Insights on Employee Cybersecurity Behavior

Edition 1, 2026

"Security isn't competing with apathy; it's competing with priorities."

Aware Force®

Table of Contents

What Employees Tell Us

This isn't another dry security report. It's a live look at what employees across a wide range of organizations are thinking about cybersecurity.

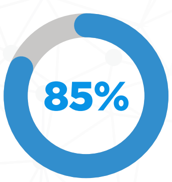
Based on over 9,000 responses from Aware Force readers in recent months, this report reveals where employees are engaging in cyber, where they're overlooking important steps, and what they think about AI.

Readers tell us they're worried about cyber threats, but the data shows something very different: their concerns aren't translating into action.

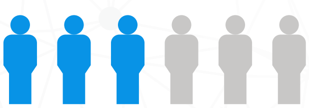
That "action gap" is where the real danger to your organization lives.

The Three Top Takeaways

1. "I'm concerned… but I haven't done anything."
Many want security, few follow through.



85% say they're concerned about AI-enabled smart home devices.



Nearly half have not recently checked the privacy settings.

2. "My passwords are strong… but not unique."
Confidence does not match behavior

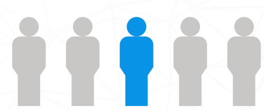
Most respondents feel they create strong passwords, but 37% struggle to maintain unique credentials, and only 19% use a password manager.

19% use a password manager.

3. "I don't trust what I see online… but I still click."
Trust is eroding, but behavior hasn't changed.

Readers know AI-generated content is increasing.

Yet 1 in 5 cannot reliably identify it, and 15% have already been misled.



1 in 5 cannot reliably identify AI-generated content

Warnings Heard, Habits Unchanged

Employees are not ignoring cybersecurity – they're navigating it without clear guidance or consistent habits. Here's what hard data shows:

AI awareness is rising, but support is not

63% are concerned about AI-driven cybercrime

65% believe AI will enable impersonation

58% report no training on AI-related risks

Unmanaged tools are creating exposure

80% use SaaS or AI tools without IT approval

67% bring personal apps into work environments

50% use unapproved AI tools

55% 55% connect them to work systems

Traditional approaches are not working

50% lack access to or do not engage with training

Security communications are frequently ignored

What This Requires

Awareness alone isn't enough. Organizations need:

- Continuous, behavior-focused reinforcement
- Real-world scenarios that employees recognize
- Simple, repeatable actions

How Aware Force Closes the Gap

Aware Force turns real-world threats and live behavioral data into short, interactive experiences that move employees from:

"I should do something." → *"I just did."*

Making Security Stick

Closing the gap between awareness and action requires more than traditional training; it requires content that employees can understand and apply in the moment.

The most effective approaches avoid complex language, focus on real-world situations, and reinforce simple, repeatable behaviors over time.

At Aware Force, we design content that reflects how employees think and make decisions. Instead of "check-the-box" training, we use clear, practical scenarios to help employees recognize risks, understand what matters, and build habits that carry into their daily behavior.

AI and Privacy

Employees see the risks with AI, but they're not acting consistently.

Smart Home Devices:

Big worry, little follow-through

85% say they're concerned about AI-enabled smart home devices.

48% haven't checked or updated their privacy settings in recent months

That means more always-on microphones, cameras, and connected devices sitting wide open where work and personal data intersect.

AI-Generated Content:

Awareness without confidence

19% of users admit they cannot reliably distinguish AI-generated content from reality

15% admit they have mistaken AI images or advertisements for real content

What this shows

Awareness is not translating into action. This disconnect is creating greater risk as AI-enabled tools and connected devices become more embedded in daily life.

What Actually Works

Reducing AI-related risk requires more than awareness—it requires action.

The most effective approaches make AI risks easy to recognize in real-world situations, reinforce small, repeatable behaviors, and provide clear actions employees can take immediately.

At Aware Force, we translate emerging AI threats into short, practical scenarios that help employees recognize risks and act in the moment. Whether reviewing device settings or identifying manipulated content, the goal is simple: build confidence and turn awareness into consistent action.

The Password Gap

Employees Are Improving—but Risk Remains Higher Than Expected

Most employees understand that passwords matter, but behavior hasn't caught up. Manual habits persist, creating ongoing exposure to credential theft and account compromise.

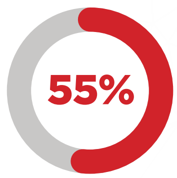
Where password behavior breaks down

37% say using a unique password for every account is the most difficult security habit

27% struggle to keep old passwords updated

19% find it hardest to remember long, complex passwords

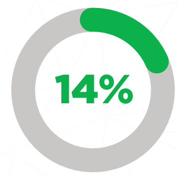
What employees actually do



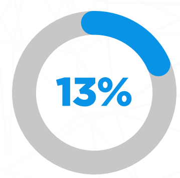
55% manually track passwords instead of using a secure tool

Only 19% use a password manager

Risky habits that persist



14% reuse the same password across multiple accounts



13% only change passwords when required

What this shows

Password risk is not a knowledge gap; it's a usability and behavior gap. Employees default to the easiest option, even when they understand the risk.

What Actually Works

Reducing password-related risk requires more than reminding employees what to do – it requires making secure behavior easier than the alternatives.

The most effective approaches focus on simplifying decision-making, reducing friction around secure tools, and reinforcing small, repeatable actions over time.

At Aware Force, we translate password best practices into short, snackable content that shows employees how to adopt secure habits in real situations, whether creating unique passwords or using a password manager. The goal is to make secure behavior the default, not the exception.

Competing Digital Priorities

Security Is Competing...and Often Losing

Employees are not ignoring cybersecurity, but they are prioritizing other aspects of their digital lives. If security doesn't fit into those priorities, it will likely get ignored.

