Chesterfield cyber expert: ‘People are not the weakest link’

September 21, 2026

“Good security isn't about expecting people to be perfect.”

A Chesterfield cyber security specialist is challenging one of the industry's most repeated phrases during Cyber Security Awareness Month - that employees are the "weakest link" in an organisation's security.

You don't improve a team by calling the players the weakest link. | Black Swan Cyber Security Solutions

Kevin Walker, founder of Chesterfield-based Black Swan Cyber Security Solutions, says blaming staff when something goes wrong can actually make businesses less secure by discouraging people from reporting mistakes quickly.

“People are not the weakest link. Let’s get that sorted straight away,” said Kevin.

“Criminals target people because people are busy, helpful and generally trust the people they work with. Put a convincing email in front of somebody at exactly the wrong moment and anyone can make a mistake.

“The important bit is what happens next. I’d much rather somebody rang me two minutes after clicking something and said, ‘Kevin, I think I’ve messed up,’ than kept quiet because they were frightened of getting into trouble.”

The warning comes as figures from the Government's latest Cyber Security Breaches Survey show that 43% of UK businesses identified a cyber security breach or attack in the previous 12 months.

Small organisations were far from immune. Some 42% of micro businesses and 46% of small businesses reported identifying a breach or attack.

Phishing remained by far the most commonly identified type of attack, affecting 38% of businesses. Yet only 19% of businesses overall had carried out cyber security training or awareness activity during the previous year. Among micro businesses, that figure fell to just 14%.

Kevin, who has worked in IT for more than 30 years and has spent much of that time supporting schools and smaller organisations across Derbyshire, believes businesses need to look beyond annual training courses and occasional phishing tests.

He said: “Training matters, but cyber security culture is what happens on the other 364 days of the year.

“If somebody reports a suspicious email and nobody responds, eventually they stop reporting them. If the boss ignores the security rules because they’re inconvenient, everybody notices.

“And if your response to somebody making an innocent mistake is to embarrass them or make an example of them, don’t be surprised when the next person decides to keep quiet.”

The National Cyber Security Centre takes a similar approach. Its guidance says organisations should create an environment where employees feel able to ask for help, report security issues and admit mistakes, with incidents investigated to learn and improve rather than simply to apportion blame.

NCSC phishing guidance goes further, warning that blaming users for clicking links does not work and that employees who feel supported can provide a valuable early warning system when an attack gets through.

Kevin says organisations should therefore think differently about what successful cyber awareness looks like.

“Instead of only counting how many people clicked the test phishing email, count how many spotted it and reported it,” he said.

“Good security isn't about expecting people to be perfect. Your technology won't be perfect either.

“It’s about putting enough layers in place that one mistake doesn't turn into a very bad day for the whole organisation.

“Your staff can be one of those layers. Treat them like part of the defence, not the problem.”

Black Swan Cyber Security Solutions is based in Chesterfield and works with small businesses, schools, charities, care providers and other organisations on cyber security and IT resilience.