Get started on your Visual Privacy Policy.

With technology enabling more employees to work in public and increased regulations on data privacy and security, it's more important than ever for organizational leaders to address the threat of visual hacking within their policies and procedures.

To that end, the following Visual Privacy Readiness Checklist is designed to outline some steps leaders can take to raise awareness of the issues of visual hacking and visual privacy among their workforce. The goal is to prevent private, confidential and sensitive data from being displayed — and potentially visually hacked — in plain sight.

Visual Privacy Readiness Checklist

This Visual Privacy Readiness Checklist touches on three fundamental areas: educating your organization's workforce about the issue of visual hacking and the importance of visual privacy, creating specific policies to address these areas, and providing or suggesting solutions to prevent breaches.

Begin Educating your Organization

☐ Include educational modules on visual privacy and visual hacking in your security awareness training

☐ Include visual privacy and visual hacking awareness education in your new employee orientation

☐ Hold specialized visual privacy and visual hacking awareness training for senior managers and at-risk employees (see below)

Implement Policies & Procedures

☐ Identify at-risk employees using the following criteria:

- Frequency of travel (flying, commuting on public transit, etc.)
- Sensitivity of data managed (financial, HR, customer data, etc.)
- Time spent working outside the office (accessing email and texts or working on sensitive documents)
- Level within the organization (senior management can be particularly at-risk given the trade secret or confidential information they deal with)

☐ Require the use of privacy filters/privacy screen protectors:

- On all in-office devices used by at-risk employees to access sensitive internal information (HR, customer data, etc.)
- On all devices used to access sensitive information in public areas (private patient or customer data)
- On all devices used by employees when working outside the office

☐ If necessary, ban working in high-risk, high-exposure environments (airplanes, trains, restaurants, cafés, etc.)

☐ Implement a "clean desk" policy requiring employees to turn off device screens and remove all papers from their desks before leaving their workspace

☐ Institute security guidelines for IT applications to protect visual privacy

☐ Require applications to mask high-risk data to onlookers using strategies listed below (from most secure to least secure):

- Masking of data along with hiding data length
- "No exposure" character-by-character masking
- "Brief exposure" character-by-character masking (popular on mobile devices to ensure accuracy of the data typed in a password field)
- Masking a data field only when the field is inactive

Enable Compliance by Providing Solutions

☐ Equip employees with privacy screen filters and protectors for all mobile devices (including laptops, tablets, smartphones, etc) that can be used to access sensitive information in public

☐ Equip computer monitors used to access confidential data inside the workplace with privacy filters

☐ Set timeouts and screen savers on laptop/desktop displays appropriately to enhance visual security on unattended screens

3Mscreens.com

Privacy is the best policy.

3M