TOCQUEVILLE

Fool Me Once

July 22, 2026

It wasn't long ago that as long as we had McAfee or Norton installed, we felt protected from online threats. But viruses have become the least of our problems, as in today's digital age the most harmful threats are no longer found in a virus or malware – it's in the human mind. Everywhere we turn, we are being warned about financial scams. Are we being driven into unnecessary paranoia about scams and fraud or is there credible evidence to be concerned? Let's take a look…

Source: Cybersecurity Ventures

Multi-Trillian Dollar Industry

Just six years ago, cybercrime's cost to the world was estimated to be $2.9 trillion. With the exponential growth of AI, recent estimates put it at $10.5 trillion worldwide and global costs are expected to reach $12.2 trillion annually by 2031 (Source: Cybersecurity Ventures). If cybercrime was a country, it would have the third largest GDP in the world.

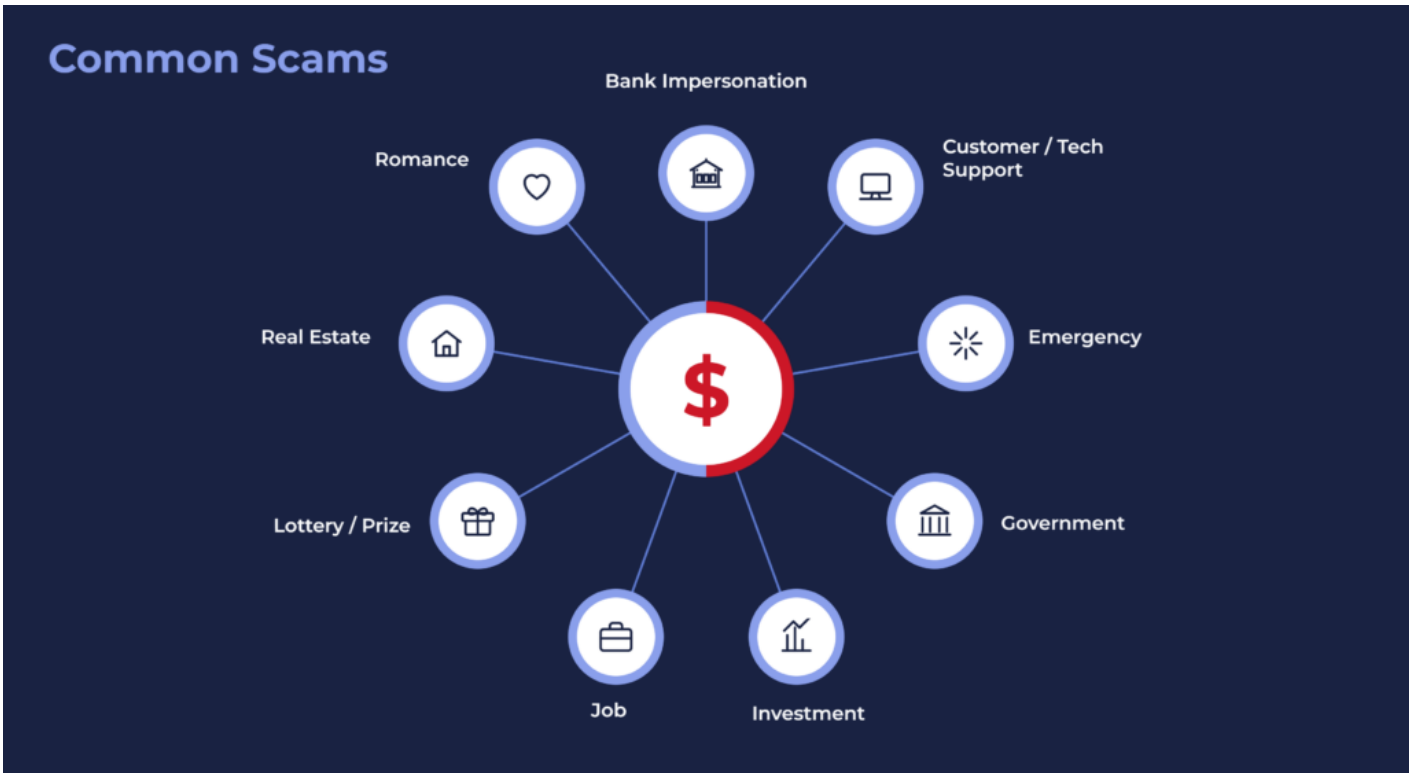
Source: Cybersecurity Ventures

Daily Assaults

