Trend report 2025

The rise of the invisible colleague: **Shadow AI**

AWARE WAYS

Summary

This trend report shows that **Shadow AI** is no longer an isolated incident, but a dominant reality. Figures show that the click rate on AI-related phishing simulations has increased fivefold in two years. The cause is not malicious intent of employees, but the desire to work faster and more efficiently.

Insights

1. **The gap between knowing and doing**: Employees score high on theoretical knowledge (**89%** know the rules), but fail in practice. More than half (**56%**) are guided by the 'Halo-effect': if a website looks professional, its security is overestimated. This leads to **54%** installing new tools without consultation.
2. **An explosive new risk**: While traditional shadow IT (such as WeTransfer) remains a stable risk, the threat from AI is growing exponentially. The number of employees clicking on ChatGPT-related phishing emails has increased **fivefold** in two years (from 1,2% to 6,8%).
3. **From banning to resilience**: The traditional reflex of 'blocking and prohibiting' is counterproductive and can even lead to a loss of talent. Complete control is an illusion. The solution lies in increasing **AI literacy**: employees must not only learn which buttons to press, but above all how to assess risks.

Conclusion

Humans are not the weakest link, but rather the key to unintentional AI use. By facilitating employee curiosity within safe frameworks, we transform Shadow AI from an invisible risk into a safe force for innovation.

While organizations secure the front door, employees unintentionally open the back door.

Why **Shadow AI** is the new reality for every organization

Modern employees no longer wait for permission from the IT department. They 'hack' their own productivity. While IT departments and security officers secure the front door with firewalls and policies, enthusiastic colleagues unintentionally open the back door via unauthorized AI tools. Often without malicious intent, but driven by efficiency. They want to do their work faster and better. And if the internal tools cannot offer that speed, they look for the solution outside the organization.

This phenomenon is also known as '**Shadow AI**'. It refers to the use of artificial intelligence tools and applications by employees without these being explicitly approved or managed by their own organization (IBM, 2025). This 'shadow' use therefore often falls outside the reach of IT and security teams and leads to invisible risks.

Revolution from below

Where digital transformation was initially a process driven from the top of an organization, we are now seeing a revolution starting from the bottom. Employees are taking control themselves and experimenting more and more with new technologies.

By 2025, Shadow AI will have grown from an incidental problem to a dominant reality within organizations:

- Figures from Microsoft and LinkedIn (2024) show that 75% of employees already use AI tools.
  - Of this group, no less than 78% say they use **unauthorized** AI tools for work-related tasks (Figure 1).
- **Among security leaders, 68% admit that AI is being used within their teams outside of official frameworks (Upguard, 2025).**
- Gartner has placed Shadow AI in the top 5 emerging business risks (Gartner, 2024).

Productivity over policy

There is usually no malicious intent behind employees' independent use of AI tools. It often stems from a strong motivation to do their work better and faster. Employees see AI as an important tool for efficiency. **Nearly half of users believe that using unapproved tools is justified because it simply makes them more productive (Invicti Security, 2025).**

Banning AI drives away talent

The old reflex of prohibiting and blocking no longer works. In fact, ignoring the need for AI tools poses personnel risks: 54% of new employees indicate that access to AI influences their choice of employer (Microsoft & LinkedIn, 2024). Organizations that try to hold back AI risk losing talent and falling behind the competition.

The invisible majority: Nearly 60% of all employees use AI outside the organization's view.

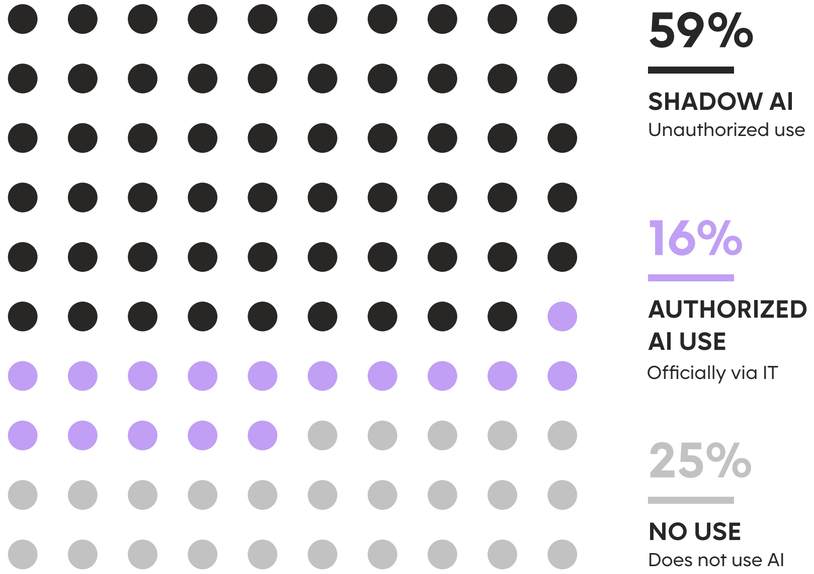


Figure 1.

Invisible risks

Although employees' intentions are good, the unregulated use of AI tools creates a blind spot. **IT teams have visibility into less than 11% of the AI applications** actually running within the corporate network (LayerX Security, 2025). This means that sensitive data or personal information can be unintentionally entered into public AI models when generating presentations, code, or emails.

Dangers of 'free'

At Awareways, we are seeing clear signs from the market that explain this trend. On the one hand, enterprise licenses for secure AI environments are expensive. For many organizations, it is not financially feasible to arrange a paid license for every employee. The result? Employees who see the possibilities of AI use free, public versions.

On the other hand, our conversations and data show that the problem also lies in a lack of awareness.

Employees often simply do not realize that the "free" version of a tool has completely different conditions regarding data processing than a paid enterprise version. They see a tool that makes them more productive, rather than the risk behind it. And that is the biggest problem, because AI tools continue to pop up everywhere, and without awareness, the use of "free" tools will only grow.

From control to resilience

The rise of Shadow AI is forcing many organizations to fundamentally rethink information security. For a long time, control was the starting point. But in a reality where the majority of employees actively seek their own solutions, complete control is an illusion.

At Awareways, we do not see this trend as a threat that needs to be suppressed, but as an opportunity that we need to steer in the right direction.

An employee who uses ChatGPT for a report, for example, is eager to learn and solution-oriented. The problem is often not the tool or the person, but the lack of the right frameworks that enable safe experimentation.

The focus should be on increasing resilience and facilitating safe use. This means that we must not only teach employees where their data is currently stored, but also where this data goes when they use a tool. By looking at where employees' strengths lie and where they need support, we can turn an invisible risk into productive collaboration.

IT teams have visibility into less than 11% of AI applications, according to estimates.

The psychology behind Shadow AI

To better understand this phenomenon, we look beyond technology in this trend report. As in our previous trend report, we use insights from social psychology. We use the structure in Figure 2, based on the Theory of Planned Behavior (Ajzen & Schmidt, 2020). This psychological model assumes that behavior is not random, but the result of a logical process in our brain.

Theory of Planned Behavior.

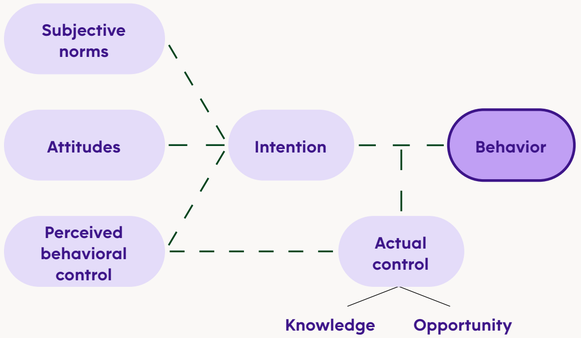


Figure 2.

