MAN & MACHINE

July 8, 2024
www.man-machine.com

See Into the Future:
Exploring Visual Hacking and Best Practices in Visual Privacy

What is "visual hacking" and why should you care?

Visual hacking is the act of physically spying on someone's computer screens. Hackers gain access to sensitive personal data merely by looking over the shoulder of a computer user. A 2015 study by the Ponemon Institute reported 88% of visual hacking attempts were successful, nearly half of visual hacking attempts were successful in less than 15 minutes, and that 70% of the visual hacking went unnoticed or unchallenged by employees.[i]

Visual hacking is a low-tech threat as compared to malware, ransomware, or other high-tech threats, however, the repercussions can be just as detrimental.

Where does visual hacking occur, and why implement visual privacy policies and procedures?

Visual hacking in healthcare settings can lead to security breaches in personal data such as Electronic Health Records (EHR), or Electronic Medical Records (EMR). In 1996, the Health Insurance Portability and Accountability Act (HIPAA), a federal law, was passed to protect medical records and other patient health information. The top HIPAA violations include 'snooping' or visual hacking of healthcare records, and failure to perform an organization-wide risk analysis.[ii]

The U.S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR) investigates HIPAA violations. In June of 2024, there were over 883 cases of HIPAA violations currently under investigation, many of which involved visually hacked data from desktop computers.

These cases, and the fines levied against the organizations found in violation of HIPAA law are astounding. In 2018, Anthem, Inc, paid $115 million in a class action lawsuit, plus an additional $16 million to the US HHS OCR for failure to implement security controls.[iii]

In the financial services arena, visual hacking can be devastating with individuals losing control of their personal finances, as well as for the institutions who should safeguard their customers' personal information and money. BankInfoSecurity magazine published guidelines for protecting customers and institutions from visual hacking including implementing a visual privacy policy in company standards as well as outfitting computer monitors and device screens with privacy filters.[iv]

The Baking Secrecy Act of 1970, and the Right to Financial Privacy Act of 1978 protects the confidentiality of personal financial records and provides that the customer authorizes access to their personal data. Sensitive data includes full names and addresses, social security numbers, account numbers and email addresses.

The list of financial institutions hit with data security violations is ever growing: Binance $4.3 billion, HSBC Bank USA $1.3 billion, JPMorgan Chase, $1.7 billion, Wells Fargo $3 billion, Deutsche Bank $7.2 million, and finally, Bank of America has paid $4.3 billion in fines for consumer protection violations since 2020.[v]

Can we change the future?

Not every instance of data privacy violations cited above involved visual hacking. However, today's back-to-the-office work policies, and hackers' access to simple, yet powerful techniques like snapping a quick photo on their

cell phone leave so many organizations vulnerable to attack. Avoid making future headlines by reviewing and reinforcing your visual privacy practices and procedures in healthcare, financial services, and retail settings.

What do you see in your Crystal Ball?

Write your own future headline:

"[Your name here] DEMONSTRATES BEST IN CLASS FEDERAL PRIVACY COMPLIANCE BY IMPLEMENTING SAFEGUARDS AGAINST VISUAL HACKERS"

Man & Machine, a USA manufacturer of waterproof washable keyboards and mice, has over 30 years' experience in modifying and enhancing LCD monitors. Our Private Eye ™ Monitors are designed to keep you and your data safe from visual hacking.

Private Eye™ is an LCD monitor with a high-quality privacy filter which obscures critically important data from any angle except direct line-of-sight of the computer operator. The privacy filter is professionally installed either behind the bezel or laminated to the front panel, creating a tamper-resistant solution. We have partnered with Dell, HP, Planar, and Samsung to provide this solution without voiding the monitor warranty.

Is it time to focus on your visual security measures?

Contact us now at 301.341.4900 and mention this whitepaper or visit our website (www.man-machine.com) for more information about our Private Eye ™ Privacy Monitors from Man & Machine.

Oliver Thompson, MPH
Health Minister at Man & Machine
oliver@mmimd.com

---

[i] Visual hacking exposed. (2015, September 22). *InfoSecurity Magazine*.

[ii] *The most common HIPAA violations you must avoid - 2023 update*. The HIPAA Journal. (2023). https://www.hipaajournal.com/common-hipaa-violations/

[iii] Morse, S. (2018, October 16). Anthem pays $16 million in record HIPAA settlement for data breach. *Healthcare Finance*.

[iv] Burks, D. (2014, November 14). *Protecting Against "Visual hacking."* Bank Information Security. https://www.bankinfosecurity.com/blogs/improve-customer-trust-visual-privacy-p-1771

[v] Good Jobs First. (n.d.). Bank-of-america: Violation tracker. Bank of America | Violation Tracker. https://violationtracker.goodjobsfirst.org/parent/bank-of-america