KnowBe4

Security Approaches Around the Globe: The Confidence Gap

Are Employees as Scam-Savvy as They Think?

In an increasingly digital world, cybercriminals are evolving their tactics faster than ever. But as organizations work to keep up, a critical question remains: Do employees really know how to spot a cyber threat? According to our latest research, 86% of employees believe they can confidently identify a phishing email. However, as we delve deeper into the numbers, a troubling paradox emerges—confidence does not always translate to competence.

The Overconfidence Illusion

Across the UK, USA, Germany, France, Netherlands, and South Africa, we surveyed professionals who work primarily on laptops to assess their cybersecurity habits. The results paint a fascinating yet alarming picture of regional differences in perceived scam-detection abilities. While confidence in spotting phishing attempts is highest in the UK and South Africa (91%), it plummets to just 32% in France. The most unsettling finding is that even in countries where employees exude confidence, their susceptibility to scams remains high.

EXPERT INSIGHT

Javvad Malik, Lead Security Awareness Advocate

The significant variation in confidence levels across regions regarding cyber threat identification stems from a complex interplay of factors. Cultural differences in risk perception and self-assessment play a crucial role, as do the quality and frequency of cybersecurity awareness training programmes. Exposure to cyber threats, regulatory environments, and media coverage of security issues also contribute to these disparities. Technological infrastructure, digital literacy, and language barriers in non-English speaking countries further shape regional differences. Corporate culture, historical context of cyber incidents, and socioeconomic factors affecting education and access to technology round out the influential elements.

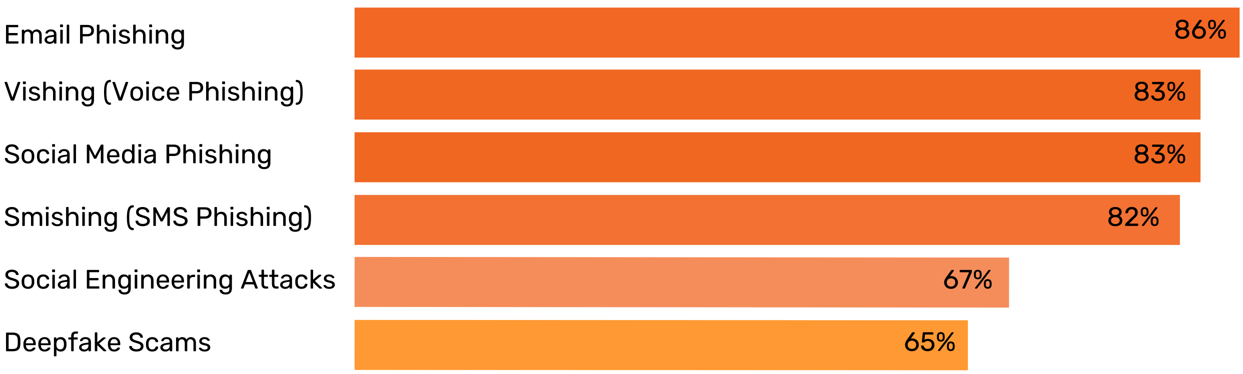
The differences suggest a need for tailored, culturally sensitive cybersecurity training approaches. This disparity also underscores the importance of not relying solely on self-reported confidence levels when assessing cybersecurity preparedness. Instead, actual performance in simulated phishing tests may provide a more accurate picture of employees' abilities to identify and respond to social engineering attempts.

Who Overestimates Their Abilities the Most?

While regional differences are notable, other patterns emerge. Men report higher confidence in detecting scams than women, a potential reflection of exposure to cybersecurity training or perceived digital literacy. Meanwhile, younger employees (25- to 34-year-olds) feel the most capable across nearly all scam types, except when it comes to deepfake scams, where their confidence aligns with 16- to 24-year-olds.

Confidence Levels by Scam Type

Across all demographics, confidence levels fluctuate based on the type of scam. Employees feel most prepared to detect traditional cyber threats but struggle with more sophisticated deception tactics:



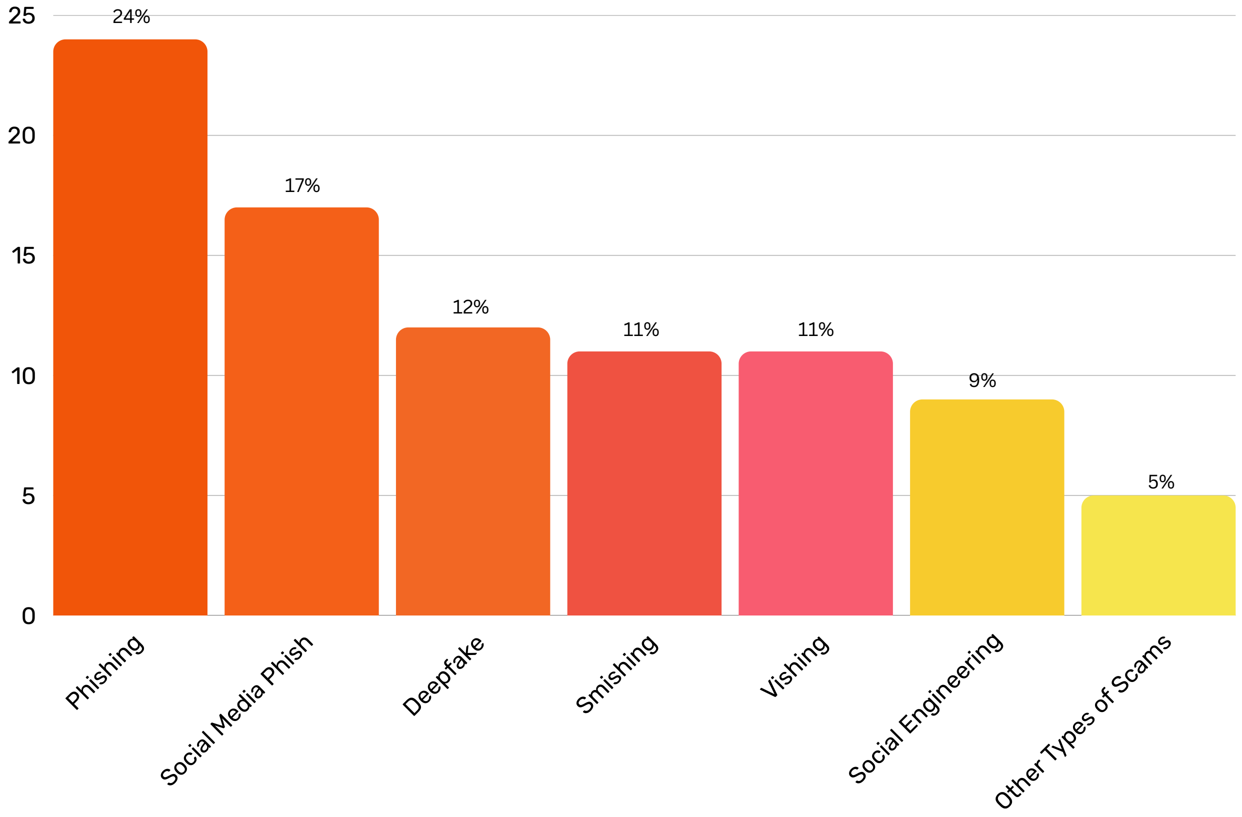
While confidence in detecting email phishing, vishing, and smishing remains high, it drops significantly for more complex social engineering tactics. Social engineering attacks (67%) demonstrate that employees struggle with manipulation-based tactics that exploit the human mind rather than obvious red flags. Deepfake scams (65%) pose an even greater challenge, as AI-generated deception becomes increasingly difficult to recognize.

Perception vs. Reality: How Many Employees Actually Fall for Scams?

If confidence levels were an accurate measure of preparedness, we'd expect low victimization rates. Instead, the data tells a different story—almost 50% of employees have fallen for a cyber attack:

- 24% fell for a phishing attack
- 17% were tricked by social media scams
- 12% were fooled by deepfake scams

Percentage of Respondents who have Fallen for Cyber Attacks



The regional differences are particularly notable. South Africa stands out with the highest confidence but also the highest rate of scam victims, with 68% of respondents admitting to being scammed. This indicates that confidence alone does not equate to immunity from scams, suggesting that employees in these regions may need more practical, hands-on training or real-world exposure. In contrast, the UK reports the lowest scam victim rate, with 57% claiming they've never fallen for a cyber attack. However, this is down by 5% from 2021, which indicates a rising vulnerability even in regions with historically high confidence levels.

EXPERT INSIGHT

Anna Collard, SVP Content Strategy & Evangelist

The Dunning-Kruger effect, which is a cognitive bias where people overestimate their ability, is alive and well in cybersecurity. Our research reveals that while 83% of African employees are confident in their ability to recognize cyber threats, more than half (53%) do not understand what ransomware is, and 35% have lost money to scams. This overconfidence fosters a dangerous blind spot—employees assume they are scam-savvy when, in reality, cybercriminals can exploit more than 30 susceptibility factors, including psychological and cognitive biases, situational awareness gaps, behavioral tendencies, and even demographic traits. With phishing, AI-driven social engineering, and deepfake scams evolving rapidly, organizations must counteract misplaced confidence with hands-on, scenario-based training. True cyber resilience comes not from assumed knowledge but from continuous education, real-world testing, and an adaptive security mindset.

Breaking the Illusion: Encouraging Honest Reporting

One of the most crucial elements of a strong cybersecurity strategy is ensuring that employees feel comfortable reporting threats. However, our findings show that 1 in 10 employees (11%) still hesitate to report security risks, revealing a trust gap between employees and IT teams. While 56% of employees report feeling "very comfortable" raising security concerns, the remaining 44% highlight a significant opportunity for improvement.

Regional differences also play a role—71% of American employees feel very comfortable reporting security issues, compared to only 40% in Germany. Meanwhile, South Africa leads with an impressive 97% of employees expressing some level of comfort in reporting.

When employees were asked why they hesitate to report security concerns, the responses were telling:

- 38% didn’t know how
- 31% found it too difficult
- 22% were too scared
- 20% didn’t want to bother the security team

> *True cyber resilience comes not from assumed knowledge but from continuous education, real-world testing, and an adaptive security mindset.* - Anna Collard, SVP Content Strategy and Evangelist

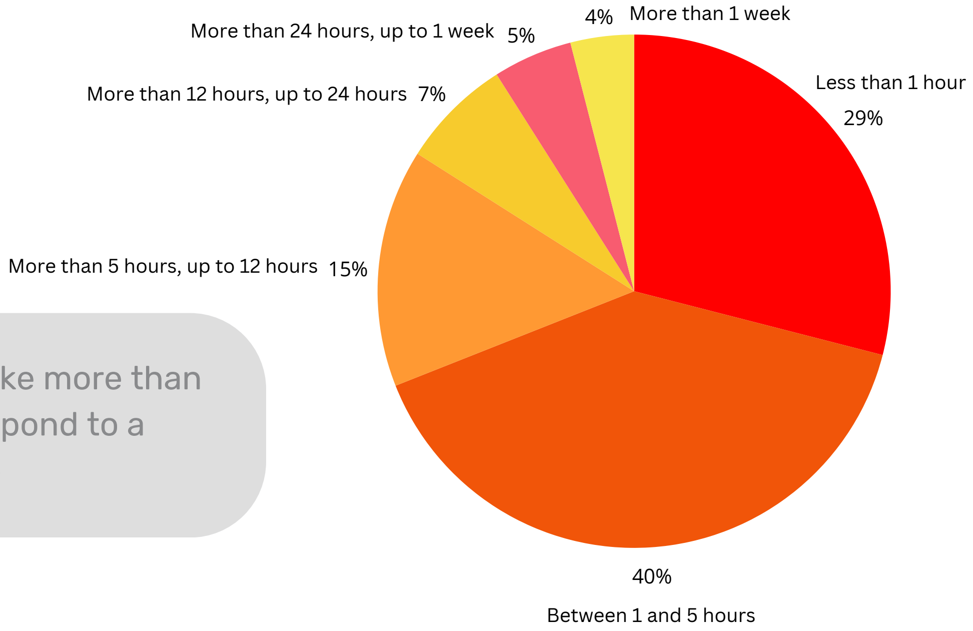
EXPERT INSIGHT

James McQuiggan, Security Awareness Advocate

Security is more than firewalls. It revolves around the trust between users and the cybersecurity team. A strong security culture fosters an environment where users feel safe reporting incidents without fear of punishment or blame. Organizations should foster transparency and a learning mindset, encouraging users to report potential issues to enhance overall security.

Security leaders must adapt their strategies to recognize the unique perspectives of different industries, regions, and age groups. This can involve tailored approaches like gamified awareness programs, rewards for compliance or recognition. Simplifying reporting processes and fostering open conversations about cybersecurity helps users see themselves as a partner rather as a hindrance in the organization. Ultimately, empowering people through human focused security programs only strengthens organizations. Building trust takes time, but integrating security into company culture transforms it from a check-box task into a collaborative effort for prevention of phishing attacks.

Average Time Taken for IT Security Teams to Respond to a Reported Security Issue



31% of IT teams take more than 5 hours to respond to a security issue

> *A strong security culture fosters an environment where users feel safe reporting incidents without fear of punishment or blame.* - James McQuiggan, Security Awareness Advocate

Closing the Confidence Gap: The Way Forward

This study highlights a glaring issue—employees think they're scam-savvy, but cybercriminals continue to outmaneuver them. The solution lies in bridging the gap between perceived and actual preparedness. Organizations must:

- **Implement personalized, relevant and adaptive training programs** that adjust to employees' strengths and weaknesses, with exposure to real-world cyber attacks.
- **Foster a blame-free reporting environment** to encourage early detection of threats.
- **Leverage intelligent cloud-based technology** to supplement human judgment with AI-driven security solutions.

In the end, cybersecurity resilience isn't built on confidence alone—it's forged through continuous education, rigorous testing, and personalized, relevant training that adapts to the evolving threat landscape. Because in the battle against cyber threats, the most dangerous thing employees can do is assume they're immune.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven ‘best-of-suite’ platform for Human Risk Management, creating an adaptive defence layer that fortifies user behavior against the latest cybersecurity threats. The HRM+ platform includes modules for awareness & compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents, and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilise workforces to transform from the largest attack surface to an organization’s biggest asset.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com