One successful Gen AI attack on your IT Help Desk could destroy your business. Frank Abagnale tells how they did it and how you can avoid being the next victim.

It's September 2023 and at the iconic Las Vegas hotels Bellagio, Cosmopolitan and Mandalay Bay, guests are suddenly unable to use their key cards or are finding that room phones and TVs are not working. Lobby ATMs and casino slot machines are unavailable and long queues are forming in the restaurants, bars and checking desks as systems go down and electronic payments are rejected.

Resort staff are urgently resorting to pen, paper and cash while prospective customers can't make online bookings. This chaos is not confined to Nevada but is happening at MGM resorts all over the US.

Just another temporary IT meltdown, right?

Wrong. This is a targeted attack and the group responsible, Scattered Spider, want a ransom paid to stop it.

I'm Frank Abagnale and I've been a fraud and cybersecurity advisor for the last 48 years, working closely with the FBI to train their agents, delivering thousands of seminars to corporations across the world and authoring several best-selling books. You may also recognise me as the inspiration for the 2002 Oscar nominated Spielberg movie 'Catch Me If You Can'.

So how did the hackers gain access to MGM Resorts? Simple, they are believed to have called the IT helpdesk and impersonated an employee, it was that easy.

They would have accrued enough information to persuade the agent to help them out, maybe they pretended to be distressed, angry or were just apologetic for being so dumb and causing all this fuss. It's called social engineering, and I first used it as a teenager in the 1960s to get a new Pan Am pilots uniform over the phone to make me look more convincing when cashing dud checks at the bank.

While I had to use the NY phone book and some bravado to succeed, today's criminals have a huge technical advantage which makes them a thousand times more dangerous.

As businesses have adopted robust security to protect both their digital front door and their back-end systems, the IT helpdesk is now the target of choice for attackers. Agents will be reliant on the caller having the right information and maybe having access to the registered phone for that employee to receive a security code.

However, phones can be hijacked and knowledge stolen. Once criminals have access to credentials, they perform an Account Takeover (ATO) and have free access to the

company's systems. They may steal confidential data or lock everything up and request a ransom in cryptocurrency to resolve.

Generative AI elevates the threat even further as with it criminals can replicate voices, IDs and even real-time images of the targeted employee. If the caller sounds like the CEO and even *looks* like the CEO are they going to deny them access?

Thankfully there is help at hand. I advise a company called Trusona Inc. who have pioneered an easy to use, Gen AI resistant tool, ATO Protect, for IT help desk agents to know who is really on the other end of the line. And it's equally applicable to finance, HR and other sensitive departments who may be the focus of an attack. Even better there's no complicated IT deployment required so it can be up and running – and protecting your company – in no time.

I will be introducing Ori Eisen, CEO of Trusona, at the SDI webinar at 2pm November 14th 2024. Ori will be presenting Trusona's ATO Protect product and I encourage you to join and see how you could use it to stop attackers targeting your IT help desk and avoid the chaos that MGM resorts experienced last year.

To conclude the MGM story, they were eventually able to recover control of their systems, but the attack cost them over $100M and caused their share price to dip nearly 5% - all from one fraudulent call to the IT helpdesk.

MGM could afford to take the hit, could your business?