3M Science. Applied to Life.™

# Protect sensitive data, wherever work takes you

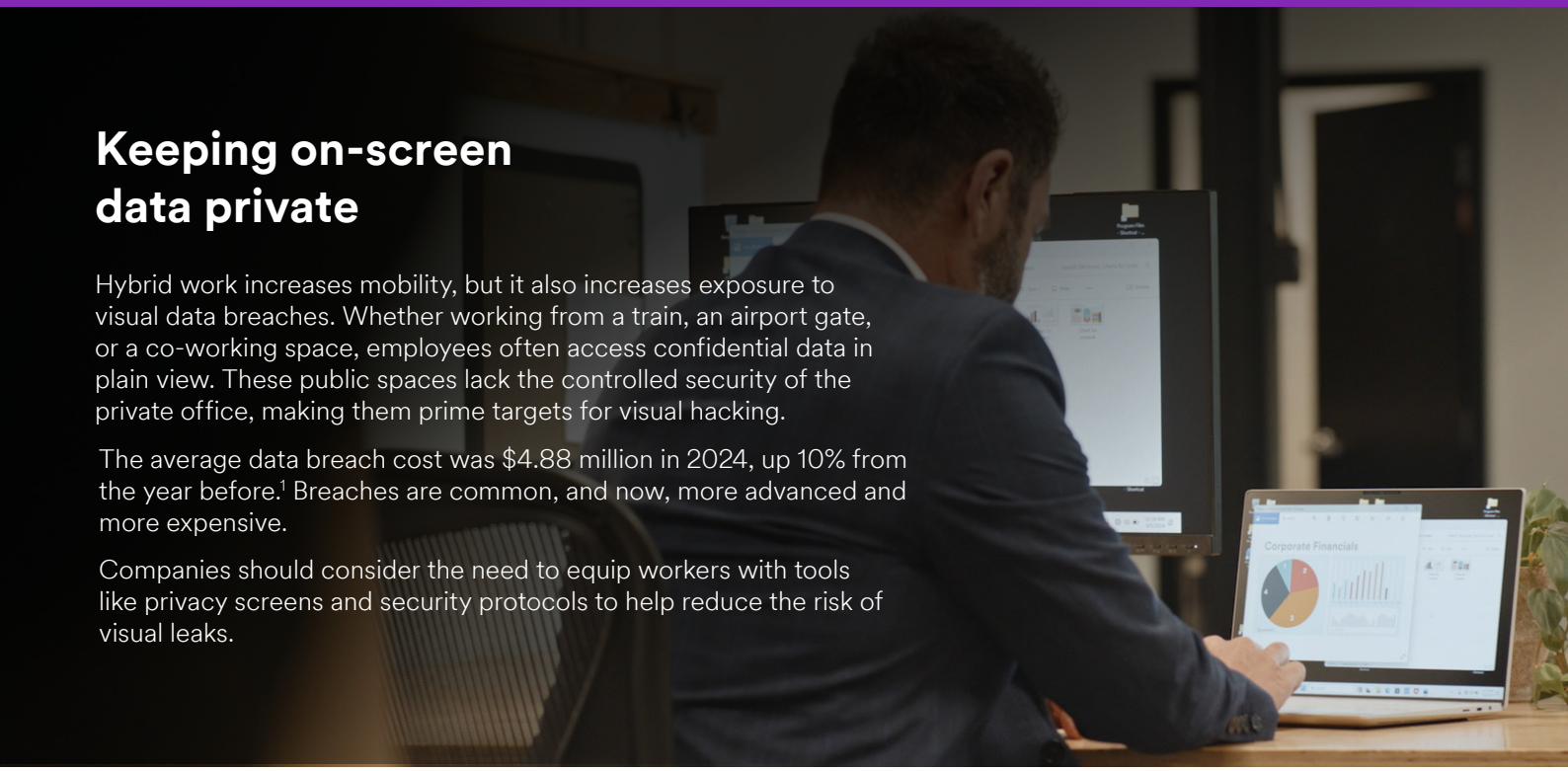
Stop on-screen data leaks before they happen with 3M Privacy Solutions

