Visual Hacking Is Highly Successful At Getting Sensitive Information

POSTED ON FEBRUARY 21, 2015

In an experiment sponsored by 3M carried out by the Ponemon Institute over a two-month period last summer, it was discovered that companies are not prepared against “visual hacking” attempts.

Sensitive info obtained in 88% of the cases

Visual hacking consists in a threat actor collecting information by simply walking in an office and snooping into confidential documents or taking pictures of computer screens. This type of activity could help with better preparing a cyber-attack on a targeted organization as well as lead to unauthorized access to company secrets.

For the study, Ponemon Institute recruited eight US-based companies that allowed a visual hacker to roam in the building and determine the type of information that could be exposed this way; except for the company liaison, the rest of the employees were unaware of the true mission of the hacker.

Walking through the offices the hacker could have harvested personally identifiable information, data about customers, consumers and employees, business correspondence, log-in credentials, confidential documents, designs, presentations and financial information.

In 88% of the trials the hacker was able to obtain sensitive data. In most cases (51%) it would be found on the desk of a “fellow co-worker.” The hacker also managed to copy sensitive details from computer screens, print bins or copiers. Important data sitting in plain sight could be collected.

During the experiment, a total of 168 pieces of information were stolen, 34 of them (20%) being marked as having a high value (i.e. access log-ins, confidential or classified documents) due to the security risks involved in losing it to unauthorized persons.

Computer screens and vacant desks were the places where most of the high value data was collected from.

The time needed to spot the assets ranged from less than 15 minutes in 45% of the cases, to two hours in 2% of the cases.

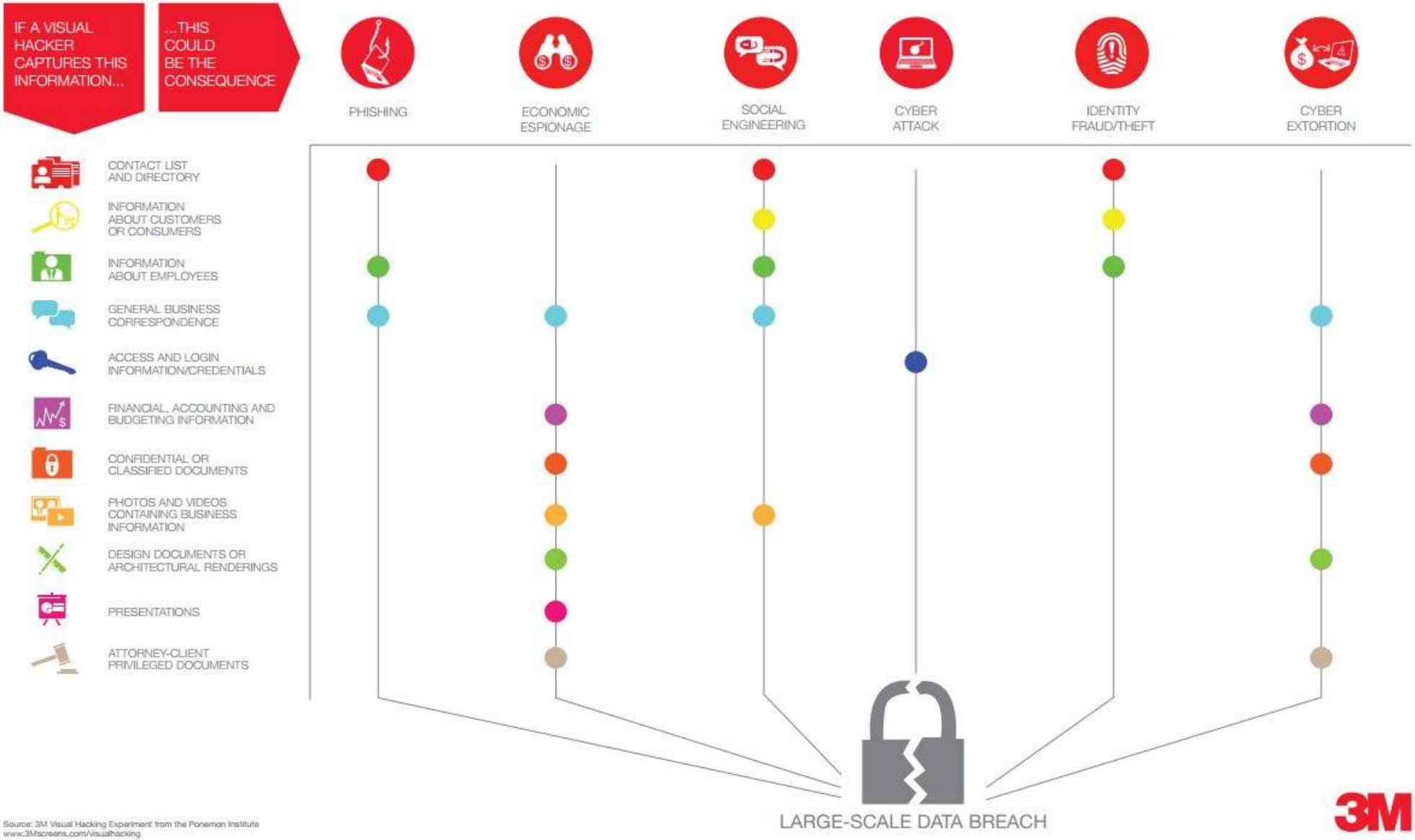
Even if the hacker was spotted to be engaged in collecting data, most of the times the other employees kept quiet and did not intervene. Only in 13 cases out of 43 someone asked questions about the dubious activity.

Although the experiment does have some limitations since the companies participated voluntarily in the research and collecting data depends on the skills of the visual hacker, the risks are still valid and organizations should implement stricter policies as far as protecting the information on and around the desk is concerned.

Source:
https://iicybersecurity.wordpress.com/2015/02/21/visual-hacking-is-highly-successful-at-getting-sensitive-information/

VISUAL HACKING: A GATEWAY TO LARGE-SCALE DATA BREACHES

A hacker often only needs one piece of valuable information to unlock a large-scale data breach. The 3M Visual Hacking Experiment exposes how simple it can be for a hacker to attain sensitive data using only visual means and where the data can take them—highlighting why visual hacking should no longer be an unaddressed security issue in today's enterprises.



Source: 3M Visual Hacking Experiment from the Ponemon Institute
www.3Mscreens.com/visualhacking

3M