3M Science. Applied to Life.™

Visual privacy

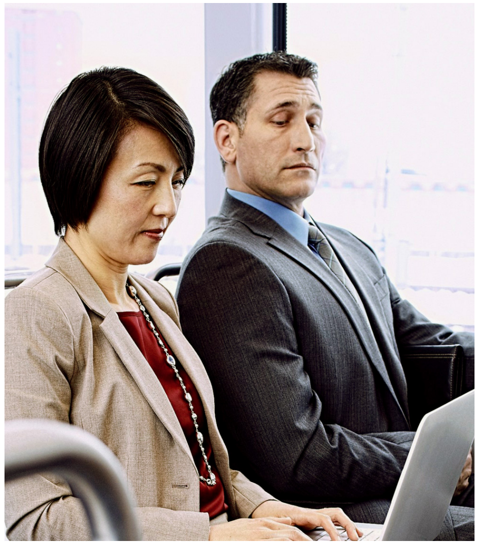
Quick guide

Why visual privacy matters

The evolution of new privacy and security software helps organisations to better protect confidential or sensitive information. However, basic physical security measures are just as important, such as preventing prying eyes from seeing a screen or printed document, because 'visual hacks' are easy to achieve, yet can have huge impact.

Visual hacking is the term given to the ability to view or photograph an image of potentially sensitive or confidential content on paper or on someone's screen – on a desktop monitor, laptop, tablet or smartphone – and then use that information for illegal or malicious purposes. Risks include:

- Identify theft
- Financial loss
- Regulatory fines
- Reputational damage



Time to act

Many organisations in the UK are already taking visual privacy seriously, across all kinds of private and public sectors – often in relation to regulation or individual industry guidelines, including:

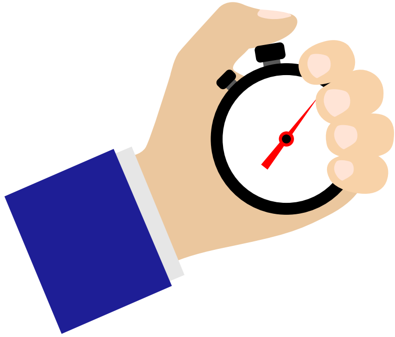
- ISO27001 compliance
- GDPR preparation
- FCA
- The Bar Council
- The Foreign & Commonwealth Office
- The Department of Work & Pensions
- UK government Security Policy Framework

Visual hacking is easy

No-one knows how many information security breaches result from visual hacking, but various studies have demonstrated just how easy and fast visual hacks can take place.

91 per cent successful visual hacks

on average worldwide, in the Global Hacking Experiment, carried out by the Ponemon Institute, across 8 countries including the UK



51 per cent took **15 minutes or less**

found the same study. 44 per cent of sensitive information was obtained by viewing screens (as opposed to paper documents)

9 out of 10 mobile workers

have caught someone looking over their shoulders at their laptop screens in public, according to the Public Spaces Survey, also conducted by the Ponemon Institute

Visual privacy best practice

Tip 1

Identify risk areas for visual hacking – whether in the office or working in public spaces – ensure screensavers and log-ins are automatically instigated after a short period of inactivity

Tip 2

Use privacy filters on all employee devices to help protect visual privacy in your organisation

Tip 3

Define a clean desk policy and procedures for visitors and mobile workers to help employees be privacy aware

Tip 4

Carry out privacy training and follow up with ongoing communications

Tip 5

Conduct ongoing visual privacy audits and training so your organisation is privacy-aware all year round

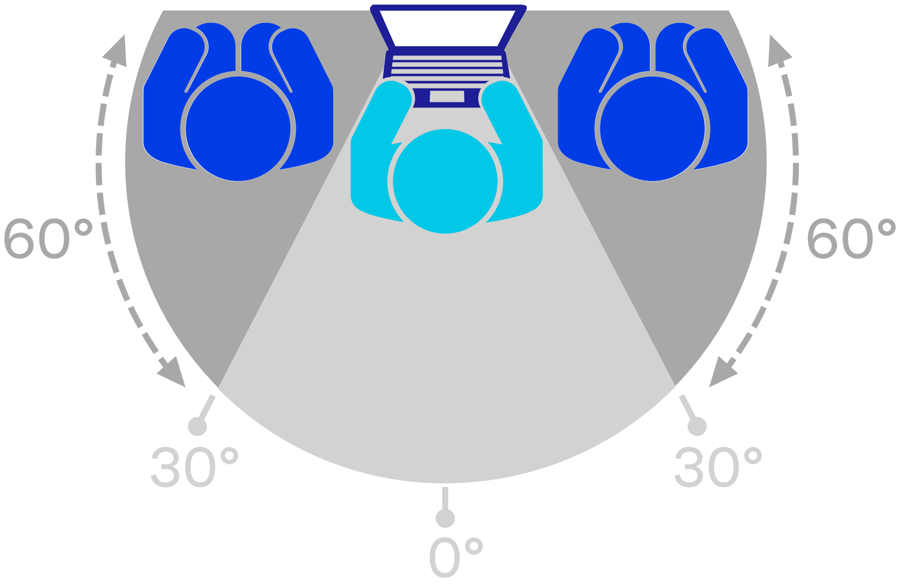
3M Privacy Filters – the fast and easy route to protect on-screen information

3M Privacy Filters keep visual hackers in the dark. Users see their screens with pristine image clarity in the centre-viewing angle, while prying eyes beside them see only a black or gold screen. This is made possible thanks to advanced microlouver technology that "blacks out" side views with world-class effective privacy.

Individuals and enterprises worldwide already trust 3M Privacy Products to help keep their private information private. The 3M range includes privacy filters for desktop monitors, laptops, tablets and smartphones, with a choice of sizes and options.

To request a sample, please visit:
www.3M.co.uk/PrivacyFilterSample

Zone of privacy protection



Display Material and Systems Division

3M United Kingdom PLC
3M Centre, Cain Road
Bracknell RG12 8HT
www.3M.co.uk/privacyfilters