LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Search for Board Members:

Do you want to increase your networking within the CFE community? Do you enjoy helping others to further their education and career?

We have 5 openings on the board as of June 30th that need filled due to long-term board members stepping down.

The Chapter's officer positions are elected by the board of directors, following the elections of new directors. (The officer positions are president, vice president, treasurer, secretary, and training director.) In addition to the officer positions, the chapter also has numerous committees in place for anyone interested in contributing: Newsletter, Social Media, Website, Membership, and Scholarship.

We need your help! And don't keep us a secret from your friends and colleagues. If you know of anyone who might be interested, please let us know!

In This Issue

Fraud Talk Podcast

The Top 5 Most Scandalous Frauds of 2024 - John Warren - Fraud Talk - Episode 152

In this episode of Fraud Talk, John Warren, CEO of the ACFE, and Jennifer Liebman, Editor-in-Chief of Fraud Magazine, delve into some of 2024's most scandalous fraud cases. From Boeing's guilty plea tied to deadly aviation crashes to Vietnam's sentencing of a real estate tycoon to death for embezzlement, they explore the global implications of these high-profile frauds. Tune in to understand the evolving nature of fraud, including the role of AI and platforms like TikTok in modern schemes, and uncover critical lessons for prevention and compliance.

https://acfe.podbean.com/e/the-top-5-most-scandalous-frauds-of-2024-john-warren-fraud-talk-episode-152/

UPCOMING EVENTS

LOCAL:

ACFE Southwest Ohio: Equine Fraud in the Insurance Industry *Part 2*
In-person: Blue Ash, Ohio
April 16, 2025
Learn more: https://swohacfe.org/event-6038190

SEMCACFE 31st Annual Fraud Conference
VisTaTech Center at Schoolcraft College,
18600 Haggerty Road, Livonia, MI 48152
April 29, 2025
Learn more: https://semcacfe.org/meetinginfo.php?id=101&ts=1739822930

ACFE Southwest Ohio: AI, Accounting, and Ethics (2 Ethics CPE)
In-person: Fairfield, Ohio, or Virtual
May 9, 2025
Learn more: https://swohacfe.org/event-5833880

NATIONAL:

ACFE 36th Annual Global Fraud Conference
In-Person, Nashville Tennessee, or Virtual
June 22 - June 27, 2025 (early registration ends March 18th)
Learn more: https://www.fraudconference.com/36th-home.aspx

** Please let Mark Lee know (president@lansingacfe.org) if you plan to attend either in-person or virtually, as there is a group rate discount if 5 or more LACFE Chapter members attend**

ACFE Bribery and Corruption
Virtual Seminar
May 14 – May 15, 2025 (early registration ends April 14th)
Learn more: Event Details

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article or job opening, please contact Jennifer Ostwald at newsletter@lansingacfe.com

The LACFE is always looking for volunteers to serve on the board, help with events, recommend training topics/speakers, grow our network to alert students to the LACFE scholarship, and more!
Let us know if you can help be part of our growth!
Email: newsletter@lansingacfe.com

Spear Phishing in the Age of AI

March 11, 2025
By Samuel May, CFE
https://www.acfe.com/acfe-insights-blog/blog-detail?s=spear-phishing-age-of-ai

An evergreen avenue for fraud, phishing is a cyber security threat that has seen substantial evolution in recent years. While the threat of widespread phishing has grown, super charged by artificial intelligence (AI) tools and a world more connected than ever, spear phishing is especially dangerous to organizations and public targets.

A standard phishing attack is a generic, seductive lure designed to entice the average person to click a link, download an attachment or otherwise compromise the security of their system. The attack is successful through volume; most recipients will not click it, but some will. The low effort required to produce the attack makes the low success rate acceptable and a good return on investment. This is especially true now, with widely available automation tools making writing and sending phishing attacks painfully easy.

Modern Spear Phishing

Spear phishing is the opposite. It is a targeted, tailored version of phishing. Spear phishing attacks are designed often for just a single individual or team within an organization. The purpose of the attack is also usually more specific than simply spreading malware. Targets are chosen for a high potential for monetary reward, to gain access to particularly sensitive systems, to hurt the reputation of a business or government, or for a variety of other malicious reasons.