According to AP-NORC Center for Public Affairs Research, 58% of U.S. adults say they receive daily texts, calls, emails, or online messages or ads they suspect are scams, and 92% encounter scam attempts at least once a month. Not all scams are after your bank or brokerage accounts, they could simply be an AI ad on social media trying to convince you to buy something, but all the testimonials are fabricated, and the product or service is ultimately a scam.   The New York Times recently investigated Fake Wellness Influences who are all AI generated and selling you so-called supplements. I'm sure as you're reading this, you are mentally reviewing the attempts you have recently been subjected to.

Social Engineering

Cybercriminals are described as sophisticated – but what exactly does that mean? Scammers use social engineering (psychological manipulation of human behavior) to get you to disclose your data, credentials and gain access to your devices. You willingly hand it over, as you believe they are a trustworthy party acting in your best interest. Victims may not be explicitly aware that they are authorizing illicit activity. These third-generation scams are designed to invoke empathy, fear and urgency in their victims, leaving you confused or pressured to comply.



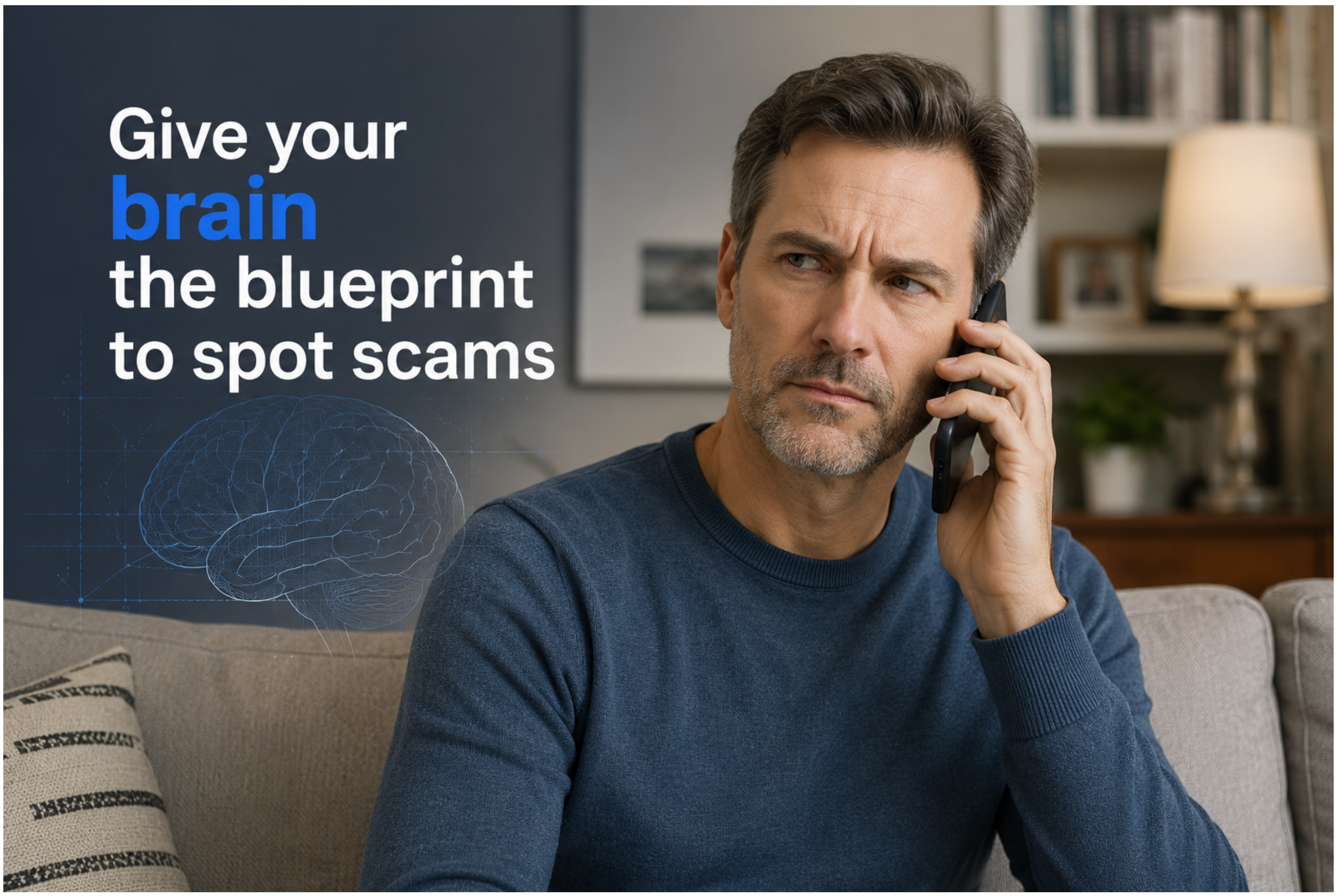
Who Are the Scammers?