## What traditional data protection misses

As organisations modernise their operations with operating system upgrades, AI tools and cloud-based workflows, new data privacy concerns are emerging. They also introduce attack surfaces that traditional data privacy protection wasn't built to handle. This is where physical and visual security controls, like 3M Privacy Solutions, become essential. When assessing cyber risks, it's wise to look for both online threats and on-screen threats, such as screens that unauthorised people can see in hybrid workspaces. These overlooked gaps can be exploited as part of broader attack strategies, making visual privacy an important layer in modern IT security frameworks.

**"From data protection to physical security, we all play a part in safeguarding the organisation's future."**

—Sooji Seo, Senior Vice President and General Counsel, Information & Digital, and Chief Privacy Officer 3M



# Keeping on-screen data private

Hybrid work increases mobility, but it also increases exposure to visual data breaches. Whether working from a train, an airport gate, or a co-working space, employees often access confidential data in plain view. These public spaces lack the controlled security of the private office, making them prime targets for visual hacking.

The average data breach cost was $4.88 million in 2024, up 10% from the year before.[1] Breaches are common, and now, more advanced and more expensive.

Companies should consider the need to equip workers with tools like privacy screens and security protocols to help reduce the risk of visual leaks.

## Modernising security means more than devices

As Windows 10 support ends, many organisations are upgrading to Windows 11 and updating their devices in the process. The operating system brings hardware-based security features, ransomware protection and performance improvements, making it a better option for modern work environments.[2]

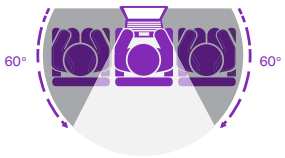
This hardware transition creates a natural opportunity to review additional layers of security. Screen privacy, for example, often goes overlooked. With more portable and shared devices, evaluating visual privacy tools like screen filters may help you reduce the risk of on-screen data exposure.


**Complete your data privacy and security plan with 3M™ Privacy Filters**

> Visual hacking is a complex issue that cannot be solved with digital technology, leaving few options for effective privacy protection.
>
> —*Sooji Seo*
>
> Senior Vice President and General Counsel, Information & Digital, and Chief Privacy Officer

## Practical protection against visual hacking

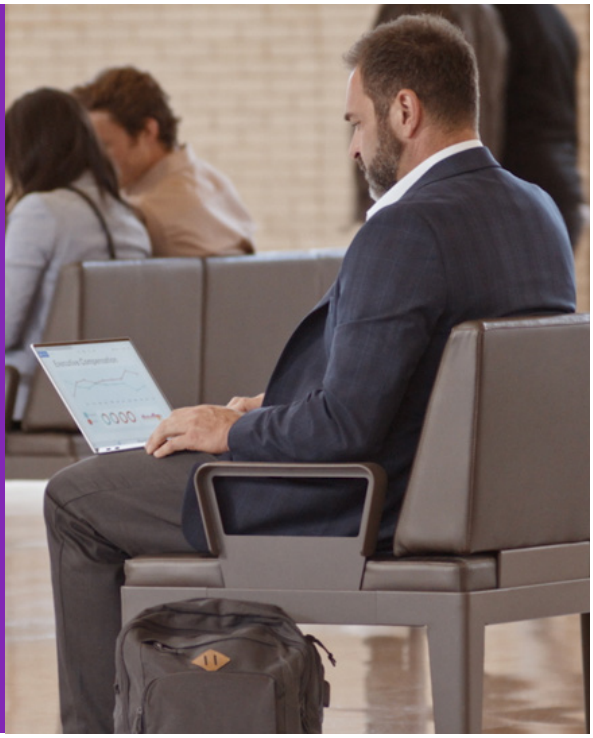
Physical tools like privacy filters offer a simple but effective way to reduce visual hacking risks, which remains a real threat to on-screen sensitive information. In environments where screens display confidential data, unauthorised onlookers can easily capture private information without ever touching a keyboard. Privacy filters, which restrict the viewing angle of screens, act as a potential deterrent and a physical barrier, making data far less accessible to shoulder surfer threats.