Traditionally, spear phishing was a heavier lift. Perpetrators had to do their own research, manually combing through available information on the target to figure out how they should approach the attack. What kind of communications does the target typically receive? Who do they communicate with? Then, there was the actual communication. Attackers would need to draft an email or text that looked legitimate. Spelling errors, odd syntax or out of place idioms could raise suspicion and cause the attack to fail. If the attacker wanted to get the victim to download malware, they would typically need to create it themselves. It took particular individuals with the requisite skills and the necessary motivation to make all this extra effort.

Today's modern spear phishing utilizes new tools that make these attacks easier and more accessible. AI tools are getting stronger at putting together personalized attacks. A study from 2024 evaluated the capability of large language model (LLM) AI tools in creating targeted spear phishing attacks. Specific AI models were tasked with gathering information and creating vulnerability profiles for specific targets. They created useful profiles 88% of the time and produced inaccurate profiles only 4% of the time. They also managed a 54% success ratio on fully AI-generated phishing emails, getting more than half of study participants to click links from the email.

AI can also handle text message phishing attempts, generating authentic-looking answers rapidly enough to appear human in any language. Need to hook a victim who only trusts someone they can see? Deepfake video conferencing has already shown itself to be successful.

What does a spear phishing attempt look like in 2025?

The attempt will come from a source that does not seem out of place. The attacker will have done their research, whether alone or with the help of AI, and know what the victim wants or needs.

The communication will mimic real communications from other reputable sources. Everything is on the internet, including an almost infinite number of example memos, email templates and style guides. Attackers can sift through all of them faster than ever.

The attacker will cover their bases and look legitimate. Most targets, especially valuable corporate targets, should know to be suspicious of emails from external sources thanks to cybersecurity training, and attackers know they will have to overcome a pretty substantial baseline suspicion. Whoever attackers claim to be in the email can be backed up with a social media presence filled with posts, pictures and potentially video appearing authentic.

Overly motivated attackers will do what they can to attack a weakened defense. They might flood the victim’s inbox with easy-to-spot phishing emails or junk mail, creating a false sense of security and confidence in the victim’s ability to spot an attack. They can plan their attack for a particularly busy day, week or season, having identified times where the target is likely to be at their most haggard.

If the victim attempts to communicate with the attacker to verify their authenticity before fully biting the hook, they will find a courteous, professional, well-written individual. Text or direct messages through apps or social media will be responded to in short order with all appropriate pleasantries.

The Plan in Action

Our example victim is a successful online influencer. They have a YouTube channel with hundreds of thousands of subscribers and similar viewership across their media. As the attacker, we want to compromise their system and gain access to their YouTube account. If we are successful, we can contact hundreds of thousands of victims from a trusted source, spreading our chosen malware over a wide net. With our target picked, we just need to figure out what our spear phishing attack will look like.

Simple enough, let’s ask an AI.

I prompted ChatGPT with: “What kind of email solicitations do YouTubers receive?” It immediately provided a list including sponsorship and brand deals, affiliate programs, free product offers and multi-channel (MCN) invitations. Let’s keep it easy and impersonate a potential sponsor.

Next step: ChatGPT again. Immediately after the first prompt, I asked: “What would a sponsorship email look like in this scenario?” Not the most elegant of prompts, perhaps, but it seemed to have worked:

A sponsorship email can vary depending on the professionalism of the company, but here’s an example of a legitimate sponsorship email that a YouTuber might receive:

Subject: *Exciting Sponsorship Opportunity with [Brand Name]*

Hi [YouTuber's Name],

I hope you’re doing well! My name is [Your Name], and I work with [Brand Name], a company specializing in [industry/product type, e.g., gaming peripherals, skincare, software]. We’ve been following your YouTube channel and really love your content, especially [mention specific video or theme].

We think your audience would be a great fit for our product, [Product Name], and we’d love to explore a partnership with you. Here’s what we’re offering:

- *A **sponsored integration** in one of your upcoming videos*
- *A **competitive compensation package** based on your audience size and engagement*
- *A **custom discount code/affiliate program** for your viewers (optional)*
- *We’ll provide a **free product** for you to test and review*

If you’re interested, we’d love to discuss further details, including payment terms and content expectations. Let me know your thoughts, and I’d be happy to set up a quick call or provide more details via email.

Looking forward to hearing from you!