We tend to think of scammers as some evil individual living in some far away country acting alone. However, these are huge international, crime rings with multiple layers of players. Scammers are willing to invest months of communications to build trust in **romantic and confidence scams**. They seem very genuine and it can be months/years before they eventually ask for money, usually a small amount to begin with and escalating to huge sums. **Investment scams** often involve crypto currency and will sound too good to be true, adding a layer of secrecy once they have gained your trust, saying you shouldn't tell anyone, as it will be 'our' secret.

Very often, the person on the other end of the phone or email is a human trafficking victim who is being forced to scam other people. There is a global human trafficking pipeline in the scamming industry, where both men and women victims were scammed into a fake job offer in another province/country. Interpol reports that there are 300,000 victims of fraud trafficking in South East Asia alone, which is deeply disturbing. Listen to Following the Trail episode on **BBC's Scam Secrets podcast** for a fascinating deep dive on this at the UN's Global Fraud Summit in Vienna.

The Blueprint

I was the Fire Warden at Tocqueville Asset Management LP for 15 years and being on the 19th floor of a Manhattan high rise, I took my job seriously. Lives were at stake. Part of my training involved reading the book The Unthinkable – Who Survives When Disaster Strikes, and Why. This book explains the importance of participating in building fire drills or reading the plane's safety pamphlet right before takeoff, because they give your brain the blueprint it needs of how to survive a disaster.



The same is true for scams — the goal isn't to make you paranoid, it's to give your brain a rehearsed response so that in the moment a scammer creates panic or urgency, some part of you already knows what to do.

When you receive emails from your financial institution about how to protect yourself from fraud, **read them**. Don't dismiss them as a waste of time, as they could very well provide your brain with the blueprint of how to spot a scam heading your way. Most people think they know already and wouldn't fall for such schemes, but you'd be surprised when your judgment is challenged, especially if you believe you are chatting on a text with a family member or friend. Their phone number or email address may have been compromised even though it’s the exact same number and email you have in your contacts. We can all be vulnerable and can be a target when we least expect it.

A Close Call at Immigration

On a recent trip to Colombia, I arrived in the immigration hall to a massive line, 85 degree heat and no air conditioning. During my tedious 2+ hours on the line, I overheard someone mention an Entry Form. I panicked as I hadn’t filled one out, so frantically I tried to connect to the Wi-Fi and googled to see how to fill out entry forms for my family. I clicked the suggested website and went through the laborious process of completing multiple forms and had to pay $130 each for “expedited processing” to get it by email immediately.   Only when I reached the Immigration Officer did I realize that I had been scammed. You didn’t need an entry form at all, and I had just provided all of our passport details and date of births, and money, to a fake website. Fortunately, I recovered my money, but my personal data is still out there floating on the web with scammers. If it can happen to someone who spends their career watching for red flags, it can happen to you on any ordinary day when you’re tired, hot, and just trying to get through a long line.

Myth – Only the Elderly are Vulnerable

Whilst the elderly are certainly a vulnerable class to being victimized as they may be socially isolated and may experience cognitive decline, do not believe the myth that you are safe if you are younger.

It seems counterintuitive, but Gen Z and Gen Alpha—despite being immersed in a digital ecosystem since birth — are falling for online scams at higher rates than their baby boomer grandparents.

Gen Z (born 1997–2012) and Gen Alpha (born 2013–2025) face greater risk than older generations when it comes to phishing attempts, romance scams, identity theft, and cyberbullying. These “Digital Natives” don’t feel comfortable talking live on the phone – they much prefer texting or “chatting” via app DMs. As such, they implicitly trust the digital space.

