Three Ways To Avoid Being Visually Hacked

(NAPSA)—Many people don't really leave their work behind at the end of the day or when traveling. Connecting to work e-mail and network files away from the office is increasingly common. While this growth of connectivity brings greater productivity, it can also mean greater risks as 75 percent of employers say it is hard to keep workers off unsecure networks.

As for your personal business, you can access your bank account or health information right on your smartphone, or make purchases at any number of online retail accounts.

Mobile devices have created more freedom and flexibility but they've also introduced challenges in protecting privacy.

The Problem

Think about the last time you accessed work or personal information using a mobile device in a public place. It may have been on an airplane or commuter train, in a hotel lobby or in a coffee shop.

How aware were you of your surroundings? Would you have noticed if an onlooker—whether sitting next to you or standing several feet behind you—viewed or even photographed your screen? Did you have hard copies of your work or other information, such as log-in details, that could have been seen?

Visual hacking is the act of viewing or capturing sensitive, confidential or private information for unauthorized use on a device screen, workspace or copier and the like. The growing sophistication of smartphone cameras and inconspicuous wearable technology is only making visual hacking easier to pull off and harder to detect.

What You Can Do

There are three actions you can take to help safeguard sensitive information:

1. Use privacy filters. A physical filter, available for laptops and mobile devices, can be applied to your device's screen. It lets you see a clear image while showing a dark, blank screen to anyone viewing the display from a side angle.

2. Don't invite an audience. When possible, angle your device away from your fellow customers or seatmates, high-traffic areas, and windows.

3. Secure your workspace. Password-protect your device and shut it down when it's not in use—even for something as brief as a phone call. Any documents that might contain sensitive information should also be securely stored away when they're not in use.

If you're a mobile worker in particular, don't wait for your employer to implement policies and technologies regarding visual hacking. In a recently conducted 3M Visual Hacking Experiment, the Ponemon Institute found that a white-hat visual hacker was able to enter a participating company and get sensitive information 88 percent of the time.

Individuals and organizations need to take a more proactive approach to combat these attacks. Your vigilance can help drive that change.

Learn More

For further facts about data privacy, you can go to www.3mscreens.com/visualhacking.