

No Need for Cyber Skills? Let's Go to the Board: Global Stats to Empower Your Incoming Skillset

BY **CHRISTOPHER SALGADO**,
CEO OF ALL POINTS INVESTIGATIONS, LLC

Mr. Dupable was elated! Elated to sit down and engage in his festive, family obligation of shopping for a birthday gift for his teenage niece – who defines super glam and modernization!

He fires up his latest laptop that, for some reason, has recently given him several problems. No matter... that 7-year warranty reminds him that he can engage IT support for the numerous tech problems at another time. Curious that this laptop is only a few weeks old but, alas, a problem for another day.

A smile crawls across his face as Mr. Dupable realizes his success in booting up his computer. With no hesitation, he enters the magical world of online goodness!

His carnal instincts briefly pull his eyes to his encrypted messaging app. No alerts indicating any message from his recent online partner. He then continues in his journey for his niece by logging into his social media account. He clicks on his niece's account and searches for her recent declaration of her birthday desires.

A quick find. He sees her recent post claiming her pseudo need for a white-colored cross body purse made by the most popular – and expensive – brand that he knows of: AwesomeGoodness. While he's familiar with this brand, the cost is unknown to him – besides it being expensive. "Ah!" he exclaims. "Of course," he follows up with.

As rough as this one may be, he realizes that he's a bit behind in purchasing a gift due to the recent hefty workload he's had. Again, being the glam girl that his niece is, he knows she's got an eye for top-shelf items. A hard swallow is followed up with a search on Google for the cross-body purse. Several purchase options present themselves on the SERP (Search Engine Results Page). As expected, all appear to be out of his price range.

He then recalls hearing about a market online offered by his preferred social media platform. He returns to his profile and begins searching for the same purse. Almost instantly, he finds numerous profiles offering the same bag for significantly less. Skeptical, Mr. Dupable scopes out the best offering that appears legit. Voilà! A goldmine! Mr. Dupable discovers a profile that seems to offer plenty of what he's looking for in an acceptable amount.

Elated once again, he confirms the details of the bag and the seller.



Conveniently located not too far from him, local pickup is requested. Ultimately, it's honored by the seller.

The next evening, Mr. Dupable feverishly drives from his work to the destination chosen by the seller. A bit of an odd spot but, once again, he's grown desperate due to the time constraints. He arrives at the location and sees his seller standing near the park bench, as relayed.

Mr. Dupable parks his vehicle, exits it and starts walking towards the seller, trying to avoid as much rain as possible in the quickly darkened night. Just as he begins his walk, his cell phone shines as a chime calls out from it; an alert from his online honey. Mr. Dupable neither hears the chime nor sees the light as it barely lights the inside of his jacket pocket. Too bad, too. His female counterpart was expressing her dire need for \$2,500 due to her mother's house being foreclosed on. This is all of the shortage needed to avert such a painful process. Alas, Mr. Dupable will never know of this endearing request. His fate calls for a different response. That is, because as he extends his right hand to shake the same of his seller, his seller raises a hidden machete from the park bench. Thunder consumes the audible sounds demanding life-assistance from Mr. Dupable.

As his body falls onto the saturated grass, his phone bounces out of his jacket pocket. Another chime and backlight occur from his phone. It's a frantic call from his sister. She leaves a voicemail screaming for him to come to her house immediately. Her teenage daughter, his niece, has just committed suicide due to a sextortion attack.

Let's shake that one off. A bit rough at the end, but all are inspired by

similar scenarios that have played out in people's lives. The above story highlights a romance scam, a fraudulent online ad and a sextortion attack. A sort of trifecta to make a point. While all of us are likely aware of all three scams, some of us may be reserved to the idea that our world is not as damning or is improving – to the benefit of the good guys and gals. I must respectfully squash those thoughts. Even still, some of us may turn a blind eye to the far-reaching impact of online attacks. Perhaps the latter is out of ignorance or a need to bury the cruelty inside the ostrich syndrome.

The type of online scams far exceeds the three above, although the outcome of the three can be dire. Nonetheless, to illustrate some of the current impacts, below are numerous statistics citing various threats, platforms, demographics (victim) throughout the globe. (Stats are not my own and are referenced below.)

