 1,000 attendees who worked in the IT departments (directors, managers, programmers, support, etc.) in a wide range of industries (e.g. finance, healthcare, retail, etc.).

[3] IDC Worldwide Mobile Worker Population 2007–2011
Forecast, http://img.en25.com/web/CitrixOnline/IDC_MobileWorker_excerpt_0_0.pdf

Hunter Public RelationsTrisha Seminara, 212-679-6600, ext. 212tseminara@hunterpr.comor3MKatherine Hagmeier, 651-575-4368
