

New Study Exposes Visual Hacking as Under-Addressed Corporate Risk

While most security professionals focus on thwarting data breaches from high-tech cyber attacks, a new study exposes visual hacking, a low-tech method used to capture sensitive, confidential and private information for unauthorized use, as an under-addressed corporate risk. The [3M Visual Hacking Experiment](#), conducted by Ponemon Institute on behalf of the [Visual Privacy Advisory Council](#) and [3M Company](#), a leading manufacturer of privacy filters, found that in nearly nine out of ten attempts (88 percent), a white hat hacker was able to visually hack sensitive company information, such as employee access and login credentials, that could potentially put a company at risk for a much larger data breach.

Click To Tweet: [#VisualHacking exposed as under-addressed corporate risk in new study from @3MScreens #VPAC http://bit.ly/1zdIVCV](#)

“In today’s world of spear phishing, it is important for data security professionals not to ignore low-tech threats, such as visual hacking,” says Larry Ponemon, chairman and founder of Ponemon Institute. “A hacker often only needs one piece of valuable information to unlock a large-scale data breach. This study exposes both how simple it is for a hacker to obtain sensitive data using only visual means, as well as employee carelessness with company information and lack of awareness to data security threats.”

During the study, a computer security expert specializing in penetration testing, also known as a white hat hacker, entered the offices of eight U.S.-based companies under the guise of a temporary or part-time worker. The white hat hacker attempted to visually hack sensitive or confidential information using three methods: walking through the office scouting for information in full-view on desks, screens and other indiscrete locations, taking a stack of business documents labeled as confidential and finally, using his smartphone to take a picture of confidential information displayed on a computer screen. All three of these tasks were completed in full-view of other office workers.

The study revealed the following:

Visual hacking happens quickly: Companies can be visually hacked in a matter of minutes, with 45 percent occurring in less than 15 minutes and 63 percent of visual hacks occurring in less than a half hour. Visual hacking generally goes unnoticed: In 70 percent of incidences, a visual hacker was not stopped by employees – even when using a cell phone to take a picture of data displayed on a screen. In situations when a visual hacker was stopped by an employee, the hacker was still able to obtain an average of 2.8 pieces of company information (compared to 4.3 when not stopped). Multiple pieces of sensitive information were able to be visually hacked. During the study, an average of five pieces of information were visually hacked per trial, including employee contact lists (63 percent), customer information (42 percent) and corporate financials (37 percent), employee access & login information/credentials (37 percent) and information about employees (37 percent) during any given hack. Unprotected devices pose the greatest opportunity for sensitive information to be visually hacked. 53 percent of information deemed sensitive (access or login credentials, confidential or classified documents, financial, accounting or budget information or attorney-client privileged documents) was gleaned by the visual hacker from the computer screen, greater than vacant desks (29 percent), printer bins (9 percent), copiers (6 percent) and fax machines (3 percent) combined. Open floor plans pose a greater threat to visual privacy. In experimental trials completed in companies with an open-office layout, an average of 4.4 information types were visually hacked, while those conducted in a traditional office layout saw 3.0 information types visually hacked. Unregulated functional areas were the most likely to experience a visual hack. On average, customer service roles consistently saw the highest number of visual hacks at 6.0, with communications at 5.6 and sales force management 5.2. Regulated functional areas like accounting & finance saw lower averages at 1.9, and legal at 1.0 experienced the least. Visual hacking controls work. Companies that had relatively low visual hacking rates had more controls in place,

such as mandatory training and awareness, clean desk policies document shredding process, suspicious reporting process, and employed the use of privacy filters, to protect against the threat than those without. For instance, in those companies that employed the use of privacy filters, 50 percent of trials saw three or less information types visually hacked while 43 percent of companies that did not use privacy filters saw four or more information types visually hacked.

“Visual privacy is a security issue that is often invisible to senior management, which is why it often goes unaddressed,” says Mari Frank, attorney/mediator and privacy consultant/expert at Mari J. Frank, Esq. and Associates and member of the Visual Privacy Advisory Council. “This study helps to emphasize the importance of implementing a visual privacy policy, educating employees and contractors about how to be responsible with sensitive data they are handling, as well as equipping high-risk employees with the proper tools, such as privacy filters, to protect information as it is displayed.”

For more information on the study, go to 3Mscreens.com/visualhacking.

3M Specialty Display Systems is committed to bringing top of the line, innovative privacy and protection solutions to market, including privacy filters and screen protectors which help secure personal and confidential data by blacking out content from unauthorized side views, allowing businesses to remain compliant with industry privacy regulations, and screen protectors that help keep mobile devices looking new longer with durable, scratch-resistant protection and an ultra-clear view. For more information, visit www.3Mscreens.com.

About 3M

3M is a science-based company with a culture of creative collaboration that inspires powerful technologies, making life better. With \$32 billion in sales, 3M employs 90,000 people worldwide and has operations in more than 70 countries. For more information, visit www.3M.com or follow [@3MNewsroom](https://twitter.com/3MNewsroom) on Twitter.

3M is a trademark of 3M Company.

Photos/Multimedia Gallery Available: <http://www.businesswire.com/multimedia/home/20150218006172/en/>

Hunter Public Relations Julia Covelli, (212) 679-6600 x 317 jcovelli@hunterpr.com or 3M Media Jane Kovacs, 512-984-6747 3M Media Relations

Multimedia Files:

□

M Visual Hacking Experiment Infographic (Graphic: 3M)

Download:

[Download original 1.30 MB 2850 x 2100](#)

[Download thumbnail 18 KB 200 x 147](#)

[Download lowres 71 KB 480 x 354](#)

[Download square 28 KB 250 x 250](#)

□

<http://3MScreens.com/VisualHacking>


Download:

[Download original 33 KB 864 x 454](#)

[Download thumbnail 10 KB 200 x 105](#)

[Download lowres 46 KB 480 x 252](#)

[Download square 26 KB 250 x 250](#)

Additional assets available online:  [Photos \(2\)](#)

<https://news.3m.com/2015-02-18-New-Study-Exposes-Visual-Hacking-as-Under-Addressed-Corporate-Risk>

