The experts in screen privacy.

Stop. Think. Protect. That's our motto.

3M makes visual screen protection part of a comprehensive IT security policy.

Not so long ago, cybercrime was the domain of the solitary hacker committing identity fraud. Technology has shifted to usher in a landscape of hacking from global syndicates or nation-states.

Security experts discuss visual screen protection.

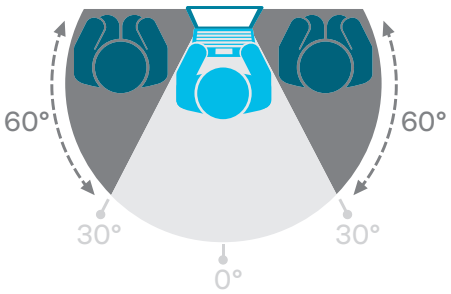
From publicly disclosed incidents, we know that more than 2.9 billion records were leaked in 2017.[1] Monetary losses due to data breaches continue to pile up; the FBI reports that U.S. victims were robbed of $1.42 Billion in 2017.[2] But money isn't the only thing at stake. Tactics like inserting ransomware have evolved to implanting ransomworms, which can cripple infrastructure.

The stakes have been raised, and the challenge faced by information security teams and their IT counterparts has never been greater. While we closely monitor networks, reinforce firewalls, and install patches, we may be ignoring a critical vulnerability — one that is staring us in the face — the sensitive information displayed on our computer screens.

Sooner or later, all data becomes visual and when it does, it's susceptible to visual hacking.[3]

"The resources behind the adversaries are often much greater than the resources of a company, making it an unfair playing field."

—John Brenberg, 3M Information Security Risk and Compliance



Zone of visual privacy.
Effective “black out” privacy from side views outside the 60-degree viewing angle.

Exposed screens can be hacked without sophisticated tools.

The next time you attend a conference or event, take a minute to look around and note the amount of exposed data displayed on phones and laptops. Anyone wandering by could snap a picture of a screen displaying sensitive data. It can happen in the blink of an eye. In the Global Visual Hacking Experiment, a white hat researcher walking through an office was successful in obtaining sensitive data 81% of the time.[4] Electronic data breaches typically leave a trail for forensics investigators to follow, whereas visual hacks may leave no trace.

A simple step toward keeping visual data private.

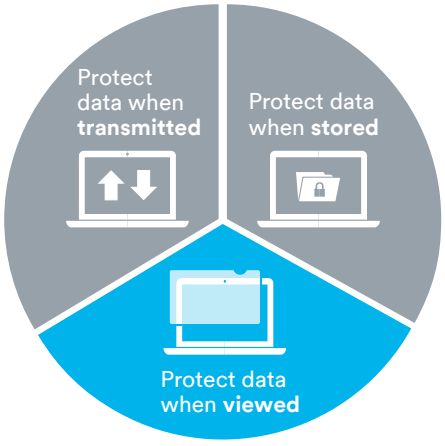
Inadvertently, or intentionally, insiders are responsible for around 30% of confirmed data exposures to unauthorized parties.[5] Consider the people that may go through an office building on any particular day — visitors, contractors, delivery persons, even employees from different departments. What can everybody see? And what is that information worth?

A low-cost solution exists.

A privacy filter attaches to a display and is designed for a user to have a clear view of their screen while blocking side views so that even someone sitting next to them won’t be able to read their data.

“Privacy filters are one of the last frontiers of IT security that IT professionals don’t think about — enough.”

—Ed Nelson, 3M Global PC Hardware Lead



Complete your IT security plan with 3M™ Privacy Filters

The privacy filter is like a firewall for the monitor.

3M and other Fortune 500 companies have begun to act. Much of the workforce switched from using desktop computers to using laptops more than 10 years ago. 3M IT security teams realized 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 intellectual property, trade secrets, communications and customer information. Now, every 3M U.S. employee receives a privacy filter with their laptop.

John Brenberg, 3M Information Security, Risk and Compliance, discusses data protection with his counterparts at other companies, he often observes that “they, like us, are overwhelmed with electronic security measures; let alone having bandwidth to take on the physical security measures of privacy screens.” John adds, “The attacks are relentless, and the threats are always changing.”

Get caught using screen protection.

Even for the leader in screen privacy solutions, 3M still struggles with getting employees to fully embrace and use privacy filters. Implementing consistent use of privacy filters across a large workforce can be challenging. Writing mandatory use into a company's information security policy is key, but changing human behavior to use them — and be fully compliant — is a continuous effort. Making the filters easy to use is important. It shouldn't be a cumbersome task to take them off 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 organization.

"Our people travel all over the world. Our workers are held to a high standard. We need to provide the tools that help them meet those high expectations."

—John Brenberg

Write screen privacy into policy.

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

—Privacy standard pulled from 3M internal guidelines

Consider your workspace. How easy is it to visually hack information?

