It's OK to make mistakes "Blame Culture" in Infosec

Courtney Bell

Rochester Security Summit, October 2023

cj@disorganizedjoy.com

whoami

- **Courtney Bell (FKA Courtney Imbert)**
- Cyber Operations Engineer, Sedara Security
- Purple team, red team / pentesting, security engineering, threat intelligence
- Living that infosec lyfe since 2001
- Master of Information Security Engineering, SANS Technology Institute
- BS Business Administration, SUNY Buffalo
- BA Psychology, SUNY Empire State (exp 2024)
- GIAC Security Expert (GSE), OSCP, other certs
- I make art

uname

- This is not a technical talk.
- This is the intersection of psychology and information security
- The “People” part of the PPT framework
- This is a call to action for organizations to acknowledge and even embrace human mistakes.

The root cause of all incidents is the creation of the universe.

The questions I asked in April 2023…

Scams have a unique trait among crimes: victims participate in their own victimization.

The "Just World" bias assumes that "people get what they deserve" (Montada et al., 1998). Victim-blaming is common for the victims of social engineering and scams (Cross, 2015).

- Do people hold victims responsible for the loss of money when they fall prey to scams?
- How much responsibility is allocated between the attacker and victim?
- Does a "guilty" (socially unacceptable) motivation for participating in a scam lead to more responsibility assigned to the victim than a benevolent one?

Methods

- Anonymous online survey, administered by sogolytics.com and distributed via Reddit, Facebook, and surveyswap.io
- Survey contained questions about demographics, and a few questions about the participants' experience with and perspective on scams
- Survey asked participants to allocate responsibility toward the victim or scammer in five different scam scenarios, sorted randomly (one anti-social scam, one pro-social scam, one "neutral" scam, and two distractors)
- 43 participants responded across all (adult) age ranges and a mix of genders, ethnicities, and levels of education / job roles.

Survey Materials

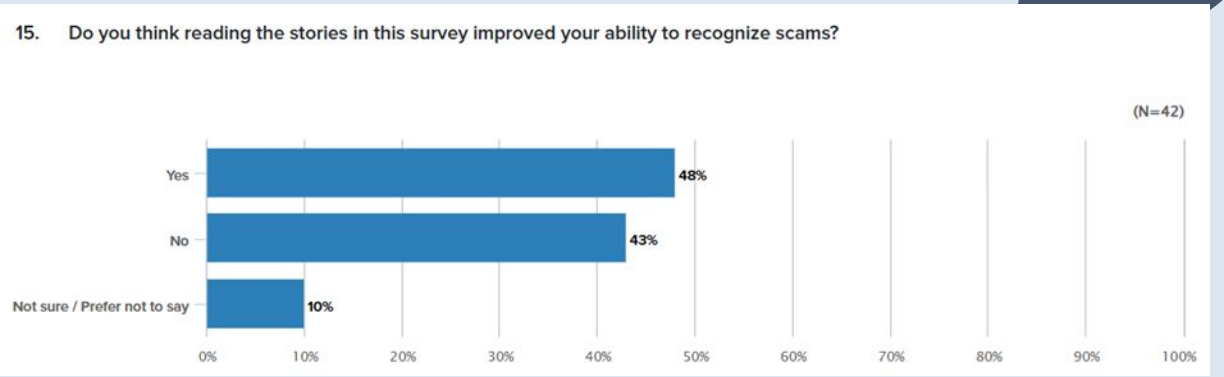
Category	Survey Question
Socially neutral premise	• Andy sent an email to Chris, containing a single web link. • Curious, Chris clicked on the link in the email. • The link led to malicious code that removed $1000 from Chris's bank account. What level of responsibility does each person have in this event?
Anti-social premise	• Cleo sent Jackie an email. • Cleo proposed that Jackie receive $1500 from an illegal business transaction, and send $1000 of the $1500 to an overseas bank account. In return for their participation, Jackie could keep the additional $500. • Jackie agreed, and got a notification from their bank that they had received $1500 in funds. • Jackie sent $1000 to an overseas bank account. • One week later, Jackie was informed by their bank that the $1500 transaction was fraudulent, and would be returned. What level of responsibility does each person have in this event?
Pro-social premise	• Logan sent Kerry an email. • Logan told Kerry that a recent earthquake had resulted in the loss of a local family's home, and requested a $1000 donation to help. • Kerry withdrew the money and sent it through a wire transfer. • Kerry was later informed by law enforcement that the charity was fake. What level of responsibility does each person have in this event?

