FALL 2024 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, and Cybersecurity Awareness Month, we discuss how deepfakes create expensive problems for organizations, a review of deepfake technology, and the slow march toward deepfake legislation.

Deepfake Criminals Trick with Fraudulent Masks

October is Cybersecurity Awareness Month and with Halloween closing in, we're looking behind the digital masks of deepfakes and the frightening scams, tricks, and frauds that can potentially cost organizations millions if not caught in time. Estimates of deepfake frauds are eclipsing billions of dollars, and there's no question that these criminals are trying their best to trick organizations out of big dollars and big data wearing some familiar masks. It doesn't have to be a nightmare though, and we'll provide tips to help pull off those deepfake masks and reveal the scam before it's too late.

The Big Heist of 2024: In February, reports surfaced that an employee in the Hong Kong office of UK engineering firm Arup, was fooled by a sophisticated deepfake "meeting," that led to the transfer of $25 million USD. While that employee reported having concerns over what he thought had been a phishing email, his concerns were alleviated when instructions were again issued during a video conference attended by "multiple employees." Unfortunately, all the employees on the other end of the video conference were deepfake images and voices. In the end, the employee made fifteen money transfers totaling approximately $25 million USD to 5 different financial institutions (CNN article updated 5/17/24).

Deepfake Employee Unmasked as North Korean Hacker. On July 23, 2024, cybersecurity firm KnowBe4 published their account of how a North Korean hacker evaded their candidate screening and background checking processing through the use of a stolen, then deepfaked identity. Fortunately, the hacker did not breach data or scam the company out of funds. Unfortunately, the hacker was able to upload malware by using a VPN to remotely connect to the company-issued laptop, and KnowBe4's SOC team was able to quarantine the user's access in less than 30 minutes. The laptop issued by KnowBe4 was sent to a "laptop mule farm," a US-based location where company-issued laptops can "go live" and be used to facilitate hacking activities that are conducted from outside the country. The Department of Justice busted up a Nashville, Tennessee

laptop mule farm suspected of aiding North Korean hackers posing as remote employees in August 2024.

The Trickster that Got Tricked: Not all deepfake scams are successful, and it's a sweet treat to hear about one that failed. In July 2024, the head of the luxury Italian sports car company Ferrari was the subject of a deepfake scam which attempted to coerce an employee for help with a "big acquisition" (Ferrari article) via the encrypted communications app WhatsApp and a convincing phone call. Feeling something was off, the targeted employee asked what book the CEO of Ferrari had recently recommended. Not getting the right answer, the employee wisely disconnected, potentially saving Ferrari a trunk load of scammed funds.

Future Ghostbusting: These examples provide several lessons for organizations fearing deepfake scam nightmares: (1) Employees are both the best prevention and the weakest link when it comes to defending against fraudsters. Training employees to recognize and report phishing, vishing, smishing, and all other communications that just don't "feel right," will never be a wasted effort. (2) Human Resources Departments now have fair warning that checking references and identities is now fair game for deepfake identity fraud. Training HR representatives to recognize the signs of deepfakes is imperative. (3) Organizational culture must support internal multifactor authentication – employees need to feel free to ask questions when they receive a request that seems off. (4) Deepfake technology requires just a small amount of authentic content to create. Organizations should include deepfake recognition as part of their security training curriculum. That's an uphill trek as deepfakes are becoming more sophisticated and realistic, however, training is available from firms like Digital Mountain to help provide education that may help employees think twice when confronted with a potential deepfake.

When studying deepfake scams, it's clear that deepfake scammers are getting more sophisticated and upleveling their technological skills to trick organizations out of big data and big money. The estimated growth for this crime shows no end in sight. With deepfake detection technology lagging, employees will continue to be on the front lines for the foreseeable future. This makes good training and supportive organizational cultures essential to defending against deepfake frauds and their tricks.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

THE SEDONA CONFERENCE WORKING GROUP 11
MIDYEAR MEETING 2024
Atlanta, GA: October 29-30, 2024

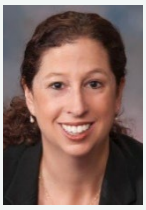
CISO-CIO FORUM
La Jolla, CA: October 30, 2024

MASTERS CONFERENCE NOVEMBER 2024
Atlanta, GA: November 12, 2024

GEORGETOWN LAW 21ST ANNUAL ADVANCED EDISCOVERY INSTITUTE
Washington, DC: November 14-15, 2024

OPENTEXT WORLD 2024
Las Vegas, NV: November 19-21, 2024

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: