WINTER 2025 E-NEWSLETTER

At Digital Mountain, we assist our clients with their eDiscovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we share our technology predictions for 2025 impacting the legal and cybersecurity sectors. We also address how deepfake strangers pose online dangers for organizations.

Deepfake Stranger Danger Proliferates in 2025

If you're longing for the days when Officer Friendly's school program or an after-school television special were all that were needed to warn us about Stranger Danger, you're not alone. The rise of deepfake technology, social media applications, and the vast amount of biographical information that's easily obtained off the internet has revamped Stranger Danger for the digital age. In this article, we'll look at some current impersonation scams making the rounds and anticipated to grow in 2025.

Catfishing Can be More Than Romance Scams

Catfishing is the slang term used for the practice of creating fake online identities which are then employed to convince people they are in authentic business or personal relationships. These aren't necessarily limited to scams where the perpetrator wants money, although those seem to be the most popular. There are also catfishing cases where the goal is to embarrass, humiliate, or intimidate the target. The basic elements of a catfishing business or romance scam are the same as most other deepfake scams. After creating a fake online identity including photos, biographical data, email accounts, and often now, voiceprints, the scammer can use these identities to create social media accounts, dating app accounts, gaming platform identities, and join interest forums. Catfishing for business and romance scams are serious business. In 2024, the FTC reported that losses from catfishing scams eclipsed one billion dollars for the year 2023 and were expected to increase. Crypto is becoming the currency of choice, but gift cards and wire transfers are also popular requests.

With advances in deepfakes, it's becoming more frequent for the perpetrator to create a voiceprint that can be sent by SMS or text message, or, left via voicemail. For this element, the perpetrator can use a number of legitimate applications that will allow the bad actor to create a script and then "record" the message using an appealing voice that will dovetail to the fake identity's biographical data. This identity matching is key to hiding the perpetrator's true identity as the real person behind the fake identity may not share any traits with their catfishing avatar.

Cloned Social Media Accounts

Cloning social media accounts is relatively simple to pull off. A near duplicate of an authentic account is created by downloading publicly available photos of the account owner, then creating a copy of the owner's identity and contacting their "friends," followers, or connections with a request to connect. If the requests are accepted, the scammer may continue to clone other accounts, spread mis- and disinformation, or attempt to direct people to scam websites. Manipulation in cloning is easier to achieve because the scammer is going after people who are already connected to the authentic account and trust is already established. Before the advancement of Gen AI applications, a scammer would have to spend time trying to imitate a person's writing style to pull off a believable cloned account. Now, the scammer can upload samples of the authentic account owner's writing into a Gen AI app and ask it to create a new post "in the style of" the true account owner. With the incorporation of AI writing apps in social media accounts, this becomes even easier to accomplish directly on the cloned page.

This is Also a Business Problem

The scams above and the tools that enable them are not just targeting the average person with a dating profile. Scammers are using these same basic techniques to catfish or clone the social media and online identities of executives, partners, and even employees as vehicles to defraud organizations. With an organization's reputation partially dependent on their online identity, a hacked social media account could lead to a public relations crisis or even a network hacking event and data breach.

As an organization that stands at the intersection of law and technology, we are frequently tested in our ability to remain agnostic about advancements in technology. We see all the amazing developments in technology, especially in the AI realm, as having the potential to advance our common good and make life better for all. We also, especially as an eDiscovery, digital forensics, and cybersecurity provider, see what happens with these advanced technologies when they are used for evil versus good. We remain cautiously optimistic that those of us working on the side of good will be able to expose scammers, even if it's just by warning you that these bad actors are creating more Stranger Dangers with less effort.

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

UPCOMING INDUSTRY EVENTS

MASTERS CONFERENCE
Los Angeles, CA: February 4, 2025

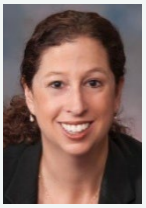
NET DILIGENCE CYBER RISK SUMMIT
Miami Beach, FL: February 10-12, 2025

MAGNET VIRTUAL SUMMIT 2025
February 10-14, 2025

9TH ANNUAL OFFICIAL SILICON VALLEY CYBERSECURITY SUMMIT
Santa Clara, CA: February 12, 2025

12TH ANNUAL UF LAW E-DISCOVERY CONFERENCE
Gainesville, FL: February 12-13, 2025

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: