New Study Exposes Visual Hacking Is A Global Problem

The 2016 Global Visual Hacking Experiment Takes an Eye-Opening Look at the Need for Visual Privacy in the Workplace—All Over the World.

Organizations around the world are at risk of sharing highly sensitive information through visual hacking in business office environments. This was revealed in the Global Visual Hacking Experiment,[1] an expansion of the 2015 Visual Hacking Experiment,[2] conducted in the United States. The new 2016 study, completed by Ponemon Institute and sponsored by 3M Company, found that sensitive information was successfully captured in 91% of visual hacking attempts globally.

In 2015, 3M conducted an experiment in the U.S. that revealed how easy it is to capture sensitive company information through visual hacking. To confirm that visual hacking was an issue on a global scale, 3M recently expanded the experiment to include offices in China, France, Germany, India, Japan, South Korea and the United Kingdom. The following findings are the combined results from the 2015 U.S. study and the 2016 global studies.

The worldwide results are alarming and serve as a good reminder of the importance of addressing visual privacy in organizations all over the world.

The Experiment

During the Global Visual Hacking Experiment, a white hat visual hacker assumed the role of temporary office worker and was assigned a valid security badge worn in plain sight.

The white hat hacker was sent into 46 participating companies to perform three overt tasks:

1. Walk through the office scouting for information in full-view on desks, monitor screens and other indiscrete locations like printers and copy machines;
2. Take a stack of business documents labeled as confidential off a desk and place it into a briefcase;
3. Use a 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 at each company.

Visual Hacking:

A low-tech method of capturing sensitive, confidential and private information for unauthorized use.

3M Global Visual Hacking Experiment At-A-Glance:

- **Visual hacking is a global problem.** 91% of visual hacking attempts were successful.[3]
- **A company's most sensitive information is at risk.** 27% of the data hacked is considered sensitive information, such as login credentials, confidential or classified documents, and financial information.[3]
- **Certain situations are more risky.** 52% of sensitive information was visually hacked from employee computer screens.[3]
- **Visual hacking happens quickly.** It took less than 15 minutes to complete the first visual hack in 49% of trials.[3]
- **Office layout affects visual hacking.** Traditional offices and cubicles make it easier to protect paper documents and more difficult to view a computer screen. In contrast, the open floor plan appears to exacerbate the risk of visual hacking.

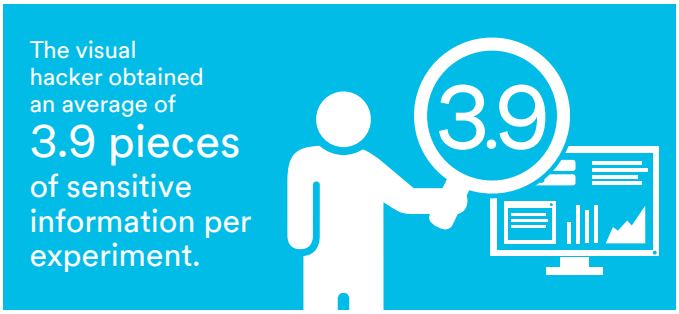
The experts in screen privacy. | 3M

Throughout 157 trials, the white hat hacker successfully captured 613 pieces of content, including login credentials, financial information, and privileged and confidential documents. This unprotected content could pose a potential security risk to organizations in the aftermath of a data breach incident.

Key Findings

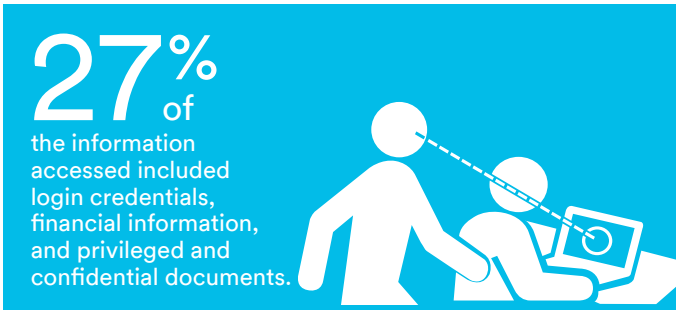
Where Visual Hacking Occurs
While the majority of visual hacks involved documents visible on employees' desks, the white hat hacker found that unprotected computer screens were considerable liabilities, with 52% of sensitive information captured by observing unprotected employee computer screens.

What's at Risk
During the experiment, an average of 3.9 pieces of sensitive information were acquired per trial, including contact lists (17%), customer information (16%), information about employees (12%) and login credentials (11%).

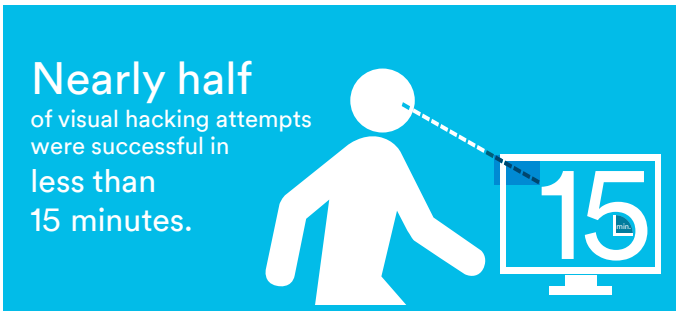


While the value of credit card or social security numbers is widely understood, seemingly unimportant information like a company directory can be valuable to hackers as well. This information can lead to a large-scale data breach through a variety of means, including phishing attacks, economic espionage, social engineering and even cyber extortion.

Vulnerability of Sensitive information
Of the 613 total pieces captured globally, an average of 27% was sensitive information such as login credentials, attorney-client privileged documents, confidential or classified documents and financial information.

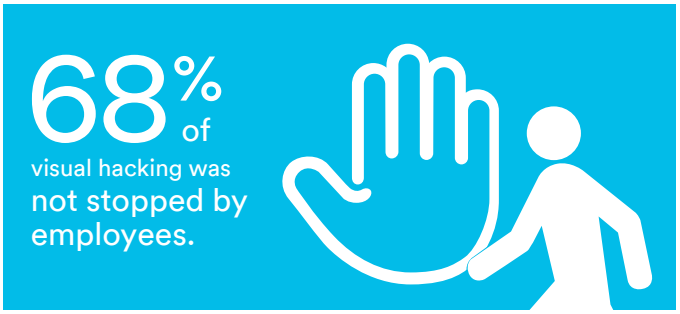


It Happens Quickly
A low-tech visual hack takes only minutes. In the study, almost half (49%) occurred in less than 15 minutes, and 66% occurred in less than 30 minutes.



Not an Isolated Problem
The experiment uncovered significant visual privacy risks in all functional areas within organizations. Globally, the highest number of information types hacked were in customer service functions and sales management.

It Often Goes Unnoticed
To compound the risk, visual hacks generally go unchallenged. Across all organizations and offices involved in the experiment, a disturbingly low number of employees confronted the white hat hacker. In 68% of trials, a white hat hacker was not stopped by employees. In only three cases did a worker contact the office supervisor about a possible insider threat.



The experts in screen privacy. | 3M

Office Layout Affects Visual Hacking Risk

The experiment also found a correlation between the type of office layout and successful attempts of visual hacking. There was an average of 3.2 visual privacy breaches in locations with traditional offices and cubicles with higher walls. By comparison, an open floor plan appeared to exacerbate the risk of visual hacking, with an average of 4.5 visual privacy breaches.

With the growing trend of open floor plans, it's critical to a company's security to educate employees in these environments on how to protect company information.

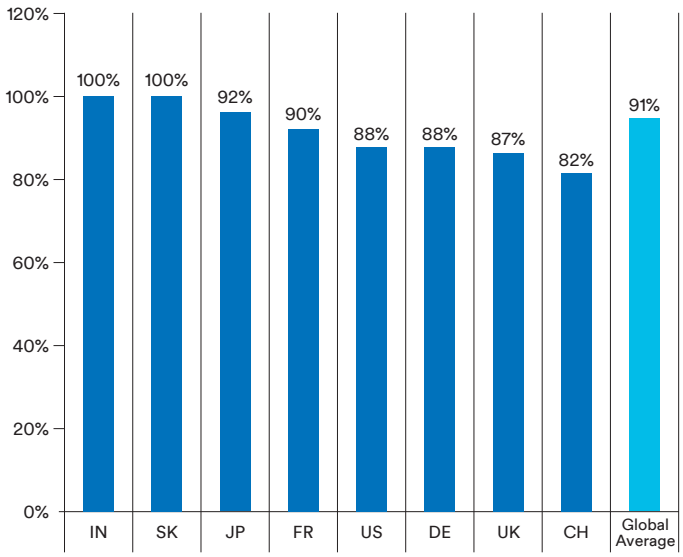


Figure 2. Visual Hacking Success Rate by Country

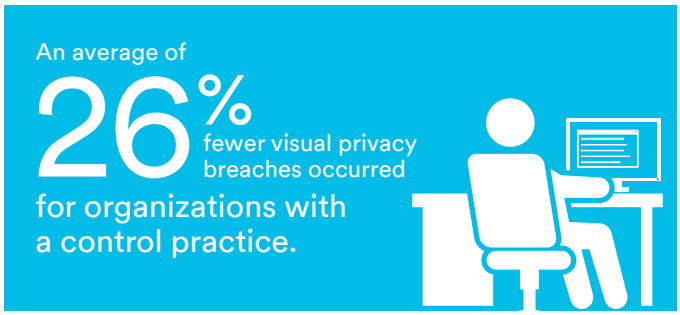
Conclusion

Visual Hacking is a Global Problem

Visual privacy is at risk globally. In all eight countries, the experiment demonstrated that companies in every country are vulnerable to visual hacking.

Companies Can Take Action

The Global Visual Hacking Experiment reveals how vulnerable an organization is to hacking. However, instilling controls to protect company information can minimize the risks. In fact, the experiment revealed that companies with sound control practices experienced on average 26% fewer visual privacy breaches.



Creating visual privacy policies and protocols is an important step in building awareness of the issue among employees. Companies should educate and train employees to properly handle company data. Issuing a clean desk policy, using privacy filters to help protect sensitive information displayed on screens, having a document shredding process, and setting up procedures that allow employees to report suspicious visual hacking behavior are other practices to lessen the chances for visual hacking. Organizations should perform regular, company-wide visual privacy audits to help identify and address vulnerabilities.

But keep in mind these policies should not be limited to what is accessible inside the office walls. Employees who frequently work outside the office are potential targets for visual hacks if they are not actively protecting their screens.

The threat of visual hacking is real. But there are many things a company can do to protect itself and its sensitive, confidential and private information.

3Mscreens.com/visualhacking

[1] Ponemon Institute, "Global Visual Hacking Experiment," 2016, sponsored by 3M.
[2] Ponemon Institute, "Visual Hacking Experiment," 2015, sponsored by 3M.
[3] Average based on global trials conducted by Ponemon Institute during the "Visual Hacking Experiment," 2015, and the "Global Visual Hacking Experiment," 2016, both sponsored by 3M.

The experts in screen privacy.

3M