Scamming in the laboratory industry: A growing threat

Jacqueline Balian, GAMBICA, jacqueline.balian@gambica.org.uk

We've all seen deepfakes, like the famous image of the Pope in a puffer jacket, or the Mona Lisa rapping, but fraudsters have now taken this technology to a new level, using manipulated video footage to cheat a company out of $25 million.

An employee at ARUP, an engineering firm, was invited to an online meeting by what appeared to be the company's Chief Financial Officer to discuss confidential transactions. The people in the video conference seemed to be fellow company staff members but were, in fact, deepfake creations generated from material from previous meetings. Following instructions, the employee transferred money to five local bank accounts in 15 separate transactions.

ARUP admitted to being scammed through its Hong Kong office and released a statement saying: "Our financial stability and business operations were not affected, and none of our internal systems were compromised." However, the company's chief information officer, Rob Greig, acknowledged that the company had been subject to frequent attacks including deep fakes. "The number and sophistication of these attacks has been rising sharply in recent months" said Greig, adding that he hoped ARUP's experience would raise awareness of the risk.

Deepfake technology, initially used primarily for creating pornographic videos of celebrities to generate web traffic and downloads, is now being used much more widely and has now become prevalent in 'revenge porn', with 'ordinary' people with little technical expertise using widely available software to manipulate video content. Endtab.org, which trains universities, law enforcement agencies, and social workers on spotting and tackling technology-related abuse, has pointed out that to begin with, creating convincing deepfakes required extensive training data, but today, passable results can be achieved with just a few shots or even a single image.

There is widespread concern about the use of this technology to disrupt the political landscape, but with the increasing prevalence of facial recognition systems as part of company security measures, the risks to business are also significant.

Leaders with online profiles are particularly vulnerable to identity theft via AI tools.

In the ARUP case, the complexity of the deepfake video conference suggested a high level of security penetration and information gathering within the organisation. Further investigation revealed that fraudsters used stolen Hong Kong identity cards to make multiple loan applications and bank account registrations, using deepfakes to trick facial recognition systems.

The ARUP case is the first widely publicised incident of deepfake scams by international criminal gangs. The company's concerns about the potential impact on its reputation and financial stability illustrate why most victims of scammers try to keep such losses under wraps. But of course, one hears about cases, and it seems that impersonation scams are becoming increasingly common in the laboratory industry.

At present, most scams we hear about in relation to lab firms still focus on the well-tried and effective strategy of intercepting email traffic, creating fake bank accounts and getting payments re-routed to criminal bank accounts.

These scams are costing lab companies many thousands of pounds. But as well as the financial cost, another worrying aspects is the amount of time and effort everyone has to expend to avoid becoming the victim of one of these scams, and the added difficulty that implementing countermeasures creates for those doing business.

I am sure everyone reading this, like me, gets tens, if not hundreds, of emails offering to sell marketing lists from exhibitions and conferences. I've even received offers to sell me the GAMBICA membership list. This is hugely galling. The GAMBICA membership list is not for sale, so if a list exists at all, it does not contain legitimate data. Naturally, I tried to take action to stop this and contacted Action Fraud, but it would appear that Inaction Fraud might be a better title because I wasn't able to get them to do anything at all.

I have heard that they have had some notable successes working quietly in the background, but the sheer volume of these scams makes their job very difficult, and means that those seeking to buy lists legitimately have the greatest of difficulty in doing so.

One of the problems has been that the law has lagged behind the scammer's technology, particularly in the area of deepfakes, but legislation is now changing in the UK, EU and US. In October, California enacted laws prohibiting the sharing of deepfakes of political figures close to elections and banning deepfake porn. At the federal level, a Bill will require a watermark indicating that a video is fake. Social media giants, currently not considered authors of harmful content under Section 230 of the Communications Decency Act, face changes now that the UK's Online Safety Act 2023 has put a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms. The Act also gives providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear. The effectiveness of these provisions remains to be seen.

At present, your only real way of avoiding becoming a victim is to try to make sure that all employees make efforts to avoid scams and are skeptical of what they read, hear, or see, even from senior management.

There are some resources to help: Action Fraud offers a Cybersecurity Toolkit for Small Business to help you target and resolve common weaknesses. They also have a series of simple mini courses, each lasting approximately 10 minutes that can be taken at any time and pace to enhance understanding of these risks - and the potential impact from a business perspective. The toolkit includes access to Quad9 - a free security solution from the Cyber Security Alliance that protects systems from accessing known malicious websites. You can access these through the Action Fraud website. Another website, takefive-stopfraud offers a tool to test how scam susceptible you might be.

If nothing else, using these tools might help keep scam avoidance at the top of your team's minds. GAMBICA will be running a webinar on cyber security featuring international laboratory expert Burhard Schafer, when webinars begin again in September. Hope you can join us.

And in the meantime - good luck!

Jacqueline