A PERFECT LIES STORY

THE FALL GUYS

WHY CYBERSECURITY IS MORE IMPORTANT THAN EVER FOR SMALL BUSINESSES



A **DARK MATTER** SERIES

In association with DELL Technologies McAfee intel

Signed, sealed, stolen

How can a seemingly innocuous happy birthday email lead to a company's entire cash reserves being stolen? You might think it far-fetched; a series of unfortunate events that could never happen to you or your business. The reality is these threats are already impacting businesses every day, and preparation is no longer optional.

AI has dramatically lowered the barrier to entry for cybercriminals, allowing sophisticated scams to be created relatively easy and at scale. "Cybercrime is an industry... today, it's a job" said Vonny Gamot, VP at McAfee. Bad actors now have an unlimited armory of tools designed to trick incognizant employees. From grammatically perfect phishing emails written with an LLM to visual and audio deepfakes of CEOs, the tactics are getting increasingly harder to spot.

For unsuspecting businesses, this can start a chain reaction of consequences both financial and reputational, posing a risk to business continuity. Aside from the threat of ransom or the transfer of funds, a cyberattack or scam can delay payroll, halt supplier payments, and shake customer confidence. All of which take time to rectify, often meaning the recovery costs can be more damaging than the scam itself. Take the true cybercrime story depicted in our docu-drama 'Butterfly', for example. Whilst the ransom cost the business £30,000, the aftermath cost upwards of £250,000.

It's a common misconception that small to medium businesses are safe from cybercrime. In fact, of all UK business cybercrime in 2025, 67% was targeted at SMEs[1]. There's no such thing as being too small, flying under the radar or having too low a turnover in the cybercrime business; it is in fact quite the opposite. Scammers are taking advantage of businesses who are still maturing. Unlike large enterprises, most growing businesses don't have a security operations centre or a team of analysts monitoring threats around the clock. Often, there is only a small IT team (if a team at all), no dedicated security staff, and a tight grasp on budgets. Even to the most meticulous among us who think they can spot a scam and hedge their cyber defenses on human judgement, Americans lose an average of 114 hours a year trying to figure out what's real and what's dishonest[2]. Time is also money, afterall.

'The Fall Guys' is the second episode in the 'Perfect Lies' series. Centered around a design studio who are about to make an acquisition to take their small business to the next level, opportunist scammers take advantage of an absent CEO, an ambitious Head of Finance and a young employee who is keen to make an impression...

What follows is an orchestrated, multi-modal attack. Using a mix of scam tactics, both seen before in Episode 1 'Mom, It's Me' and entirely new to the series, 'The Fall Guys' takes 'Perfect Lies' into the corporate setting. In partnership with Dell Technologies, Intel and McAfee, we're bringing together the technology your business needs to stay ahead of cybercrime, alongside expert guidance and practical steps to help you and your employees spot a scam before it lands.

Sources

[1] gov.uk/government/statistics/cyber-security-breaches-survey-2025

[2] mcafee.com/blogs/wp-content/uploads/2026/01/Scamiverse.pdf

What does good cybersecurity look like?

For small businesses, owners, finance leaders and administrators often become the first line of defense. Here, simple, integrated protection and employee awareness are more important than ever. Requiring more than just isolated tools, business safety demands an integrated, hardware-to-software security ecosystem. Through the combined strength of Dell Technologies, Intel, and McAfee, businesses gain enterprise-grade defense built specifically to withstand the multi-channel tactics demonstrated in 'The Fall Guys'.

Attacks like the one depicted in 'The Fall Guys' are often referred to as a Business Email Compromise (BEC), where criminals impersonate trusted colleagues, suppliers or business leaders to manipulate payment processes. Instead of relying on human judgment, businesses need a protective layer to guide employees in making safer decisions and keep teams safe wherever they work. The malicious phishing email that started the chain needs to be flagged before it's even opened; network firewalls need to block unauthorized access to core systems and databases. These necessities - among many other protective measures needed today - are why Dell, Intel and McAfee have partnered to help keep businesses secure, no matter their size. Designed specifically for small teams, McAfee Business Protection takes the guesswork out of daily decisions; extending to remote workers via secure VPN, all without requiring a dedicated IT department to run it.

