

A PERFECT LIES STORY

MOM, IT'S ME

HOW TO PROTECT YOURSELF AND
YOUR LOVED ONES IN THE ERA OF
AI ENHANCED SCAMS

A **DARK MATTER** SERIES

In association with

DELL Technologies

McAfee

intel.

Defending against the Deepfake

“Mom, it’s me...” Written in a text from an unknown number, it’s a tactic most of us have learned to spot, flag as spam, and ignore. But what if it isn’t a text? What if your phone rings and it’s a voice, the unmistakable voice of your child calling you in distress? You know how they sound no matter what they’re feeling, but in the era of AI, that human instinct is the vulnerability cybercriminals are weaponizing.

AI technology has fundamentally changed the landscape of fraud. With just a few seconds of audio scraped from a rogue phone call or a social media video, the well-known text scam has been mutated into a sophisticated, hyper-personalized threat. Whether through cloned voices or deepfake videos, scams are becoming incredibly difficult to detect. Backed by the rise of “Fraud-as-a-Service” (FaaS) platforms, we are entering a challenging new era where we can no longer trust what we see or hear.

In the UK, on average, **1 in 5 people receive scam calls or texts most days, with 10% of people receiving them daily**¹. It’s a massive operation, and public confidence is shaking; 35% of respondents to a McAfee survey admitted they are not confident in their ability to spot a deepfake scam.² When psychological tactics, like emotional manipulation with a manufactured false sense of urgency, are combined with these hyper-realistic AI tools, the pressure can bypass our rational thinking. Yes, even yours.

Sources

¹nationaltradingstandards.uk/news/phone-scams-take-sinister-twist-as-victims-voices-cloned/

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

At Dark Matter, it is our mission to cut through the noise of technological change to help people navigate it through education. Our latest drama series, 'Perfect Lies', demonstrates some of the ways in which cybercriminals are targeting people every day.

Partnering with three industry leading technology organisations, Dell Technologies, McAfee and Intel, we're combining the technology you need to keep yourself and your loved ones safe, with education on the practical steps you can take to stay one step ahead of AI infused cybercrime.

Dell Technologies, McAfee and Intel provide the preventative layer, which, when combined with knowledge and education, provides true defense. Dell PCs, powered by Intel® Core™ Ultra processors, are built with three AI engines, CPU, GPU and NPU, and are designed for optimal performance, efficiency and security. All of which come with a limited time subscription of McAfee's award-winning protection to keep you safe online.

Why is this important?

Cybercriminals are increasingly taking a multi-modal AI approach and by using personal information found online, they can attack from all angles. A well-meaning social media post celebrating a birthday or making your CV publicly available through an online job posting could be all it takes to provide an adept scammer with enough information to build up a convincing profile.

It may be that you are already well-informed and take all the right precautions, but scammers are constantly evolving. In order to safeguard yourself against the type of distress scam we focus on in our first episode, 'Mom, it's me', there are a number of steps you can take:

01

Verify immediately:

Hang up and call your friend or family member on the number you have saved for them. Just because it sounds personalized doesn't make it real.

02

Establish a safe word:

Agree on a phrase with your family. If the person calling is who they say they are, they will be able to answer this easily.

03

Lock down your digital footprint:

Think about the content you're sharing online. Tighten your privacy controls and don't accept connection requests from strangers.

04

Resist the artificial urgency:

Hyper-urgency works in the scammer's favor. If there is 'no time to check' because a payment is demanded immediately, treat that pressure as a major red flag.

05

Don't click links:

It is now much easier to create authentic looking websites with fillable forms, be cautious of suspicious links. Check the URL to see if there are any signs to suggest it is a faux website.

For more practical advice, we sat down with VP at McAfee, Vonny Gamot to find out how the proactive solutions from McAfee help shift the power back to you.

Watch the interview with Vonny [here](#) and the Perfect Lies Decoded video [here](#), where we break down the Mom, It's Me episode to dissect the AI scam in detail.

Scams are designed to catch you off guard. It doesn't matter where you're from, your level of education, your job; all of this is irrelevant. Scammers know how to expose your vulnerabilities, and this isn't anything to be ashamed of, after all, it's what makes us human. But knowing more about the capabilities of AI, means we can be more prepared and, hopefully, take a second to question things more thoroughly.

Take control of your digital safety

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

DELLTechnologies **McAfee** intel



Shop Dell PCs

[Scan QR code](#)



Explore McAfee Protection

[Scan QR code](#)

DARK MATTER