New Global Study Reveals Majority of Visual Hacking Attempts Are Successful

Experiments conducted in eight countries reveal high risk of low-tech hacking methods

Organizations around the world are at risk of sharing highly sensitive information through visual hacking in business office environments. This risk was revealed in the 2016 Global Visual Hacking Experiment, an expansion of the 2015 Visual Hacking Experiment conducted in the United States by Ponemon Institute and sponsored by 3M Company. The global study included trials in China, France, Germany, India, Japan, South Korea and the United Kingdom. The combined results found that sensitive information was successfully captured in 91 percent of visual hacking attempts globally.

The global experiments involved 157 trials with 46 participating companies across the eight countries. They exposed low-tech hacking methods as a significant risk to corporations around the world. The findings revealed that organizations need to create awareness among employees on protecting data displayed on device screens, as 52 percent of the sensitive information captured during the experiments came from employee computer screens.

In the experiments, a white hat visual hacker assumed the role of temporary office worker and was assigned a valid security badge worn in visible sight. 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; observing computer monitor screens and other indiscrete locations like printers and copy machines; taking a stack of business documents labeled as confidential off a desk and placing it into a briefcase; and using a smartphone to take a picture of confidential information displayed on a computer screen. All three of these tasks were completed in front of other office workers at each participating company.

Combined average highlights from the 2015 U.S. Visual Hacking study and the 2016 Global Visual Hacking study revealed the following:

1. Visual hacking is a global problem. Visual hacking occurred in all countries where the experiment was conducted, with 91 percent of attempts being successful.

2. Employee computer screens are most at risk for visual hacking. Globally, 52 percent of sensitive information was visually hacked from employee computer screens.

3. A company’s most sensitive information is at risk. Of the visually hacked data, 27 percent was considered sensitive information, including login credentials, attorney-client privileged documents, confidential or

classified documents, and financial information. The information was deemed to be sensitive because of the potential security risk to the organization in the aftermath of a data-breach incident.

4. Visual hacking happens quickly. It took less than 15 minutes to complete the first visual hack in 49 percent of the hacking attempts.

5. Office workers are timid about confronting a visual hacker. In 68 percent of the hacking attempts, office personnel did not question or report the visual hacker even after witnessing unusual or suspicious behavior.

6. 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, an open floor plan appears to exacerbate the risk of visual hacking.

7. Companies can take action. The experiment revealed that companies with sound, privacy-control practices experienced 26 percent fewer visual privacy breaches on average.

"The results of these experiments uncover the significant visual privacy risks that all organizations face globally, regardless of their size, business type or location," said Dr. Larry Ponemon, founder of Ponemon Institute and chairman of the 3M-sponsored Visual Privacy Advisory Council. "While visual hacking is often considered a low-tech threat, the repercussions can be just as detrimental as a high-tech cyberattack."

As the expert in screen privacy, 3M offers the industry's broadest line of privacy products to fit most of today's popular devices. 3M Visual Privacy solutions can be applied to the screens of desktop monitors, laptops, tablets and smartphones to help organizations prevent visual hacking by protecting information displayed on screens and help comply with data privacy rules. Learn more at www.3Mscreens.com.

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

Download the full 2016 Global Visual Hacking Experiment report.
Download the white paper revealing key findings from the 2016 study.
Download the 2016 study infographic.

About 3M
At 3M, we apply science in collaborative ways to improve lives daily. With $30 billion in sales, our 90,000 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 @3MNewsroom.

PadillaCRT Heidi Wight, 612-455-1795 heidi.wight@padillacrt.com

Multimedia Files:

ee key findings of the Global experiment as an infographic. (Graphic: 3M)
)ownload:
)ownload original 1.34 MB 1530 x 1980
)ownload thumbnail 33 KB 155 x 200
)ownload lowres 153 KB 371 x 480
)ownload square 67 KB 250 x 250

ttp://www.3mscreens.com
)ownload:
)ownload original 40 KB 244 x 128
)ownload thumbnail 15 KB 200 x 105
)ownload lowres 20 KB 244 x 128
)ownload square 42 KB 250 x 250

Additional assets available online: Photos (2)

https://news.3m.com/2016-08-10-New-Global-Study-Reveals-Majority-of-Visual-Hacking-Attempts-Are-Successful