New Study Exposes Visual Hacking as Under-Addressed Low-Tech Threat

A hacker may need only one piece of information to expose a company to a data breach. While large-scale breaches may make headlines, today's leading security professionals understand that low-tech threats can be dangerous to exposing company and customer information. A new study looks to expose visual hacking, a low-tech method used to capture sensitive, confidential and private information for unauthorized use, as a growing area of concern that can no longer be ignored.

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 for computers, tablets and smartphones, found that in nearly nine out of ten (88 percent) instances, a white hat hacker was able to visually hack corporate information, such as employee access and login credentials, through various visual means, including viewing physical documents on desks or viewing data on screens. The findings reveal how easy it is for a visual hacker to obtain sensitive information using only visual means, playing on both employee carelessness with company data and the lack of awareness to low-tech security threats.

The 3M Visual Hacking Experiment also revealed the following key findings:

Unprotected devices pose one of the greatest opportunities for sensitive information to be visually hacked. During the experiment, a white hat hacker (a non-malicious person hired to help expose security vulnerabilities) explored the offices of eight U.S.-based participating companies under the guise of being a contractor or part-time worker to see where and how he could obtain various pieces of corporate data in full view of other office workers. Throughout each phase of this experiment, the white hat hacker found that unprotected computer screens were a considerable liability.

These companies were fully aware of this experiment and had previously agreed to take part. 53 percent of information deemed sensitive, including access and log-in credentials, confidential or classified documents, financial and accounting information and attorney-client privilege documents, was gleaned by the white hat hacker from an unprotected device. This is greater than information gleaned from desks (29%), printer bins (9%), copiers (6%), and fax machines (3%) combined.

It is important to educate employees on the proper privacy controls available, including the use of a privacy filter to help secure information from snoopers while working and deploying a screen saver, or password-protecting devices when they step away.

Visual Hacking

A low-tech method used to capture sensitive, confidential and private information for unauthorized use.

Visual Privacy

The act of protecting sensitive, confidential and private information from visual hacking.

Sensitive Information Hacked[1]:

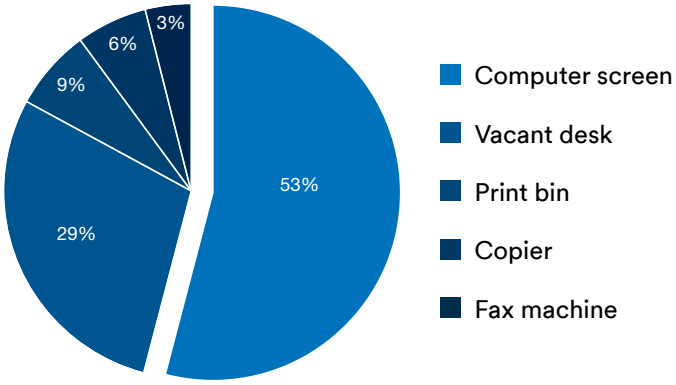
- Access and login credentials (47%)
- Confidential and classified documents (35%)
- Financial, accounting and budget information (12%)
- Attorney-client privilege documents (6%)

Sensitive information was obtained **88%** of the time.[2]

Privacy is the best policy.

3M

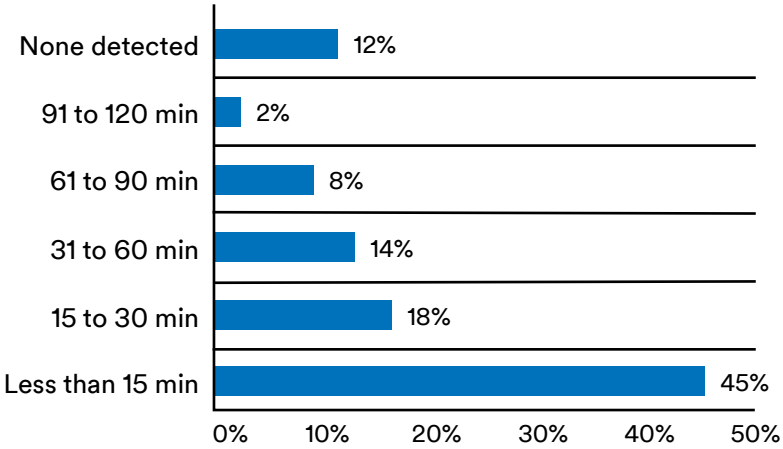
Locations where sensitive information assets were hacked



Visual hacking happens quickly and generally goes unnoticed.

Companies can be visually hacked in a matter of minutes, with almost half (45%) occurring in less than 15 minutes, and 63 percent occurring in less than a half hour. To compound the risk, visual hacks generally go unnoticed. As part of the experiment, 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 or indiscrete locations, taking a stack of business documents labeled as confidential, and finally using a smartphone to take a picture of information displayed on a computer screen. In 70 percent of incidences, a white hat hacker was not stopped by employees, even when a phone was being used to take a picture of data displayed on screen. In situations when a white hat hacker was stopped by an employee, the hacker was still able to obtain, on average, 2.8 pieces of company information, compared to 4.3 pieces of information when not stopped.

Elapsed time to complete first visual hack
n = 43 trials



Privacy is the best policy.

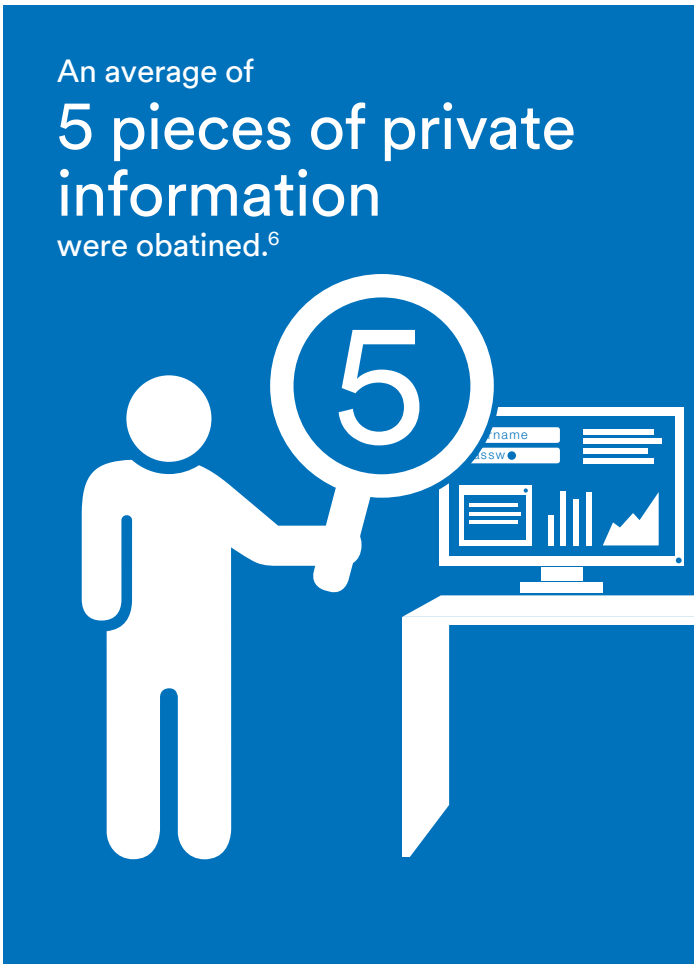
3M

Open floor plans may pose a greater threat to an organization's visual privacy.

As a means to increase productivity, many organizations are creating open workspaces, allowing their employees to work within a more free-flowing setting. With 70 percent of American employees working in open-office environments, it becomes all too easy for vendors, third parties or even malicious workers to see confidential information from a device screen or hard copy file.[5] 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. With the increased trend towards open floor plan offices, it's critical to a company's security to set up the proper privacy protocols and educate employees on how to better help protect visual privacy outside the comfort of office or cubicle walls.

It's not just about the data that was visually hacked—but where it can lead.

Often, employees and contractors are not aware that the information they work with is desirable to white hat hackers. As a result, they often do not take the appropriate safeguards to help prevent such information from being displayed openly and without the proper protections. During the experiment, an average of five pieces of information were visually hacked per trial, including employee contact lists (63%), customer information (42%), corporate financials (37%), employee access and login information/credentials (37%), and information about employees (37%). While the value of credit card numbers or social security numbers is widely understood, many do not realize that seemingly harmless information like a company directory or general business correspondence can be valuable to hackers as well. This type of information has the potential to open a company up to a large-scale data breach through a variety of means, including phishing attacks, economic espionage, social engineering and even cyber extortion. Stressing the importance of protecting all levels of data when it is being stored, transmitted, used and displayed is an important step in helping limit opportunistic data breaches.



Privacy is the best policy.

3M

Conclusion

The 3M Visual Hacking Experiment reveals just how easy it may be for a company to be hacked without even knowing it. However, visual hacking controls do help. For example, in those companies that employed the use of privacy filters, like those made by 3M, 50 percent of trials saw three or less information types visually hacked while 43 percent of companies that did not use a privacy filter saw four or more information types visually hacked.

Creating visual privacy policies and protocols is an important step in building awareness of the issue among employees, including contractors. In addition to using privacy filters to help protect sensitive information as it is displayed, companies should educate and train employees to properly handle the data they are responsible for maintaining. Issuing a clean desk policy, having a document shredding process and setting up procedures that allow employees to report suspicious visual hacking behavior are other ways to round out a visual privacy policy for better protection. Lastly, organizations should perform regular company-wide visual privacy audits to help identify and address any visual privacy vulnerabilities throughout the office.

Finally, these policies should not be limited to what is accessed inside the office walls. Working remotely is often part of the job, and any employees who frequently work outside the office are also potential targets for visual hacks if they are not actively protecting their data. In addition to equipping a mobile worker with a privacy filter, companies should clearly define what types of data can be accessed while working outside the office and what additional protocols need to be put in place to help ensure people can be productive but not careless with company and corporate data.

3Mscreens.com/visualhacking

[1]Ponemon Institute, "3M Visual Hacking Experiment," 2015, sponsored by 3M and the Visual Privacy Advisory Council.
[2]Ibid.
[3]Ibid.
[4]Ibid.
[5]International Management Facility Association.
[6]Ponemon Institute, "3M Visual Hacking Experiment," 2015, sponsored by 3M and the Visual Privacy Advisory Council.

Privacy is the best policy.

3M