The modern work environment has changed nearly as rapidly as information technology. Cubicle walls have shrunk over time, migrating staff from enclosures to open office environments. Office space architects are designing conference rooms with expansive glass windows, where meeting participants don't feel confined and trapped. Large format monitors can be easily visible from the halls or even outside on the street. If these screens are unprotected there may be unintended consequences. A company may discover too late that an early earnings report meant for the C-suite, became the talk of Wall Street when an inquisitive visitor wandered by.

IT managers and information security officers can work on solutions together. Take a walk through the building and take note of what can be seen on screens, especially in high traffic areas. Organizations where client data is displayed and collected — e.g., hospitals, airport terminals and even coffee shops — need to take extra precautions to ensure that personal and financial information is shielded.

Mobile employees need screen privacy too. Many people have experienced the annoyance of sitting in the middle seat on an airplane, laptop open, when they notice the passenger next to them staring at their screen. It's human nature to innocently glance at an exposed screen, but not everyone has innocent intentions.

87%

of office workers report they've caught someone looking over their shoulder at their laptop in a public place.[6]

Meet our 3M experts.

Ed Nelson

3M Global PC Hardware Lead

Ed Nelson has served in information security, project management and hardware procurement at 3M. In his current role, he tests and evaluates PC's, monitors and accessories for all global employees. Prior to this, he worked in endpoint security as the LANDESK administrator for global patch management where he maintained a 95% deployment rate of workstation patches within two weeks of patch release. Ed regards 3M employees as clients, and strives to provide high-performance computing tools that will support productivity while keeping valuable company data secure.

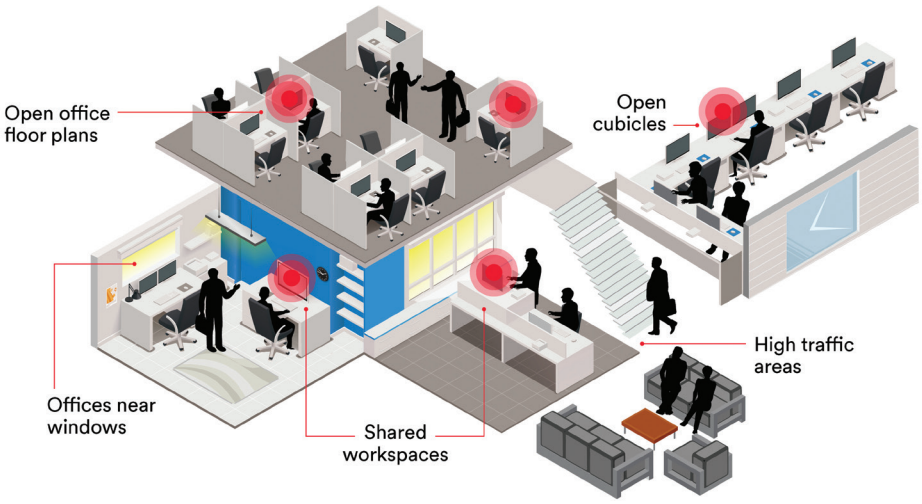
John Brenberg

3M Information Security, Risk and Compliance

John Brenberg has over 30 years experience spanning marketing research, system development, infrastructure management and information security and compliance across multiple business segments and processes. In his role at 3M in Information Security, Risk and Compliance, he has been responsible for leading programs for information security, compliance and risk, all for the protection of company and customer information, as well as for the protection of critical business processes. Brenberg credits his success to many strong internal partnerships across intellectual property, privacy, compliance and systems management.

3M | The experts in screen privacy.

Visual privacy risk areas



The value of a good reputation cannot be underestimated.

What we learn from newsworthy data breaches is that we need to be vigilant and help protect our valuable data both electronically and physically.

At 3M, IT hardware managers like Ed Nelson can and do assist in these initiatives. Their efforts may help deter hackers, address insider threats, and help prevent mobile related leaks by providing privacy filters with company issued laptops. It's a low-cost investment with the potential of saving millions of dollars of damage caused by unauthorized use of company information.

Have a question about our products? Need help finding the right-size or type?

We're here to help. Looking for a privacy product to evaluate? Work together with 3M screen privacy experts to find the right solution for your organization. Based on your work environment, we will provide our best practice recommendation.

Learn more at 3Mscreens.com or call 1-800-553-9215.

[1] IBM X-Force Threat Intelligence Index 2018
[2] FBI Internet Crime Complaint Center, 2017 Internet Crime Report
[3] Visual hacking is the practice of capturing sensitive, private, or confidential information for unauthorized use.
[4] Average based on global trials conducted by Ponemon Institute during the "Visual Hacking Experiment," 2015, and the "Global Visual Hacking Experiment," 2016, both sponsored by 3M.
[5] Reporting on 53,000 incidents and 2,216 confirmed breaches in 2017 – 2018 Data Breach Investigations Report
[6] Ponemon Institute Public Spaces Survey Study, 2017