And true defense should be designed with workforce productivity in mind. Dell PCs, powered by Intel® Core™ Ultra processors don't affect hardware performance, running security protocols in the background to prevent threats.

It's about empowering business owners and employees with enterprise-grade protection, and peace of mind that takes away any second-guessing. With ease-of-use built into its design, you don't need a dedicated team of experts to set it up or keep it running.

By pairing defensive technology with employee awareness, protection works continuously to stop attacks before they disrupt operations. Together, this ecosystem neutralizes threats before they reach your bottom line, giving growing businesses the confidence to innovate without leaving their front door unlocked; an easy mistake with limited IT resource and budget.

So, what do businesses need to look out for?

The average American receives 14 phishing emails a day[3], many of them to their work addresses. Now that scammers can use LLMs to perfect grammar and even brand voice, these emails can no longer be caught by looking for spelling mistakes. A higher level of scrutiny is now required to identify a scam, whether that be an email, phone call, or live video. To remain vigilant, below are the best practices to implement into your day-to-day:

Source

[3] mcafee.com/learn/how-to-reduce-spam-emails-and-protect-yourself-from-phishing

01

Familiarise yourself with phishing

Ensure your employees know the signs behind a phishing email. Whilst the grammar in the body of an email may now be perfect, the address of which it came from will be different from the profile it's trying to imitate. Other signs include urgent language, questionable links, or any requests for personal data.

02

Authenticate, authenticate, authenticate

Enable multi-factor authentication across critical business systems to reduce the risk of compromised credentials being used to gain access.

03

Always verify

A voice note from a colleague can now be entirely AI-generated from just three seconds of audio. Never act on an urgent request without verifying through a separate channel first.

04

Slow down

Slow down before you send. Scammers rely on urgency - a two-minute pause to double-check a request is often all it takes to stop the scam working.

05

Audit regularly

Scammers can manipulate data within a breached system. Regular audits of databases will help identify any anomalies that have been planted by bad actors, future-proofing your systems and business. In addition, security software continuously scans your data in the background to ensure it is protected.

06 Know your vendors

Criminals are increasingly targeting supplier relationships, altering invoices or impersonating legitimate vendors to redirect payments. A simple callback to a known contact before processing any change to payment details can be enough to verify its legitimacy.

07 Pair awareness with cyber defense

In today's AI world, no single habit catches every scam. A combination of staying educated on the latest innovations of AI and utilising cyber security technology is essential for catching every scam, no matter how many attacks are thrown your way.

08 Implement payment rules

Best practice involves implementing mandatory dual-sign-off policies for transfers exceeding a specific threshold, and pay attention to warnings and guidance from your bank - they are there for a reason.

Cybersecurity shouldn't slow down growing businesses. With the right combination of employee awareness, trusted devices and intelligent protection, small businesses can focus on growth with confidence, knowing they're prepared for the evolving threat landscape. For more information, we sat down with Small Business Country Manager Brian Horsburgh, and Client Solutions Technologist Ross Haddow of Dell Technologies to walk us through where businesses are prone to cyberattacks and how to defend against them, here. For a scene-by-scene breakdown of 'The Fall Guys', examining each scam tactic in detail, take a watch of 'Decoded', here. And for all the latest in cyber news, you can follow the McAfee blog, providing you with consistent updates in this ever-changing world of AI, here.

Not sure if your business endpoints are secured against deepfake attacks?

Outsmart AI driven threats with multi-layered protection from Dell Technologies, McAfee and Intel.

DELL Technologies McAfee intel

Shop Dell PCs

Scan QR code

Explore McAfee Protection

Scan QR code

DARK MATTER