**Zone of visual privacy**

Unlike many other data privacy measures, privacy filters are low-cost, easy to deploy and immediately effective. Their affordability and scalability make them one of the most accessible ways for organisations to strengthen security without straining budgets.

> When your office is anywhere, your mind must be everywhere. Smarter thinking is one of your best tools against those who remain anchored in old norms.
>
> —*Sooji Seo*
>
> Senior Vice President and General Counsel, Information & Digital, and Chief Privacy Officer



## Treat every screen like a security checkpoint

3M and other Fortune 500 companies have taken action. Over the past decade, the shift to laptops and the widespread use of additional monitors has dramatically increased, making screen-based data more exposed and more in need of protection. 3M IT security teams realised then that screen privacy had become an essential component for a comprehensive IT data protection plan. The impetus behind investing in privacy filters is to help safeguard on-screen data such as intellectual property, trade secrets, communications, and customer information.

When 3M Senior Vice President and General Counsel, Information & Digital, and Chief Privacy Officer, Sooji Seo, discusses data protection with her counterparts at other companies, she often observes that “Many businesses have reservations about co-working and hot-desking environments, as some supervisors choose to work remotely when handling confidential budget and personnel files, given the limited privacy in office cubicles”.

## Encouraging everyday use

Even as a leader in screen privacy, 3M finds it challenging to ensure consistent employee use of privacy filters. Policies can help, but changing daily habits takes effort. Making the filters easy to use and readily available is important. It shouldn’t be a cumbersome task to remove them and put them back on when co-workers collaborate and share screens, but ease of use sometimes isn’t enough.

Incentives can help. 3M Global PC Hardware Lead, Ed Nelson, has some ideas about motivating staff. “In an initial rollout, you could have a ‘Spot: Reward’ campaign — get caught using your privacy filter and get a discount coupon for the company cafeteria.” Ed believes that, given the opportunity, all employees want to contribute to the good reputation and financial stability of their organisation.

## Write screen privacy into policy

When using 3M's electronic resources in public places, protect on-screen 3M confidential information, for example, by using a privacy screen and being aware of surroundings

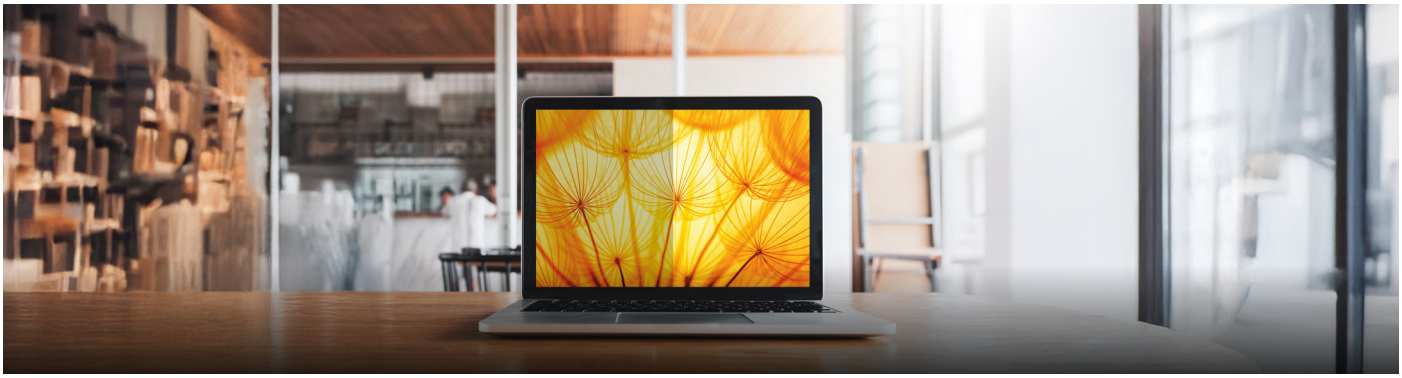
*—Privacy standard pulled from 3M internal guidelines*

## Spotting risks in everyday workspaces

The modern workplace has evolved alongside rapid advances in information technology. Cubicles have given way to open offices, and conference rooms now feature glass walls to create a sense of openness. However, large monitors visible from even the street can expose sensitive information if left unprotected.