Everything starts with **intention**: does the employee *intend to* exhibit the behavior? This intention is shaped by three psychological processes:

- **Attitude**: What does the employee themselves think about the behavior? In the case of Shadow AI, we often see a conflict here. The employee considers security important ("*I don't want to leak data*"), but also considers efficiency important ("*I want to perform this task quickly*").
- **Subjective norms**: What does the employee think others expect? For example, if colleagues all use ChatGPT and the manager insists on quick results, social pressure arises that leads to "unsafe" behavior.
- **Perceived behavioral control**: Does the employee believe they can do it? ("*I am smart enough to judge whether this site is safe*"). This self-confidence can sometimes be misplaced, which can lead to risks.

Even with the best intentions ("*I want to work safely*"), things can go wrong if the right resources are lacking. We call this **actual control**. It consists of two parts:

- **Knowledge (Internal)**: Does the employee really know how things work? Does anyone understand the difference between an enterprise license and a free account? Or are they basing their assumptions on guesswork ("The site looks professional, so it must be fine")?
- **Opportunity (External)**: Does the organization facilitate safe behavior? Is a safe AI tool available and approved? If the organization does not offer an alternative (no budget, no policy), it becomes difficult for employees to work safely and efficiently, no matter how much they want to.

The stronger all these factors are, the greater the chance that you will turn your intention into actual **behavior**.

The three pillars

This model helps us understand why employees do what they do by looking at these factors that drive our behavior. In this report, we will focus on the three main pillars of this model:

- **Saying (Intention)**: What are employees planning to do? Do they want to work safely and do they understand the importance of this? Here we look at employee motivation and perception.
- **Knowing (Actual control)**: Do employees have the right knowledge and resources? Do they understand the difference between a safe and unsafe tool, and does the organization facilitate this?
- **Doing (Behavior)**: What actually happens in the workplace? Do intentions and knowledge match actions, or do we see different behavior?

This way of looking at Shadow AI shifts the focus from controlling and prohibiting to understanding and empowering.

What do employees say?

While global reports offer a macro perspective on Shadow AI, data from our own Culture Scan questionnaires show how this behavior manifests itself in the workplace. We analyzed 33,690 responses from employees at various organizations regarding baseline measurements and follow-up measurements. The results reveal a fascinating difference between "old" and "new" awareness.

Safe emailing, but not safe prompting?

The crux of Shadow AI is that innovation moves faster than policy. This is clearly reflected in the figures. In response to the statement "*I consult with the security team before I start using new software (such as AI),*" less than half (46%) of respondents in the baseline survey said they do so.

This means that in organizations that are just starting a security awareness program, as many as 54% of employees do not take the standard step toward security. Of these, 29% are neutral and 25% even say explicitly that they do not do so (Figure 3). This confirms the image that employees independently introduce tools to speed up their work.

However, there are signs of progress. In the follow-up measurement, we see the percentage of employees who consult with security rise to 55%. A substantial group (45%) continues to skip consultations with security or fails to take an active approach, but a positive trend is evident when attention is given to this issue through a security awareness program (Figure 4).

Saying | Knowing | Doing

The new blind spot: More than half of employees implement tools without conducting a security consult.

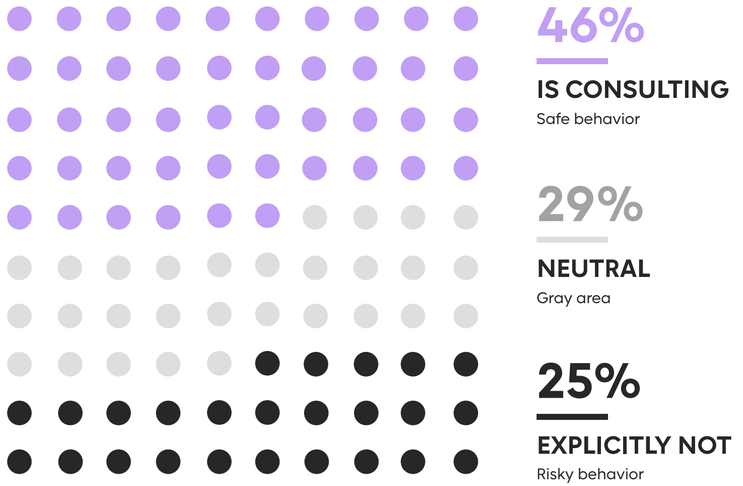


Figure 3.

