Nottinghamshire businesses warned: The next cyber scam may look like ordinary office admin

chad.co.uk/business/nottinghamshire-businesses-warned-the-next-cyber-scam-may-look-like-ordinary-office-admin-8787459

John Smith July 9, 2026

Small businesses and community organisations across North Nottinghamshire are being warned that the next cyber scam they face may not arrive as an obvious fake email.

Kevin Walker, founder of Black Swan Cyber Security Solutions, says criminals are increasingly hiding their attacks inside normal workplace routines, using prompts and instructions that look familiar to busy staff.

Kevin's Chesterfield-based firm supports smaller organisations across the region, including businesses, schools, care providers, charities, trades and professional services firms.

"For years, people were told to spot phishing by looking for bad spelling, strange email addresses and urgent demands," said Kevin.

Kevin Walker, Founder, Black Swan Cyber Security Solutions

"That advice still has its place, but it is no longer enough. Some of the attacks we are seeing now look like normal admin.

"They look like a CAPTCHA, a Microsoft sign-in, a browser message, or a document that just needs one more step before it opens."

Kevin says two techniques being tracked in the cyber security industry, known as ClickFix and ConsentFix, show how quickly online scams are changing.

ClickFix usually presents the victim with a fake technical problem. It might claim that a document will not load, a browser needs fixing, or a verification step must be completed.

AI-generated illustration supplied by Black Swan Cyber Security Solutions.

The page then tells the user to press certain keys or paste a command to solve the issue.

The victim thinks they are fixing a simple problem. In reality, they may be following instructions written by a criminal.

ConsentFix uses a similar idea, but focuses on Microsoft 365, which is now used by many small organisations for email, files, team’s meetings and day-to-day communication.

Rather than stealing a password in the traditional way, this type of attack can trick a user into approving access or completing what appears to be a normal sign-in process. That may give an attacker access to email, OneDrive, Teams or SharePoint.

"That is what makes these attacks so dangerous for smaller organisations," said Kevin.

"The person does not always feel as though they have done anything wrong. They may not have typed their password into an obvious fake website.

"They may simply have clicked through something that looked routine because they were busy."

Kevin says the risk is not limited to large companies.

"An accountant, nursery, care provider, solicitor, charity, manufacturer or trades business may all rely on Microsoft 365 every day," he said.

"One compromised email account can lead to invoice fraud. One hijacked mailbox can be used to contact customers or suppliers. One stolen session can expose files, conversations and sensitive information.

"This is not just a boardroom problem for big corporations. It is a real risk for ordinary local businesses."

Kevin is urging local organisations to give staff more practical advice than simply "do not click suspicious links".

"Most people do not click things they believe are suspicious," he said.

"They click things that look normal, useful or necessary. The better advice is to pause when a page asks you to do something unusual to continue.

"If it asks you to copy and paste a command, stop. If it asks you to press an odd key combination, stop. If it asks you to drag a link into a browser, stop. If it asks you to approve access for an app you do not recognise, stop and check first."

He is also encouraging businesses to review their Microsoft 365 settings, including who can approve app access, whether multi-factor authentication is configured properly, and whether unusual sign-ins are being monitored.

Kevin says the answer is not panic, but better layers of protection.

"Updates, backups, email security and staff training still matter," he said.

"But smaller organisations also need to think about monitoring their devices and their online accounts. If something odd happens after the click, someone or something needs to be watching.

"The goal is simple. One rushed click should not be allowed to become a business-ending event."