GLOBAL OVERVIEW:

- **Total Global Losses:** > \$1T stolen globally in the past year ("Global State of Scams Report 2024," Global Anti-Scam Alliance (GASA))
- **United States:** >\$16B lost in 2024, per FBI – a 33% increase from 2023 (CBS News)
- **Australia:** >\$2.5B lost in 2023, with scams often involving deepfake technology and social media platforms (*The Australian* (2024))
- **Singapore:** >46K scams were reported in 2023 in Singapore; losses totaled >\$650M (ChannelNewsAsia.com)

ROMANCE & PIG BUTCHERING SCAMS (FINANCIAL GROOMING):

- Global Losses: >\$3.5B lost to romance scams and confidence schemes in 2023 ("Four Unexpected Insights on Romance Scams," Nasdaq Verafin)
- United States: >\$1B lost in 2023, with a median loss of \$2K per victim ("Romance Scams & IDV: The Battle Against Online Fraud," Regula)
- UK Finance reported >£1B was lost to fraud and scams in 2023 ("UK Finance Fraud Report Results: Banks Face a Perfect Storm of Change," Feedzai.com, 2024)
- Pig Butchering Scams: In 2024, a 40% increase in scam revenue was appreciated, contributing \$9.9B to the \$12.4B in loss by crypto scams ("Crypto scams likely set new record in 2024 helped by AI..." *Reuters*, 2025)

CRYPTOCURRENCY & INVESTMENT FRAUD:

- **Global Crypto Fraud:**
 - >\$9B lost in 2024, a 66% increase from 2023 (FBI, 2024)
- **United States:**
 - >\$6.5B in losses in 2024 (IC3.gov)

ACCOUNT TAKEOVERS & IDENTITY THEFT:

- **Account Takeovers:**
 - "99% of orgs monitored by Proofpoint experienced ATO attempts; 62% suffered at least one successful attack" ("Proofpoint Research: 2024 Account Takeover Statistics," Proofpoint)

- ATO fraud resulted in >\$15.5B in losses in 2024; up from >\$12.5B in 2023 (AARP and Javelin Identity Fraud Study)
- 24% of consumers experienced ATO incidents in 2024; an increase from 18% in 2023 (Spycloud.com)

• Identity Theft:

- In 2024, 34% of Americans fell victim to identity theft ("American Fraud and Identity Theft Statistics 2024," Investment Property Exchange Services, Inc.)
- >1M identity theft reports filed in 2024, marking a 9.5% increase from 2023 (FTC)
- American adults lost \$47B to identity fraud and scams in 2024, an increase of \$4B from 2023 ("Identity Fraud and Scams Cost Americans \$47 Billion in 2024," AARP)

• Sextortion:

- United States: The National Center for Missing & Exploited Children (NCMEC) received >26K reports of sextortion in 2023, up from >10K in 2022, a 149% increase.
- Canada: The Canadian Centre for Child Protection reported sextortion cases having tripled in 2022 ("Teen boys make up majority of victims of recently reported sextortion crimes, new data shows," CBC/Radio-Canada)
- United Kingdom: The Internet Watch Foundation (IWF) claimed an increase in sextortion reports of 8 times from prior reports in 2023 ("Teenage boys targeted as hotline sees 'heart-breaking' increase in child 'sextortion' reports")
- Australia: One sextortionist was believed to have sextorted 286 victims ("How sexual predators are using social media and dating apps to target women and children in Australia," 2025, News.com.au)

Given the above stats – coupled with the many unlisted here for sake of conciseness – highly concerning odds foretell that 1 in 2 persons will be engaged by some sort of scam while they are online. Even more concerning are the more aggressive odds that claim many of those engaged by scammers will be successfully victimized in the deployed scam. Furthermore, in general, your odds of being engaged by a scammer are significantly higher if you are in the U.S. and above the age of 65.

While I can go on and on, I believe the above stats make my point. Many investigators have confessed to me that the above offenses are above their paygrade. While adopting and rolling out a full-fledged cyber support system for clients can be daunting, it all begins with one step. So

- Asset & Witness Locates
- Market Sweeps
- CnD Service
- Criminal
- Seizures
- Death
- Fraud
- Civil



A GLOBAL INVESTIGATIONS FIRM
Former Facebook Investigator
Social Media Investigations
Cyber Investigations
Surface web • Deep web • Dark web

- Hazard Risk & Vulnerability Assessments
- Travel / Event / Property Risk Assessments
- Business Resiliency Assessments
- Competitor Intelligence
- Litigation Support
- Digital Forensics
- Social Media

Cyber Consulting!

www.AllPointsInv.com | info@allpointsinv.com | 408-365-4144 | Florida Agency License A1800260
Surveillance | Supply Chain | Corporate Security | Online & Brand Protection



"Big enough to serve and small enough to care."

Our Policy Is Designed For:

- Private Investigators & Detectives
- Forensic Investigators
- Accident Reconstructionists
- Consultants
- Background Checkers
- Attorney Services
- Process Servers
- Public Record Retrievers
- Insurance Adjusters

We Offer:

- Commercial General Liability
- Errors & Omissions
- Workers' Compensation
- Cyber Liability
- Crime
- Business Personal Liability
- Bonds

Free On-Line Quick Quotes



AMIS / Alliance Marketing
& Insurance Services, LLC

(800) 843-8550

www.amisinsurance.com
mnowell@amiscorp.com

CA Lic: 0K21904

how can you assist as effectively as possible by onboarding a litany of cyber skills? These days, there are numerous ways for you to start acquainting yourself with the tools and methodologies necessary to identify, monitor and take down bad actors online and, yes, even hackers! The latter will really test your skills. In the name of safety, let's build up to taking down hackers. After all, you don't want to poke a dragon.

Some first steps can include (1) building a cyber foundation to understand how websites and data work. This will allow you to ascertain a generic understanding of the digital landscape. (2) Learn the basics of OSINT. Obviously, this is the kernel of investigating online. While there are degrees as to how you can jump into understanding this world, a healthy starting point can include both the available OSINT data as well as the tools to engage such. The degree that you want to start with certainly goes far beyond Googling people and reverse image searching photos. It even goes far beyond your algorithm-based search companies that offer vanilla reports with a dozen or more of a subject's online accounts. I tell folks all of the time that my firm starts where these surface-based companies end. I recently had a discussion with a newer PI who appeared to praise one of these surface-based companies as the golden choice. I urge you, my readers, to go much further than that. Employ diligence in your cases and avoid regurgitating that false mantra.

Additionally, you can (3) read up on how to successfully memorialize online evidence that can be court-ready or acceptable to law enforcement. Once you've become familiar with the above three steps, I'd say it's time for you to choose your poison, so to speak, and identify if you want to specialize in a specific element of cyber/OSINT investigations. Options include the dark web, cryptocurrency, etc. Certainly, you can be a generalist and avoid specializing. It's simply your choice.

Many investigators have asked me if there is any official training that I prefer, such as a Certified Cyber Investigator (CCI) or such. I am less impressed with a piece of paper on your wall than the true knowledge required for the task. Keep in mind that the paper on your wall is only valuable because it is a testament to your skillset. I say, if you can showcase your skillset without a piece of paper, that's absolutely acceptable. Plus, you save a tree by not having that paper!

Regarding OSINT, I know there are some OSINT schools that claim to be universally accepted but I disagree that any of them are unequivocally universally accepted as the single source for OSINT training. This is because

OSINT is not governed by a specific international body – or even a national body, such as the American Medical Association (AMA), the American Bar Association (ABA) or the Federal Aviation Administration (FAA). OSINT is a decentralized discipline. As such, training programs vary significantly in scope. Yes, there are respected OSINT training institutions in the U.S. that offer OSINT certifications; however, they are not regulatory bodies, nor are they unequivocally universally accepted as OSINT standards across the U.S. Opinions vary on such sources. One employer may cheerlead for one training entity while another will tout the teachings of another.

Given the above, I don't officially stamp my approval on any of these institutions. Especially since my firm offers OSINT training directly. (AGGOSO Training™) (AGGressive Open SOurce intelligence)

Regardless of how you wish to get started, I say, do so! It's going to take an online village to support those who need our OSINT/cyber help. The aforementioned stats are crippling but not unstoppable. Yes, it will take a herculean task by many, many investigators but with power in numbers, we can begin to stifle the growing number of attacks, perhaps even save a life from a sextortion attack. So, I urge you to reconsider the idea that scams are above your paygrade. Join us in the fight and strengthen our collective, global impact against those who seek our money... and sometimes our lives. **PI**



Christopher Salgado is the CEO of All Points Investigations, LLC, a global cyber and physical investigative firm serving Fortune-listed corporations, law firms, and other entities. A former Facebook investigator, he brings over 20 years of

expertise in cyber investigations, OSINT, cryptocurrency, social engineering, and threat management. His work spans corporate risk, brand protection, cults, cyberstalkers, SIU matters and others. In 2024, he was named a Top Investigator by PI Magazine. Christopher is a member of the London Speaker Bureau and a keynote speaker at industry events, including CrimeCon. He has briefed agencies such as the FBI, DEA, HSI, CBP, Interpol, Europol and members of the EU Commission. He is also the Founder of Anti-Hackathon, an online safety initiative, and AGGOSO™ Training, an advanced OSINT education program. He may be reached at csalgado@allpointsinv.com