LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Sourced from World Art News

In This Issue

Fraud Talk Podcast

Scam's Calling: Unraveling the Robocall Racket - Alex Quilici - Fraud Talk - Episode 136

"We've been trying to reach you about your car's extended warranty" is an all-too-common robocall scam aiming to bilk victims out of their money. Alex Quilici, CEO of YouMail, discusses the intricacies of robocalls, what differentiates beneficial robocalls from scams and the regulations that both aid and obstruct the fight against these schemes with Jennifer Lieberman, assistant editor of Fraud Magazine, in the latest episode of Fraud Talk.

https://acfe.podbean.com/e/scam-s-calling-unraveling-the-robocall-racket-alex-quilici-fraud-talk-episode-135/

UPCOMING EVENTS

LOCAL:

Twin Cities ACFE and Central Ohio Chapter Present:
Wirecard Scandal
Virtual
November 8, 2023
LACFE Members in good standing are eligible for the 'membership rate'.
Learn more: https://twincitiescfe.org/meetinginfo.php

Michigan Chamber of Commerce: The State of Michigan Business – A 2024 Outlook
Virtual
November 9, 2023
9:30-11 a.m.
Learn more: https://www.michamber.com/mibusiness2024outlook/

ACFE Southwest Ohio Chapter
5th Annual Dayton Fraud, Cyber & Ethics Conference
In-Person/Virtual
November 15 - 16, 2023 (early registration ends October 31st)
Learn more: https://swohacfe.org/event-5351176 and see poster below!

Behavioral Forensics Group, LLC
(partnering with the Lansing Chapter of the ACFE)
Virtual Fraud Symposium
December 6-7, 2023 (early registration ends November 23rd)
Lansing Chapter receives 40% of the fee for LACFE members that attend. Use code: MI143
Learn more: https://my-cpe.com/virtual-events-detail/event/virtual-event-fraud-symposium

ACFE Southwest Ohio Chapter: Fraud Vulnerabilities in Today's Contracts
Virtual
December 8, 2023
12:00 – 2:00 pm
Learn more: https://swohacfe.org/event-5352987

NATIONAL:

ACFE Controlling the Risk of Asset Misappropriation
Virtual Seminar
December 12-13, 2023 (early registration ends November 13th)
Learn more: Event Details (acfe.com)

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article, please contact Jennifer Ostwald at jenny1661@hotmail.com

2023 CHAPTER OF THE YEAR
SOUTHWEST OHIO CHAPTER

ACFE
Association of Certified Fraud Examiners
Southwest Ohio Chapter

5th Annual DAYTON FRAUD, CYBER & ETHICS CONFERENCE

NOVEMBER 15 & 16, 2023

12:00PM-4:30PM EASTERN

VIRTUAL CONFERENCE *(HELD ON ZOOM)*

8 total hours of CPE* *(4 each day)*
(including 2 hours of Approved ACFE Ethics/Ohio PSR Ethics credit)

Co-sponsors:
AXIUM® CONSULTING
University of Dayton Center for Cybersecurity & Data Intelligence

Pricing: EARLY BIRD *(By October 31, 2023)*
$75 one day | $100 both days
Regular Price: $100 one day | $125 both days

REGISTER AT: **https://swohacfe.org**

*CPE credits are based on a 50-minute hour. CPE is offered through the ACFE as well as the Accountancy Board of Ohio (sponsor number CPE.00467).

NOVEMBER 15TH

ADAM LAWSON
Supervisory Special Agent, FBI Cincinnati – Cyber Squad
1 CPE

FBI Overview of the Cyber Threat Landscape

Mr. Lawson's FBI cyber team covers the lower 48 counties of Ohio for cyber intrusion matters. Mr. Lawson will provide an overview of the cyber threat landscape to include a description of threat actors and their motivations, the most common methods of cyber attacks, what to expect from the FBI after reporting an attack, and lessons learned from the victim's perspective.

JENNIFER MACKOVJAK *CFE, PI*
ANDREW KEITH *PI*
Co-founders and Partners, 221B Partners
1 CPE

A Look Under the Hood: What You Don't See if You Stop with Databases

Databases and municipal, state, and federal information and records indices provide invaluable research leads but typically don't tell "the full story." This presentation will highlight the importance of obtaining information from primary sources and not just relying on database records, court and government portals, and secondary sources.

HARRY LIDSKY
Special Agent in Charge (retired), U.S. Department of Justice and Founder, 4th Dimension Investigative and Security Solutions (4DISS)
2 CPEs

Off-Beat: Fugees Founder Pras Michel's $100,000,000 Failed Attempt to Influence President Trump and the DOJ

Mr. Lidsky will present a case study focusing on the domestic arm of an international conspiracy. He will discuss how Fugees band member Prakazrel "Pras" Michel organized a small group of co-conspirators seeking to facilitate the dismissal of the 1MDB investigation and secure the extradition of a Chinese asylum-seeker at the request of Low Taek Jho, a.k.a. Jho Low, the alleged mastermind behind the 1MDB scheme, and subject of the bestseller book "Billion Dollar Whale." Michel's group aspired to influence the top echelons of the US government, including the President of the United States and the Attorney General of the United States.

NOVEMBER 16TH

MARY BRESLIN *CFE, CIA*
Founder & Managing Partner, Verracy
ACFE 2023 Baker Award Recipient
1 CPE

Unveiling the Thrilling World of ChatGPT and Fraud Detection

ChatGPT isn't just a buzz term; it's a gateway to a whole new level of intrigue and deception. In this session, Ms. Breslin will delve into the cutting-edge applications of ChatGPT and explore the innovative ways in which fraudsters are exploiting its power to commit fraud. But that's not all! Get ready to witness a captivating showdown as we reveal how ChatGPT and other awe-inspiring AI tools can become formidable allies in the fight against fraud. Don't miss this face-off between deception and defense, as we unlock the potential of ChatGPT to empower fraud-fighters worldwide.

PIERRE RIVOLTA *Ph.D., CFE*
Associate Professor, Department of Criminology and Criminal Justice - Mount St. Joseph University
1 CPE

Fraud Theory, Revisited: An Examination of the Fraud Triangle and Competing Explanations For Fraud and Other Financial Crimes

In this session, Dr. Rivolta will summarize academic research on fraud theory, with a particular emphasis on the "fraud triangle." Attendees will learn about the origins of the fraud triangle, examine its empirical assessments, review its geometric (and other types of) evolutions, ponder its limitations and criticisms, assess its relevance to practitioners, and contemplate other theories of fraud causation.

ANTHONY J. MENENDEZ *MSA, CPA, CFE*
George A. Dasaro Distinguished Clinical Assistant Professor of Accounting, Loyola Marymount University
ACFE 2016 Sentinel Award Recipient
2 Ethics CPEs

A Whistleblower's Tale

Mr. Menendez is the renowned "Accountant Who Beat Halliburton" and a corporate whistleblower under Sarbanes-Oxley whose work ultimately led to significant advancements in protections for corporate whistleblowers. In this presentation, Mr. Menendez will recount the key events that led him to blow the whistle on oil giant Halliburton, and he will detail the ensuing fight for his livelihood, his credibility, and his family during a decade-long legal battle.

Thanksgiving

In the blink of an eye,
life moves us from
give to borrow,
bliss to sorrow.

Ever-changing,
flowing,
sometimes staccato-like.
Moving us,
kneading us,
reshaping us.

Requiring us
to reflect, rejuvenate;
finally absorbing
what we always avoided.
Forcing a much deeper
understanding, making us
better, more whole.

Allowing us to
sense things,
rather than
just see things.
Finally, we approach the
truth.

Discovering our real worth,
of what we're made,
what we've become.

All the pieces are here,
even those who aren't.
Our family's fabric
woven together –
sinewy and strong.

Reunited, rejuvenated,
regenerated –
everyone sustaining
the present, preparing
our future preserving
the past.

New and old blend
together.
Year in year out, life gets
better.

November 12-18, 2023
Join the global effort to minimize the impact of fraud by promoting anti-fraud awareness and education

Find details and shareable information at https://www.fraudweek.com/

What You Can Do

Fraud Week is the perfect time to go a step further in your role as an anti-fraud professional and to start discussions amongst peers, coworkers, executives and stakeholders in your community about how important fraud prevention is to society as a whole. You can use any of the free resources provided, or get creative and put your own twist on some of the ideas presented below.

Ways to Get Involved

- Post on social media using informative images with the tag **#fraudweek**
- **Invite a CFE** to talk to your employees and coworkers virtually on how to avoid common mistakes when preventing fraud.
- Download the **free Fraud Week logo** to share on materials or websites.
- Involve your local chamber of commerce or city council to **spread tips on fraud prevention** for small businesses.
- Encourage your governor to **issue a proclamation** declaring that your state supports Fraud Week.
- Issue a press release showing your organization's support by using this **customizable press release template**.
- Host a talk or seminar for your coworkers or community on regularly staying aware of fraud prevention best practices. You can **post that event** to share what you are doing on our events page.
- Perform a **fraud check-up** for your organization and present your findings to executives, as well as a proactive plan for how to remedy weak spots in your current controls.

Your Spam Blocker Won’t Protect You from This New Email Scam—Here’s What to Know

by Jaime Stathis
https://www.msn.com/en-us/lifestyle/smart-living/your-spam-blocker-won-t-protect-you-from-this-new-email-scam-here-s-what-to-know/ar-AA1iY0FP

Just as we become savvy to the latest online scams, con artists come up with another clever way to evade our email providers' spam blockers. Phishing is one of the most common types of cyberfraud—where the ultimate goal is to steal your personal information or install spyware or ransomware on your device—and scammers are always looking for new ways to trick you.

"Cybersecurity is the ultimate game of cat-and-mouse, which means it's at least partially reactive," says Monica Eaton, owner and founder of Chargebacks911. "Fraud threats are constantly evolving, and unfortunately, cybercriminals never stop seeking new and novel ways to defraud victims."

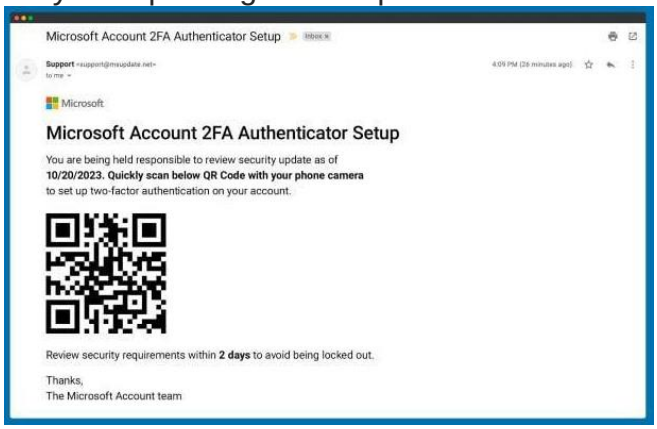
But what's new in the world of email scams? It's called quishing—the latest iteration of phishing—and there are a few things you should know to stay safe.

What is this new email scam?

A new form of phishing, quishing is designed to bypass spam filters. To accomplish this, cybercriminals do not include words in the body of the email. Instead, they use a QR code. According to Paul Bischoff, a privacy advocate at Comparitech, quishing is a standard phishing scam in which recipients are tricked into navigating to a fake login page controlled by the attacker. "Instead of a link or attachment, however, it urges recipients to scan a QR code," he says. If you receive a quishing email, you'll open it and see what looks like a legitimate QR code, and there may also be words instructing you to scan the code.

There isn't data on how many people have fallen for this email scam just yet, but security researchers at Inky, which specializes in phishing solutions, have identified 500 emails targeting various organizations in the United States and Australia.

Why can quishing evade spam blockers?



"The best way to understand how and why this scam is so successful is to take a step backward and consider the thought process that originally created your email's anti-spam protection," Eaton says. Spam filters are designed to read words, but scammers have gotten clever and embedded words into an image that contains both text and a fake QR code.

Since they are simply image files, QR codes do not trigger spam blockers, says Chris Hauk, a consumer privacy champion at Pixel Privacy.

Standard text analysis doesn't work on images, and filters won't detect the words embedded within the image. "Spam filters normally analyze text to determine whether a message is spam or not, such as scanning for common keyphrases used by scammers," Bischoff explains, which is why this new email scam sneaks through even the sturdiest spam filters.

Who is at risk?

So far, quishing scams have focused on companies. These emails ask employees to click the link to update their information. But Hauk cautions that anyone with an email address can be targeted. "While phishing schemes targeting companies make the headlines, plenty of phishing schemes target regular users too," and that includes the fake QR code scam.

What can happen if you fall for this scam?

"You may be tricked into paying money to the scammers," Hauk says, adding that the QR code could install malware onto your device or computer. Bischoff warns that victims may also be tricked into handing over account usernames and passwords, which is why strong passwords and two-factor authentication are so crucial to helping you stay safe online.

Bischoff adds that bad actors sometimes pose as authority figures and try to get you to fork over money to pay a bogus bill or other fabricated fees. The goal is to make you act out of fear.

How can you identify and avoid a quishing scam?

Don't click on QR codes in unsolicited emails. "While they are convenient to use, QR codes can contain all sorts of malicious surprises," Hauk says, and the risk isn't worth it. But what if you're worried that the sender is legitimate and follow-up is required to avoid consequences? In that case, you should carefully look at the sender's email address and ensure there isn't an extra dot, dash or underscore, which may signify an imposter account.

Eaton says that people reason with themselves, thinking if the email wasn't official, their email filter would've flagged it. But she points out that users can be lulled into a false sense of safety. "There's a psychological aspect to this scam as well: QR codes look official," she adds. "Most people don't have the know-how or IT skills to make QR codes on their own, so it's more plausible for them to assume that this fancy-looking code must've come from a reliable, official source."

What should you do if you fall for this scam?

If you fall for this QR code email scam, take the same steps as you would for any scam. "Contact the authorities, keep an eye on your banking and credit card statements, monitor your credit and perhaps even put a freeze on new accounts," Hauk says.

Other tips to avoid email scams

Eaton points out that cybercriminals are some of the most creative, out-of-the-box thinkers, and sometimes, it's almost admirable how much ingenuity can go into their schemes. "But when you stop and consider the harm they're doing to innocent, unsuspecting people, you feel less admiration and more concern: One bad actor with an ounce of creativity can trigger widespread havoc on an international basis," Eaton says. Here are some other tips to avoid email scams.

- Never scan unsolicited QR codes.
- Never provide your personal information in response to an unsolicited request.
- Never click a link or open an attachment in an unsolicited email or message.
- At work, take your IT department's cybersecurity training seriously.
- IT departments should allocate resources to prevent future actions, not just based on employees' past actions. "Yes, it's always good to know what's happened in the past, and someone's previous behavior is often indicative of future actions," Eaton says. "But if you're only focusing on what's already been done, you're going to have a gaping blind spot in your cybersecurity: When a criminal tries a new tactic or a new scam, you won't be ready. You won't even see it coming until it's too late."

Video of the Month

What is Fraud Week? - YouTube

Every November, hundreds of organizations around the world pledge to increase fraud awareness in their workplaces and communities. Learn more about the ACFE's annual International Fraud Awareness Week in this short video.

Social media: a golden goose for scammers

By Emma Fletcher
October 6, 2023
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers

Scammers are hiding in plain sight on social media platforms and reports to the FTC's Consumer Sentinel Network point to huge profits. One in four people who reported losing money to fraud since 2021 said it started on social media.[1] Reported losses to scams on social media during the same period hit a staggering $2.7 billion, far higher than any other method of contact. And because the vast majority of frauds are not reported, this figure reflects just a small fraction of the public harm.[2]

Social media gives scammers an edge in several ways. They can easily manufacture a fake persona, or hack into your profile, pretend to be you, and con your friends. They can learn to tailor their approach from what you share on social media. And scammers who place ads can even use tools available to advertisers to methodically target you based on personal details, such as your age, interests, or past purchases. All of this costs them next to nothing to reach billions of people from anywhere in the world.

Reports show that scams on social media are a problem for people of all ages, but the numbers are most striking for younger people. In the first six months of 2023, in reports of money lost to fraud by people 20-29, social media was the contact method more than 38% of the time. For people 18-19, that figure was 47%.[3] The numbers decrease with age, consistent with generational differences in social media use.[4]

Image

The most frequently reported fraud loss in the first half of 2023 was from people who tried to buy something marketed on social media, coming in at a whopping 44% of all social media fraud loss reports. Most of these reports are about undelivered goods, with no-show clothing and electronics topping the list.[5]According to reports, these scams most often start with an ad on Facebook or Instagram.[6]

While online shopping scams have the highest number of reports, the largest share of dollar losses are to scams that use social media to promote fake investment opportunities.[7] In the first six months of 2023, more than half the money reported lost to fraud on social media went to investment scammers. To draw people in, these scammers promote their own supposed investment success, often trying to lure people to investment websites and apps that turn out to be bogus. They make promises of huge returns, and even make it look like an "investment" is growing. But if people invest, and reports say it's usually in cryptocurrency,[8] they end up empty handed.

After investment scams, reports point to romance scams as having the second highest losses on social media. In the first six months of 2023, half of people who said they lost money to an online romance scam said it began on Facebook, Instagram, or Snapchat.[9] These scams often start with a seemingly innocent friend request from a stranger followed by love bombing and the inevitable request for money.

Here are some ways to steer clear of scams on social media:

- Limit who can see your posts and information on social media. All platforms collect information about you from your activities on social media, but visit your privacy settings to set some restrictions.
- If you get a message from a friend about an opportunity or an urgent need for money, call them. Their account may have been hacked—especially if they ask you to pay by cryptocurrency, gift card, or wire transfer. That's how scammers ask you to pay.
- If someone appears on your social media and rushes you to start a friendship or romance, slow down. Read about romance scams. And never send money to someone you haven't met in person.
- Before you buy, check out the company. Search online for its name plus "scam" or "complaint."

To learn more about how to spot, avoid, and report scams—and how to recover money if you've paid a scammer—visit ftc.gov/scams. If you spot a scam, report it to the FTC at ReportFraud.ftc.gov.

Quote of the Month

"The fraudster's greatest liability is the certainty that the fraud is too clever to be detected."

— Louis Joseph Freeh, attorney and former judge who served as the fifth Director of the U.S. Federal Bureau of Investigation.