The positive trend: Awareness programs are leading to visible growth in safe behavior.

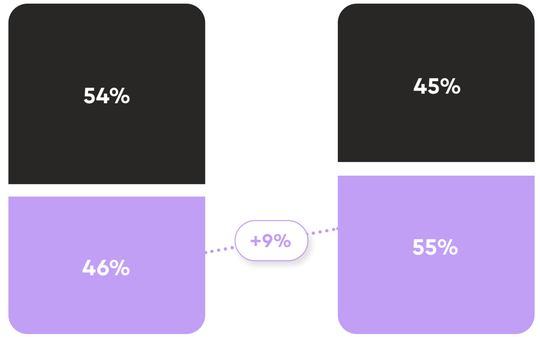


Figure 4.

What do employees say?

AWARE WAYS

The comparison with the more “traditional” form of shadow IT is quite interesting. After all, most employees seem to be well aware that they shouldn’t transfer work data to their personal devices.

Most respondents reacted positively to the statement “I never share files between my work and personal accounts” (Figure 5).

- In the baseline survey, 67% of respondents indicated that they never do this.
- In the 1-measurement, this figure remained at 67%.
- It then rose to 74% in the 2-measurement.
- In the 3-measurement, as many as 89% indicated that they do not share files with private accounts.

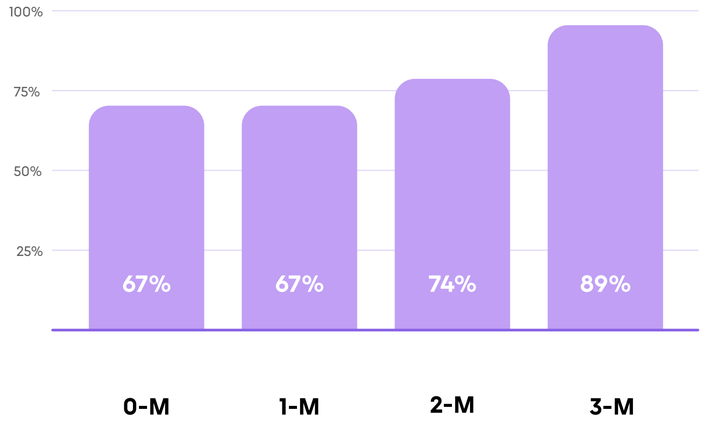
The new blind spot

These figures provide important insights for security officers and policymakers. Most employees now recognize that “old” data leaks, such as sending an Excel file to their personal email, constitute inappropriate behavior.

But the real risk in the coming period lies in how this is interpreted. An employee who would never send a file to their personal email for security reasons might still copy that same text into a public AI tool to generate a summary. From the employee’s perspective, this isn’t “sharing a file,” but “using a tool.”

The discrepancy between what employees say they do when sharing files and what they actually do when using a new AI tool confirms that we need to shift our focus. **We must not only teach employees where data is stored securely, but above all make them aware of the risks involved when they enter that information into external AI tools.**

Traditional Shadow IT: Sharing files using personal accounts is widely recognized as undesirable behavior.



89%

SAFE BEHAVIOR

Never shares anything with personal account

Figure 5.

Saying | Knowing | Doing

What do employees know?

While the Culture Scan tells us what employees say they do, we use the data from our Wave training sessions to dIve deeper into their actual knowledge. Do employees actually know what the rules are? The results of 38,642 responses from our interactive microlearning modules paint a promising but complex picture.

A strong theoretical foundation

First, the good news: the basic knowledge is remarkably strong. When we ask employees what they should do if they want to use a new application, a majority of 89% choose the correct process: submitting an official request to the IT department or through the service desk (Figure 6).[1]

Awareness of the risks associated with unauthorized tools is also high in theory. In scenarios where colleagues use unapproved software, 90% of respondents correctly note that this makes it easier for information to fall into the hands of malicious actors. Employees therefore understand that using shadow IT carries risks.

A "reliable" website

If awareness of these processes is so high (89%), why does the Culture Scan show that only 46% to 55% of employees actually consult with security before deploying new software?

The answer lies in a specific knowledge gap revealed by the Wave data. When asked whether an app can be safely downloaded from a website that "looks trustworthy," only 44% gave the correct answer ("*via an IT request*").[2]

This means that more than half of employees (56%) base their judgment on a website's appearance or their own assessment of its reliability. This phenomenon is known in psychology as the *Halo effect* (Nisbett & Wilson, 1977): if one aspect of something is judged positively (a professional-looking website), we wrongly assume that other aspects (the safety of the download) are also in order (Figure 7).

Theory vs. Practice: We have the knowledge, now we need to put it into action.

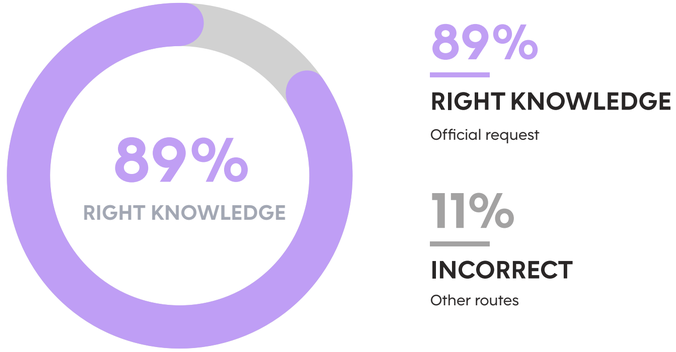


Figure 6.

The Halo Effect: A professional appearance often takes precedence over safety **procedures.**

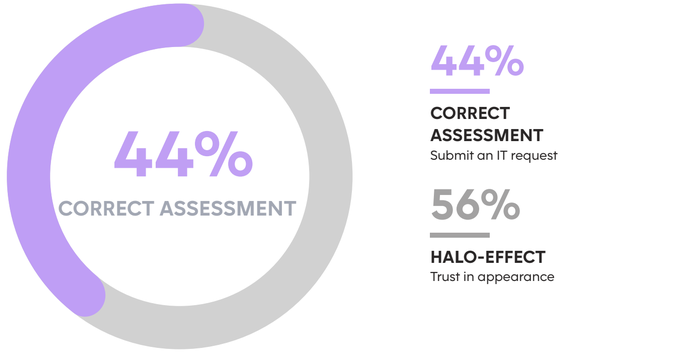


Figure 7.

Saying | Knowing | Doing

[1] *The questions and answer options are tailored to the organization's procedures.*

[2] *The questions and answer options are tailored to the organization's procedures.*

What do employees know?

AWAREWAYS

The gap between knowing and doing

Here we see that knowing something does not necessarily mean doing it (Figure 8):

1. **The Knowledge** (Wave): Employees know: "I need to ask for official permission" (88%).
2. **The Pitfall** (Wave): Employees think: "*This specific tool looks reliable, so it must be safe*" (56% incorrect assessment).
3. **The Behavior** (Culture scan): Employees act: They install the tool without consulting anyone (54% in 0-measurments).

Note: These figures come from different data sources and may not represent the exact same population. However, these data sources do show a similar pattern.

The employee does not view themselves as a rule-breaker in this situation. Because the website looks trustworthy, the employee does not mentally label this action as "Shadow AI" or "risky behavior," but rather as "proactive work." This also explains why the term "Shadow IT," which is closely linked to Shadow AI, itself causes confusion. Only 62% were able to provide the correct definition of "Shadow IT" in the Wave microlearnings.

The illusion of control

The data shows that the basic rules regarding requesting consent are clear; 89% are already aware of this. The challenge for 2026 lies in shaking off the illusion of control among employees. We shouldn't be teaching employees what the rules are, but rather why their own judgment of what constitutes a "trustworthy website" is no longer sufficient in the age of AI.

Knowledge doesn't protect: Despite high levels of knowledge, the halo effect leads to risky behavior.

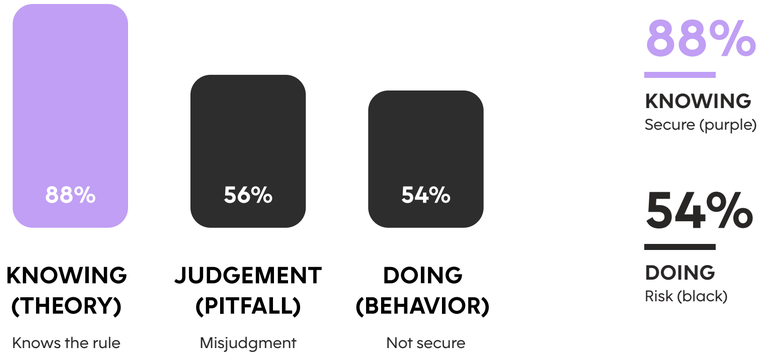


Figure 8.

The challenge for 2026 lies in shaking off the illusion of control among employees.

Saying | Knowing | Doing

What do employees do?

AWARE WAYS

While the intentions and insights from the previous chapters tell us what employees say they do, the results of our phishing simulations reveal what actually happens in the hustle and bustle of the workday. The results of our simulations, which involved 132,044 recipients, show an interesting trend that aligns with the Culture Scan and Wave data.

Knowing is not (yet) doing

In the Culture Scan, we found that 67% of employees already claimed in baseline measurements that they never share files via personal accounts. In the 3-measurement, this figure was as high as 89%. They know it's not allowed. The phishing simulation figures show a different picture. In emails simulating that a file is ready via WeTransfer (classic Shadow IT), an average of 15.6% of recipients click on the link. This underscores the assumption that knowing does not equate to doing.

The Rise of the AI Clicker

The trend we're seeing with Shadow AI (based on ChatGPT templates) is even more interesting. While we've observed a stable average click-through rate of 15.6% at WeTransfer for years, we're seeing a type of adoption curve with Shadow AI.

In Q1 2023, the click-through rate on ChatGPT emails was low (1.2%). AI was still new, unfamiliar, and may have been viewed as irrelevant. **In two years, this click-through rate increased fivefold to 6.8% in Q1 2025.** The trend line is clearly visible (Figure 9). And that was already a year ago. Since then, AI has only continued to grow in popularity.

Although the overall average click-through rate for ChatGPT (5.4%) is still lower than that of WeTransfer (15.6%), the growth in AI click-through rates has been explosive. This confirms the trend that employees are embracing AI to boost efficiency. They are on the lookout for tools, updates, and opportunities.

Adoption curve: Employees are increasingly embracing AI, which is leading to a growing risk.

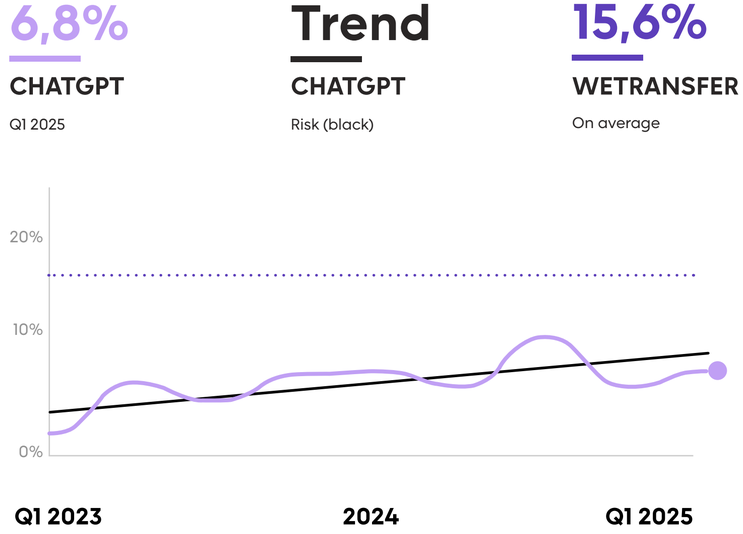


Figure 9.

Saying | Knowing | Doing

What do employees do?

AWARE WAYS

The ‘Curiosity Gap’

The rising number of clicks on AI-related phishing emails can be explained by the Curiosity Gap Theory (Loewenstein, 1994). Employees are convinced that AI makes their work easier (Invicti Security, 2025), but often do not (yet) have access to it through official channels.

When an email appears promising: “Activate your license here” (Figure 10), this email bridges the gap between what employees want to use and what they can currently use. The email taps into their motivation to be more efficient. Because, as we saw in the Wave data, employees struggle to assess the reliability of websites and apps (due in part to the Halo effect), a compulsion to click arises.

A changing risk profile

The data shows that employees are vulnerable on two fronts, but for different reasons:

- **Old behavior (Shadow IT)**: Habitual behavior and curiosity about files, even though they know it’s not allowed.
- **New behavior (Shadow AI)**: A desire to learn and a wish to work more efficiently. This risk is growing by the month.

For security awareness, this means we must not only focus on “hover, check, decide,” but also on addressing the need. If there is no secure alternative for sharing large files or using AI tools, employees driven by their ambition will continue to click on not secure links.

Curiosity Gap: a phishing email that capitalizes on the need for AI tools to bridge the gap between desire and official access.

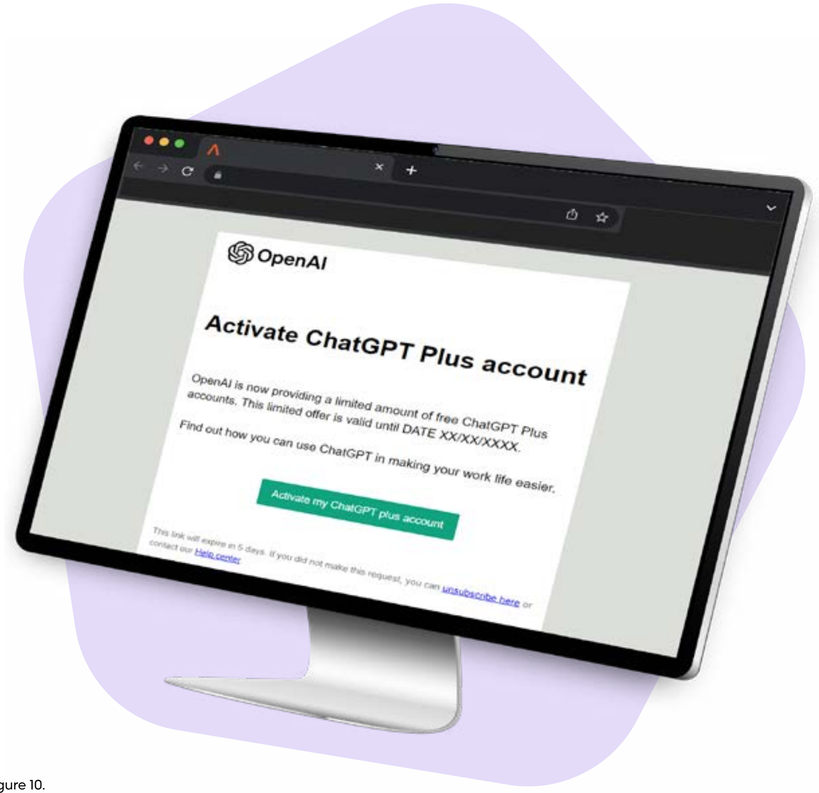


Figure 10.

Saying | Knowing | Doing

Conclusion

From an invisible risk to a visible strength

The rise of the "invisible colleague" is irreversible. This trend report shows that Shadow AI is not a passing fad, but a structural shift in the way we work. The numbers speak for themselves: with 78% of employees using AI tools on their own initiative (Microsoft & LinkedIn, 2024), digital transformation is no longer a process driven solely from the top down, but rather one that originates from the bottom.