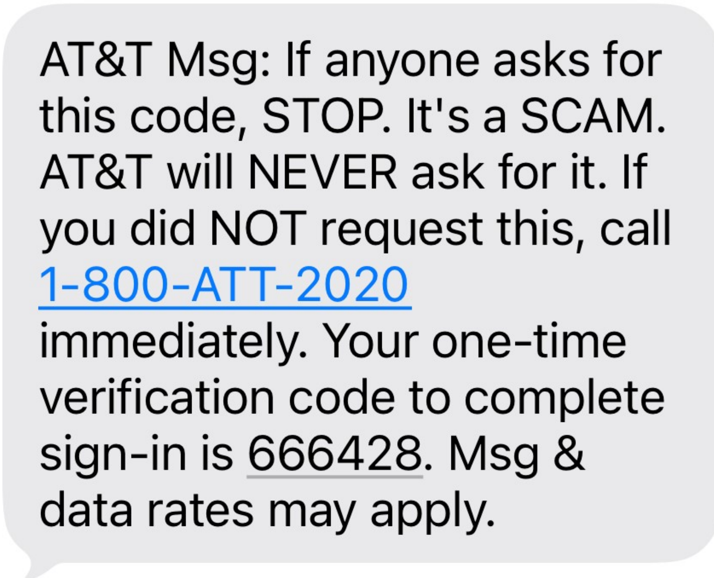
A 2024 Deloitte survey found that Gen Z and Gen Alpha are twice as likely to be scammed online compared to Baby Boomers. Drawing on nearly 4,000 responses, the study also revealed these younger groups experience social media account hacks at double the rate of older users.

Again, while many assume older adults are the primary targets of digital fraud, the data tells a different story: younger people are consistently on the receiving end of cyberattacks. Roughly 29% of Gen Z respondents reported having a social media account hacked, versus just 12% of older participants.

Critical Thinking

There are some key rules you may want to consider adopting:

- · Never share your **passwords** or give an agent your password.
- · Use **two-factor authentication** (MFA) whenever offered.
- · If a request for money is urgent or is unexpected, even from family, pause and call them back on a **known** contact number or the publicly listed number for a company.
- · If someone calls you from a financial intuition unexpectedly and says they'll **text you a link** to verify your identity, do not click it. Hang up and go to the official website instead to logon and chat with a representative, or call back on a known number.
- · Never click links in unsolicited emails or text messages – this could lead to a **takeover** of your accounts and identity.
- · Don't buy from or subscribe to **ads on social media**. Go directly to the official website on your browser.
- · Avoid sharing **sensitive information** on websites and in emails.
- · If anyone asks you to pay for services or products by **cryptocurrency** – this is a huge red flag for a scam.
- · Check the sender's **domain name** in the email address of suspicious or urgent emails.
- · Avoid mailing physical checks –it makes you an easy target for **check washing**.
- · Trust your **instinct** – if something feels off, slow down and hit pause before taking action.



No Shame

Sadly, victims of fraud and scams tend to feel an enormous amount of shame, so these crimes often go unreported. They feel it's their own fault for believing it was true, and that they should carry that burden and any consequences. They feel more like a fool than a victim of a crime. This is why global statistics tend to misrepresent how vast this crime is and how many people are affected each year.

When you have a deeper understanding of social engineering and how this could happen to anyone, no matter their intelligence, you can see clearly that shame does not belong here. Hopefully we can lift the shame for cyber fraud victims by having these types of conversations and sharing our experiences in hopes it can save someone else from the same outcome. "Shame must change sides" as French Icon Gisèle Pelicot so eloquently stated about her own case. The shame in these cybercrime cases, needs to reside with the Perpetrators, not the victims.

We hope that you have found this article useful.

We'd love to hear from you about your recent fraud or scam experiences and whether you escaped unscathed or whether you realized too late…

Natalie Blundell

Head of Client Services

This article reflects the views of the author as of the date or dates cited and may change at any time. The information should not be construed as investment advice. No representation is made concerning the accuracy of cited data, nor is there any guarantee that any projection, forecast or opinion will be realized. References to stocks, securities or investments should not be considered recommendations to buy or sell. Past performance is not a guide to future performance. Securities that are referenced may be held in portfolios managed by Tocqueville or by principals, employees and associates of Tocqueville, and such references should not be deemed as an understanding of any future position, buying or selling, that may be taken by