Best,
[Your Name]
[Brand Name]
[Your Position]
[Company Website]

ChatGPT was not done there, however. (Un?)Helpfully, at the end of this prompt, the AI threw in the following:

🚩 *Red Flags of a Scammy Sponsorship Email*

1. ***Generic greeting*** *("Dear Sir/Madam" instead of your actual name).*
2. ***Poor grammar/spelling*** *(legit brands have professional communication).*
3. ***Unrealistic offers*** *(e.g., thousands of dollars for a small channel).*
4. ***Weird email address*** *(e.g., random Gmail instead of an official domain).*
5. ***Requests to download files or sign in*** *(phishing attempts).*
6. ***No clear details*** *about what they expect from you.*

Great! We will be sure to avoid putting any of these red flags in our phishing attempt.

Next, let’s decide what kind of sponsor we are. ChatGPT provided a list of potential companies: gaming peripherals, skincare and software. Gaming peripherals are easy enough; assuming we have no knowledge in this area, I asked ChatGPT: “What are the most popular gaming peripheral sponsors?” The list is too long to include here, but to be on the safe side, we will go with one of the companies further down on the list. Without putting in additional effort to figure out what sponsors the YouTuber already has, our chances are probably better with a less well-known brand. We will choose number eight on ChatGPT’s list, which was a provider of “gaming monitors, motherboards and graphics cards.”

The next step should be obvious. Ask ChatGPT: “Can you write an example sponsorship email from this company to [Influencer’s name] for a new gaming motherboard?”

All these prompts took less than five minutes to create. Another few minutes to review the draft and make sure none of those pesky “red flags of a scammy email” are present, and our phishing email is ready.

The email could be finished and sent from a throwaway account without additional work. Maybe it catches the influencer on a bad day and they take the bait, responding to the email and initiating a conversation that the attacker ultimately steers toward following a link to a fake website or clicking a spoofed link to sign a contract on DocuSign.

If the attacker is motivated enough, there are additional, more involved steps they could take. Spoofing email addresses is more common than most people would like. Additional research, perhaps again helped by AI, on social media (LinkedIn, X, etc.) can reveal individuals with sponsorship responsibilities employed by a company. Instead of coming up with a good-enough fake name and email address, now an attacker has a real person to impersonate. Perhaps, just in case the target is particularly cautious, we will include a link to the employee’s social media accounts. If the potential reward is substantial enough, the attacker can spend time copying the entire X (formerly Twitter) account of this employee and pay for “verification” on the X platform, providing a link to the fake account in their phishing email. If the target takes the time to verify the attacker’s fake identity and reach out on X, they will find an account, a picture and maybe even some posts. The attacker will be able to respond to X messages sent to the fake account and keep the charade going. Add in a deep faked teleconference, and who wouldn’t click a link to sign a contract for a big payday?

Now, imagine the target is someone at your organization. What kinds of real emails do they see every day? Maybe ChatGPT’s answer is not as clear as our example above, so the attacker is forced to pivot. Instead of working off the person’s occupation, the attacker can go to social media, identifying what the actual individual desires. Perhaps they have one too many posts about their gardening or photography hobby. "Hey ChatGPT, what kinds of emails would a gardener be interested in? What would a “seasonal gardening guide” email look like? What would a trustworthy source be for seasonal gardening guides?" Next thing you know, a hobbyist gardener who manages database access for your organization receives an email from the American Horticultural Society with an enticing link to a guide specifically created for her hardiness zone.

Playing Defense

Fortunately, some of the tools phishers use are also being implemented to help defend against these targeted attacks. Automated tools are scouring emails for dodgy links and just-not-quite-right email addresses, but they will never be fully successful at keeping them out of our collective inboxes.

Ultimately, it is up to each and every individual to maintain constant, at times exhausting, vigilance against phishing attempts. It is especially important to avoid being lulled into feeling secure because we have become adept at spotting typos or translation errors, or hovering over links to reveal unrecognizable spaghetti, in our texts and emails. Attackers are better equipped to make fewer mistakes and figure out what shiny lure to dangle to get us to drop our guard.

WHAT WILL BE THE IMPACT OF CHATGPT ON OUR BUSINESS?
THERE'S A LOT WE DON'T KNOW FOR SURE...
LIKE HOW MUCH OF WHAT IT SAYS IS MADE UP...
OR IF IT WILL TAKE AWAY OUR JOBS...
OR THE SECURITY RISKS...
OR IF IT COULD DAMAGE OUR REPUTATION...
WHAT DO WE KNOW FOR SURE?
ONLY THAT WE WANT TO ADOPT IT EVERYWHERE AS FAST AS WE CAN.
TOM FISH BURNE
© marketoonist.com

Overcoming Rejection

March 12, 2025
By Larry Benson
https://fraudoftheday.com/overcoming-rejection/

When Three Brothers Supermarket didn't get approved to redeem Supplemental Nutritional Assistance Program (SNAP) benefits, owner Jenny Tejada didn't let that stop her from being a SNAP retailer. She got creative, by becoming a fraudster in a scheme that stole almost $2 million in SNAP benefits to support her store.

Tejada gained access to the program by stealing merchant identification (MID) numbers that had been assigned to local stores that participated in the program legitimately. By using the stolen MID numbers, Tejada was able to work around the rules of SNAP and accept the benefits to purchase groceries in her store. But she didn't stop there! Tejada further abused the program by trading benefits for cash. A side hustle that stocked her store shelves with groceries she bought at other stores with the fraudulently gained SNAP benefits.

Numbers didn't add up for the Department of Agriculture and upon an investigation, found Tejada guilty of food stamp trafficking. The illegal buying, selling or exchanging of SNAP benefits. Trafficking in SNAP Benefits is the worse offense an EBT retailer can be accused of. It's also the most common SNAP violation that the USDA charges. Approximately 12.7% of authorized SNAP stores engage in trafficking. And Tejada wasn't even authorized! She trafficked with MID numbers she stole from other stores.

Tejada is trading in her grocery store for a prison cell. On February 5, 2025, Tejada was sentenced to 18 months in prison for SNAP fraud. She was also ordered to pay $1,841,402 in restitution and forfeit the proceeds of her offenses.

Great job by the U.S. Department of Agriculture Office of Inspector General in this case.

Today's Fraud of The Day is based on article "Pennsylvania woman sentenced for nearly $2 million in SNAP fraud" published by ABC News on February 5, 2025.

A Philadelphia store owner has been sentenced to more than a year in prison after defrauding the Supplemental Nutrition Assistance Program (SNAP) of nearly $2 million.

The U.S. Attorney's Office in the Eastern District of Philadelphia says Jenny Tejada was charged after using her corner grocery store to redeem SNAP benefits, even though she knew the store had not been approved to participate as a merchant. Investigators say Tejada gained access to the program by misappropriating merchant identification numbers that had been assigned to other stores. In addition to an 18-month prison sentence, Tejada will have to pay $1,841,402 in restitution and forfeit the proceeds of her offenses.

Not The First Mix-Up

April 7, 2025
By Larry Benson
https://fraudoftheday.com/not-the-first-mix-up/

There are at least four women with the name Sandra Martin in Broward County, FL. Three of them didn't think much of it. But one of them thought of fraud and using the other Sandra Martin identities went on to scam Broward County out of thousands of dollars in COVID relief rental assistance funds. It's not the first there was a Sandra Martin mix-up, but it might be the first time a sheriff had to get involved.

Last year, one Sandra Martin got a call from the Broward Sheriff's Office asking if she was renting out her Deerfield Beach home. County records showed her property was being rented out, had a homestead exemption, and had supposedly received thousands of dollars in COVID rental assistance relief funds. Homestead exemptions are typically available only for primary residences. Therefore, they did not qualify for COVID-19 rental aid that was established to help with unpaid rents that had left investment property owners struggling to make their mortgage payments related to their real estate businesses.

There were four properties owned by a Sandra Martin in Broward County – all four received COVID rental aid. Luckily repeated payouts to the same name set off alarm bells for crimes against property at the Broward Sheriff's Office. And they quickly found their fraudster. Sandra Janet Martin from Lauderhill. She had assumed the identities of all these other Sandra Martin's that owned properties in Broward Count to apply for rental assistance to the tune of $80,000.

On March 31, 2025, Sandra Janet Martin was found guilty of COVID-19 Relief fraud.

Shout out to the Broward County Sheriff's Office.

Today's Fraud of The Day is based on article 'I had no idea': This Maryland snowbird's Florida beach home was embroiled in an identity theft fraud scheme — how one scammer took a small coincidence and turned it into $80K" published by Money Wise on March 31, 2025.

For Sandra Martin, sharing a name with three other women in Broward County seemed like a harmless coincidence — until it made her the target of identity theft. According to NBC 6 South Florida, the 62-year-old snowbird from Maryland learned that her Deerfield Beach home was fraudulently listed as a rental. Apparently, it was tied to thousands of dollars in COVID relief funds — money she never applied for.

"I was very surprised, I had no idea," Martin told reporters. Investigators discovered that another Sandra Janet Martin from Lauderhill had assumed the identities of multiple Sandra Martins in Broward County.