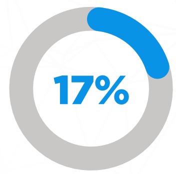
What employees say they want to change

44% say reducing screen time is a top goal

Only 10% prioritize installing a password manager

Where attention is focused

18% want to cancel unused subscriptions



17% want to learn how to use AI to be more productive: this is framed as lifestyle or career upgrades rather than security moves

What this shows

Security is not competing with apathy; it is competing with priorities. Employees are actively trying to improve their digital lives, but security is not actually part of that effort.

What Actually Works

Security efforts are most effective when they align with employees' existing priorities...not when they compete with them.

The strongest approaches position security as part of productivity, digital wellbeing, and everyday decision-making, rather than as a separate task.

At Aware Force, we focus on integrating security into the platforms and behaviors that employees already use. This includes highlighting risks in social media environments, demonstrating how default settings create exposure, and using short-form video to show how everyday actions can impact security.

Risks of Mobile Gaming

Everyday Behavior Is Creating Continuous Exposure

Mobile app risk is not hidden. It is constant, visible, and largely ignored.
Employees encounter aggressive prompts, misleading ads, and excessive permission requests regularly, yet security decisions are often made quickly and without review.

How people think about app security

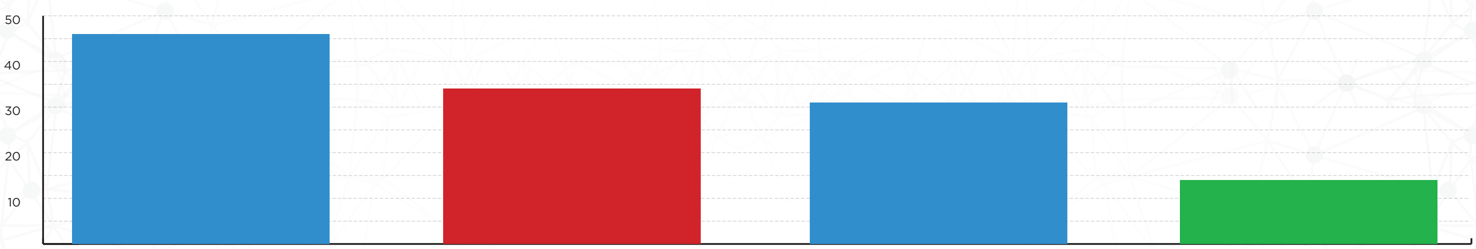
Only 20% consistently review and manage their app permissions

17% don't actively consider security at all

47% say they're aware of mobile security but admit their behavior is inconsistent

11% openly prioritize convenience and features over protection

What they're exposed to in mobile games



46% **encounter in-app purchase prompts or upsells**

34% **report misleading or aggressive ads or messages**

31% **encounter apps that ask for more access than expected**

14% **have been asked to share personal information**

What this shows

Mobile risk is not a rare event – it is part of the everyday user experience.
Employees are making frequent, low-friction decisions that collectively increase exposure over time.

What Actually Works

Reducing mobile app risk requires addressing the way decisions are made in real time, not just increasing awareness.

The most effective approaches focus on helping employees recognize common patterns such as aggressive prompts, unnecessary permission requests, and misleading interactions, while reinforcing simple, repeatable behaviors.

At Aware Force, we tackle security risks through engaging video content, informative infographics, or even cyber games that encourage employees to slow down, recognize risk, and make better decisions as they happen. App safety isn't glamorous, but we help employees see how simple actions lead to big security gains.

From Insight to Action

Aware Force uses real-world behavioral data to design cybersecurity content that aligns with how employees actually think, work, and make decisions.

What drives behavior change

Make the secure choice the easy choice
Employees adopt secure tools when they are clearly easier than the existing habits, not just more secure. We use step-by-step guides, quick comparisons, and real-world scenarios so the secure option feels like the obvious, low-effort choice.

Align security with real priorities
Security is more effective when it aligns with employees' existing goals. When employees see that "locking down accounts" sits next to "decluttering their phone," they're far more likely to act.

Making emerging risks recognizable
Abstract AI threats like AI scams become actionable when employees can identify them in real-world situations. We use concrete stories, short scenarios like Spot the Fake challenges, and side-by-side examples to build a mental library they can draw on later.

Simplify decisions into clear actions
Complex settings and permissions are more likely to be addressed when broken into small, manageable steps. Clear before/after examples to show exactly what changes and why they matter, so people feel confident clicking through screens they used to ignore.

Address behavior beyond the workplace
Mobile apps, social platforms, and family device use all influence workplace risk and must be part of the conversation: What kids tap on, how free games make money, and why "Allow" shouldn't be automatic. We use relatable framing that makes people more protective and more willing to review permissions, unsubscribe, and push back on manipulative prompts.

Reinforce habits over time
Behavior change happens through consistent, repeatable exposure, NOT once-a-year training. Aware Force content is delivered in small, snackable doses delivered twice a month: quizzes, polls, short videos, and "what would you do?" questions that employees come back to.

Use real feedback to stay relevant
Ongoing audience input ensures content reflects current behavior and preferences, not assumptions. We use ongoing polls, up- and down-vote systems, and open-ended questions to learn where employees are confused, anxious, or curious, and then adjust our topics, tone, and tools in response. That feedback loop means our next piece is always shaped by what employees have told us, not by a static annual plan.

That's why Aware Force content doesn't just land in inboxes: it becomes something people talk about, share, and remember when it really counts.

Contact Us

Ready to close the gap between awareness and action?

Aware Force helps organizations turn employee behavior into a measurable security advantage—at work and at home.

Start the conversation

Contact: Jeff Brown
jeff@awareforce.com
awareforce.com

Bring behavior-based security awareness to your team.

Aware Force®

Aware Force®