Visual Hacker Alert - Risk Is Everywhere

by Steve Brown

Here is a weird thing for you to think about today. Consider how much you spend on IT security, guards, vaults and the like. Add it all up and it is a whopping big number. Then, consider how little you spend protecting data lying all over the bank. We have all been there with stacks of paper on the desk at times (some perpetually operate like this) as we try to get through our daily task list. Eventually, nature calls and we get up and wander down the hall. When we return, we notice a few of the papers seem out of order and wonder if someone came in and dropped something off or the air conditioning unit blew them around. Few ever think it could be a case of visual hacking.

Stop your work for a moment and look around the bank. Think about how many people working right around you are carrying smartphones with built-in cameras that can now zoom in to capture the eyelashes on a gnat. If someone were to take a quick picture of important information laying around they could potentially buy or sell your stock, sell a list of customers to others, or take social security numbers or other sensitive information right out the door in their pocket at the end of the day.

Consider that the proliferation of digital cameras has made it easier than ever to spy on unsuspecting victims. Law enforcement agencies in fact, have reported a marked increase in the number of these cases in recent years as visual hackers have been increasingly able to buy better, easier-to-conceal cameras.

Now before you go checking the photos of coworkers, consider the problem is a whole lot larger. We're talking about the potential for maintenance workers, contractors, delivery persons or even criminals posing as customers to slip away undetected with sensitive information.

To see how bad things might be, 3M recently teamed up with the Ponemon Institute to conduct a covert experiment. In it, an undercover white hat hacker was sent into the corporate offices of several participating companies. Alarmingly, the undercover hacker was able to obtain sensitive information in 88% of the tests and then walk right out the door with it.

Here are some interesting snippets from the study. First off, virtual hacking tends to happen quickly. In nearly 50% of the tests, the hacker obtained confidential information in 15 minutes or less.

Second, visual hackers tend to hit companies from multiple directions at once. In the tests, the hackers were able to obtain an average of 5 pieces of confidential information per test. These included corporate financials and confidential employee or customer information.

Third, visual hacking often slips under the radar. Everyone carries a phone, people love to take pictures and phones are part of our everyday lives so we don't think they will bring us any harm. In the tests, visual hacking incidents went unnoticed or unchallenged by employees 70% of the time, so maybe it is time to rethink how we think about smartphones. Further, even when attempts were interrupted, hackers still got away with an average of 2.8 pieces of sensitive documents.

Knowing there may be many wandering eyes within your bank on any given day requires employees to step up efforts to ensure sensitive information is protected at all times. For best practices, banks may find it helpful to consult the Visual Privacy Advisory Council's readiness checklist--which offers educational tips, protection policies and solutions.

Training is important and so is increasing awareness so actions can be taken to help protect against visual hacking. Beyond a clean desk policy, this effort should be top-down and include employees across all levels. Banks should also equip all computer monitors with privacy screen filters and protectors. This also goes for mobile devices such as laptops and tablets used in public places.

Here are a few other tips to help ensure data privacy: 1) implement a "clean desk" policy requiring employees to turn off device screens and remove all papers from their desks before leaving their workspaces; 2) ensure computer monitors with sensitive information aren't oriented toward publicly accessible spaces; 3) turn down screen brightness on monitors, so data can't be easily read by onlookers; 4) implement strict policies about the types of data employees can access from outside the office. We say this because a surprisingly large 67% of employees access sensitive company data in public places, according to the Visual Privacy Advisory Council.

BANK NEWS

Crisis Response

Research by Deloitte of executives, managers, analysts and crisis professionals from companies worldwide finds respondents said the following people would lead their organization when responding to a crisis: CEO or C-suite (38%), don't know or not applicable (30%), chief risk officer (15%), general counsel (6%), chief security officer (8%), and corporate communications (4%).

Oil Price Impact

A study by the JPMorgan Chase Institute finds consumers spent 78 cents of every dollar they saved from the drop in gasoline prices, spending 18% on eating out and 10% on groceries.

Cyber Concerns

A survey by Travelers finds American consumers worry most about financial concerns & risks (66%); followed by personal privacy loss & identity theft (60%); cyber, computer technology, data breaches & risks (57%); personal safety concerns & risks (51%); extreme weather & natural disasters (43%); transportation & travel risks (42%) and food safety concerns & risks (41%).

Mobile Deposits

Bank of America reports mobile check deposits climbed from 150,000 per day in 2014 to 225,000 per day this year.