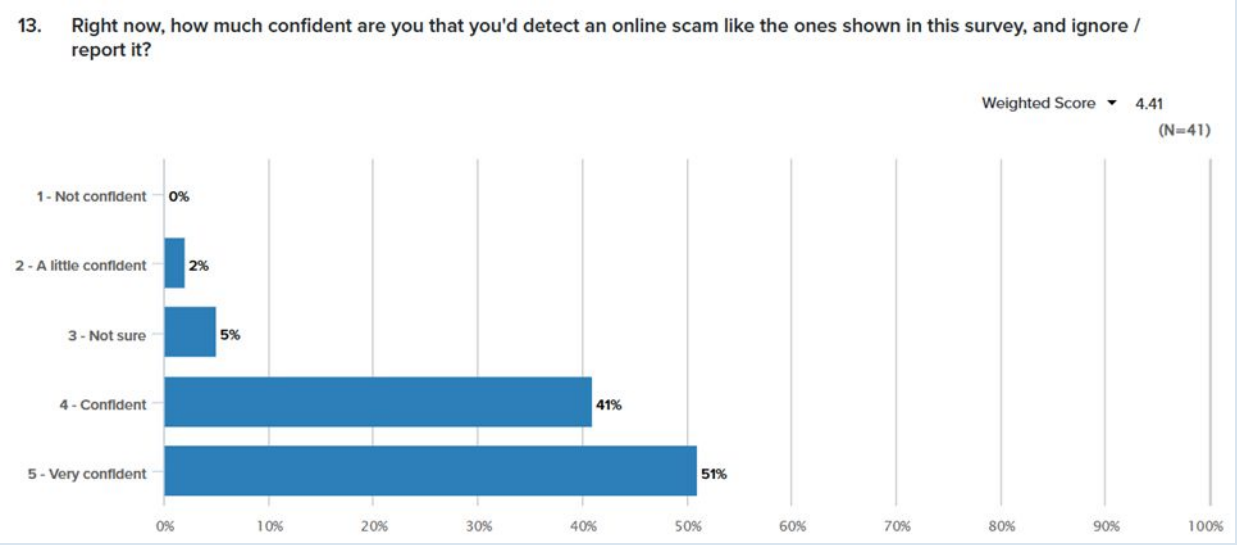
Results

- The scammer was always considered the most responsible in the execution of the scam, but victims were almost universally perceived to share responsibility
- Interestingly, the socially neutral premise (clicking on a malicious link by accident) was considered the **most** responsible for their own victimization, but it shared similar results with the victim of the anti-social premise (participating in money laundering)
- **Victims, even the most sympathetic ones, were all considered 25-49% responsible for their own victimization across all scenarios**
- Victims of a pro-social premise receive more social support and less blame, since that scenario stood out from victims of both anti-social and socially neutral (accidental) premises

Stats

Premise	Responsibility assigned to scammer (mean)	Responsibility assigned to victim (mean)
Neutral	51.5 %	48.5 %
Pro-social	74.1 %	25.9 %
Anti-social	54.25 %	45.75 %





My hot takes on the results

- **In a situation where an attacker is targeting a user, the attacker is always responsible.**
- No one is completely immune to social engineering.
- We all feel confident we would not fall for a scam.
- The right time, place, and circumstances can lead to a failure in judgment, even in someone who would normally recognize an attack.
- Given enough time and resources, a persistent attacker will find a vulnerability.
- Sharing our stories is **powerful** – about half of respondents believed reading just the few stories in the survey improved their ability to detect scams or social engineering attacks.

Let's connect it to social engineering!

- The threat of the "accidental insider"
- 70-90% of data breaches start with social engineering attacks
- Social engineering is highly asymmetric, with a low bar to entry
- AI will increase volume, efficiency, and sophistication of attacks
- Even solid security defenses like MFA fall to social engineering

No one is immune…even smarties like us

- HBGary hack (2011)
- Uber's "MFA Fatigue" attack (2022)
- Okta "Super Admin" IT Support advisory (2023)
- MGM Resorts (2023)

From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

What makes us vulnerable?

- Heightened emotions, especially fear
- Fatigue, illness, sleep
- Overwork or distraction
- A sense of urgency
- Desire for helpfulness
- Sympathy or susceptibility to specific narratives
- Attackers giving us a crumb of "private" information breaks down normal suspicion

It's not a bug, it's a feature – we are human beings that trust other human beings.

What happens in a “blame culture”?

- It’s widespread – in a recent survey, 88% of global respondents believe there is a blame culture in the cybersecurity industry (Security Magazine, 2022)
- Less information sharing and disclosure
- Slowed reporting
- Inaccuracy in debriefings and root cause analysis
- Wasted time and damaged relationships from trying to deflect blame
- Poor decision making
- Same $%&#, different day – without systemic fixes, mistakes are repeated

Attackers benefit when we assign shame or blame to victims.

How we can save us from ourselves

- Least privilege access – separate administrative accounts, jump boxes
- Zero Trust architecture
- Well-documented authentication protocols
- Verify out-of-band for unusual or urgent security requests
- Protect against mistakes - backups, change management, development/testing/staging environments, logging
- Regular security training and assessment, with targeted training for IT support and administrators
- Be aware of your own biases and vulnerabilities

How to break through the blame

- “Security First” culture (with executive buy-in!)
- Commit to transparency and deep observability
- Collaborate internally and externally (industry groups)
- Encourage self-reporting
- Use the power of stories
- Embrace open communications
- Practice with tabletop exercises and problem solving
- Look to systems, not people, for root causes
- Consider mistakes **inevitable** and make plans accordingly

Mistakes are opportunities

Reading & References

- Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187-204.
- Modic, D., & Lea, S. E. (2013). Scam compliance and the psychology of persuasion. Available at SSRN 2364464.
- Montada, L., Lerner, M. J., & Lerner, M. J. (Eds.). (1998). Responses to victimizations and belief in a just world. Springer Science & Business Media.)
- Neuhaus, Till. 2020. "A (Nudge) Psychology Reading of the 'Nigerian Scam'". Brolly 3 (3):7-28.//
- Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and applied social psychology*, *36*(3), 272-279.
- Vedova, H. (2023, February 23). *Consumer Sentinel Network Data Book 2022*. Federal Trade Commission. Retrieved April 23, 2023, from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022
- Okta: Hackers target IT help desks to gain Super Admin, disable MFA | bleepingcomputer.com
- Does cybersecurity's 'blame culture' affect incident reporting? | Security Magazine