Saying, Knowing, and Doing

Through the lens of the Theory of Planned Behavior (Ajzen & Schmidt, 2020), we see an interesting dynamic emerging between the employee's ambition and the organization's security:

- **Saying (Intent)**: The employee's intent is positive. The use of Shadow AI stems from a strong desire to be more efficient, not from malice. However, the automatic reflex to involve security when introducing new tools is still too often missing. Nearly half of employees skip this crucial step.
- **Knowing (Actual control)**: In theory, awareness is high; 88% know they need to ask for permission. In practice, however, we see that employees are misled by the "Halo effect": if a tool looks professional, they skip the mental security check.
- **Doing (Behavoir)**: The knowledge gap leads to risky behavior. The "Curiosity Gap" is causing employees to increasingly click on phishing emails that capitalize on their need for AI tools. The percentage of people clicking on such emails has increased fivefold in just two years.

AI literacy

The conclusion is clear: in an era where innovation outpaces policy, total control has become an illusion. Simply banning tools is counterproductive and can even lead to a loss of talent (Microsoft & LinkedIn, 2024).

The solution lies in shifting the focus from *control* to *resilience*. This applies not only to Shadow AI but also to the use of approved licenses. Because even with a secure, paid tool, the risk of data breaches remains if employees don't know how to classify data.

The challenge for 2026 is therefore not technical, but human. We must harness the power of the employee through **AI literacy**. We must not only teach employees which buttons not to press, but rather teach them how to assess a tool's reliability and how to classify data securely.

Bring AI out of the shadows: by facilitating experimentation, we turn invisible risks into safe development. In this context, the employee is not the problem, but the solution to safe and effective AI use.

List of References

Ajzen, I., & Schmidt, P. (2020). Changing Behavior using the Theory of Planned Behavior. In M. S. Hagger, L. Cameron, K. Hamilton, N. Hankoren, & T. Lintunen (Eds.), The handbook of Behavior Change, 17-31. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/9781108677318.002

Gartner. (2024, 21 oktober). Gartner Identifies the Top 10 Strategic Technology Trends for 2025. Gartner Newsroom. Geraadpleegd van: https://www.gartner.com/en/newsroom/press-releases/2024-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2025

IBM. (2025, november). What Is Shadow AI? IBM Topics. Geraadpleegd van: https://www.ibm.com/think/topics/shadow-ai

Invicti Security. (2025, 29 september). Shadow AI: Risks, Challenges, and Solutions in 2025. Geraadpleegd van: https://www.invicti.com/blog/web-security/shadow-ai-risks-challenges-solutions-for-2025

LayerX Security. (2025). Enterprise GenAI security report 2025: Exposing hidden AI security blind spots. Geraadpleegd van: https://go.layerxsecurity.com/enterprise-genai-security-report-2025

Loewenstein, G. (1994). The psychology of curiosity: A review and reinterpretation. Psychological Bulletin, 116(1), 75–98. https://doi.org/10.1037/0033-2909.116.1.75

Microsoft & LinkedIn. (2024). 2024 Work Trend Index Annual Report: AI at Work Is Here. Now Comes the Hard Part. Geraadpleegd van: https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part

Nisbett, R. E., & Wilson, T. D. (1977). The halo effect: Evidence for unconscious alteration of judgments. Journal of Personality and Social Psychology, 35(4), 250–256. https://doi.org/10.1037/0022-3514.35.4.250

Upguard. (2025, 10 november). New Research from UpGuard Reveals 68% of Security Leaders Admit to Unauthorized AI Usage. Geraadpleegd van: https://www.upguard.com/press/new-research-from-upguard-reveals-68-of-security-leaders-admit-to-unauthorized-ai-usage

Colofon

Title: Trend Report 2025: The Rise of the Invisible Colleague: Shadow AI
Published by: Awareways
www.awareways.com

Author: Sjoerd van Veldhuizen, MSc
Co-authors: dr. Jan-Willem Bulée & Remy Dijkstra, MSc
Editing and final editing: Leon Baauw
Design and layout: Bruna da Silva Gerage

Publication date: March 2026

Contact:
Email: info@awareways.com
Telephone: 030 227 14 67

Human resilience is not about avoiding risks, **but about building strength.**

Contact details
www.awareways.com
info@awareways.com
030 227 14 67