IT and security teams should regularly assess screen visibility throughout the office, especially in high-traffic areas. Extra caution should be essential in environments where personal data is handled, such as hospitals, airports, and cafes.

Mobile workers also face privacy risks. On planes or in public spaces, open laptops can attract unwanted attention. While it's natural for people to glance at exposed screens, not all viewers have harmless intentions.



# Overlooked and underestimated: the threat of visual hacking

Our recent Qualtrics study showed what many organisations miss: visual hacking isn't rare, it's routine.

**78%**
have admitted to looking at other people's screens.

**Over half**
say they've caught others watching their device screen.

**4 out of 5**
have confessed to feeling worried about others looking at their screens.

**71%**
changed their behaviour because they felt someone was watching.

## This is particularly concerning when

**84%**
use their devices in public for work.

&

**87%**
of office workers have caught someone looking over their screen in public.[3]

## 3M™ Privacy Filters are here to help.

For over 35 years, we've refined our designs to enhance user experience. The 3M™ Bright Screen Privacy Filter delivers sharp clarity and outstanding privacy, helping to block side views while maintaining high brightness, making it ideal for travellers and high-traffic spaces. As remote work continues to grow, 3M™ COMPLY™ Attach Solutions offer quick and reliable privacy solutions, including magnetic attachments for monitors and flip options for laptops.


**Disclaimer:** Survey programmed in Qualtrics on September 14, 2024, with 1,015 U.S. respondents. The statements, information, views, and opinions expressed in the survey results are those of the respondents and do not necessarily reflect 3M's factual understanding or its views or opinions. 3M paid for, but did not participate in the survey, the preparation for the survey, or the gathering of responses of those being surveyed.

## Meet our 3M experts

Ed Nelson oversees the testing and selection of PCs, monitors and accessories for 3M employees worldwide. With a background in information security and global patch management, he has led initiatives that kept workstation updates at a 95% compliance rate.

*—Ed Nelson*
3M Global PC Hardware Lead

Sooji Seo brings two decades of legal and privacy leadership to 3M. She partners with IT and cybersecurity teams to strengthen digital security while enabling innovation across the company. Known for her clear guidance and collaborative approach, she champions both strong data protection and inclusive teamwork in a rapidly evolving digital landscape.

*—Sooji Seo*
3M Senior Vice President and General Counsel, Information & Digital, and Chief Privacy Officer

## The value of a good reputation cannot be underestimated

Newsworthy data breaches remind us to protect sensitive information both digitally and physically. At 3M, IT hardware managers like Ed Nelson support this effort by evaluating and ideally equipping company laptops/monitors with privacy filters, a low-cost step that could potentially prevent costly on-screen data leaks.

## Find the right screen privacy solution for your team

Have a question about our products? Need help finding the right size or type? We're here to help. Work together with 3M screen privacy experts to help you find the right solution for your organisation. Based on your work environment, we will provide our recommendations.

Learn more at **Screen Privacy and Protection | 3M UK**
or email at 3M-privacy-sales@mmm.com

1. The cost of data breaches. Thomson Reuters Law Blog. Published December 11, 2024. https://legal.thomsonreuters.com/blog/the-cost-of-data-breaches/
2. Windows 11 Benefits For Businesses | Ingenio Technologies. Ingenio Technologies. Published January 15, 2025.
3. Ponemon Institute Public Spaces Survey Study, 2017