



## Don't Blame the Victim: 'Fraud Shame' and Cybersecurity

From people who “donate” money to a supposedly dethroned prince of Nigeria to buying a shady cryptocurrency based on an internet meme, our society often pokes fun at victims of fraud.

There is often a culture of blaming fraud victims for their predicament even in less obvious cybercrimes, like falling for an aggressive phone scam or clicking on a well-written phishing email. As a society, we have a strong tendency to focus on something the victim didn't know or didn't do, rather than focusing on the criminal and the crime.

### What is “fraud shame”?

This victim blaming leads to what we call “fraud shame,” where people feel it is their fault for being the victim of a cybercrime, even though the real person responsible for fraud is the criminal perpetrating it, of course. Fraud shame and victim blaming can divide families, friends, and workplaces. It can cause victims of fraud, who are often older adults, to not report that they are the victim of a crime. Our 2023 *Oh Behave!* survey found that over 1 in 5 older adults (born before 1964) reported losing money or data due to [phishing](#) or other harmful online activity.

“Think about the intent of the victim,” says Kathy Stokes, Director of Fraud Prevention Programs for AARP. “They didn't wake up one day and decide to send money to criminals. They were trying to help a beloved grandchild get out of trouble or trying to build generational wealth.”

Instead of looking at people who lose money due to online fraud as gullible marks, first remember that they are victims. At the end of the day, the person at fault is the criminal.

An AARP report on victim shaming found that the vast majority of Americans (85%) think that fraud can happen to anyone. Still, a majority (53%) also believe that fraud victims are culpable and blameworthy. We need to work together to change this cultural contradiction!

“Victims are all too often blamed for the crime they experienced,” the authors of the report [claim](#). “And this misdirection of blame has played a role in how financial crimes are prioritized (or not) in the US.”

### Why is “fraud shame” a problem?

This victim-blaming attitude is not only unjust but also counterproductive in fostering a safer digital environment. Instead of supporting victims, ‘fraud shame’ adds insult to injury, leaving them feeling embarrassed, humiliated, and reluctant to [report the crime](#). As a result, many incidents go unreported, making it easier for cybercriminals to continue their illicit activities undetected.

It also makes the victim even more vulnerable, according to Lisa Plaggemier, Executive Director of the National Cybersecurity Alliance. “When an aging loved one of mine was defrauded, her adult children made her feel even worse about it than she already did. This caused her to pull away from them, increasing her sense of loneliness and isolation. Loneliness is one reason the aging population is vulnerable to scams, especially things like romance scams.”

It is essential to recognize that anyone can become a victim of cybercrime, regardless of their age, education, or technological proficiency. Cybercriminals are becoming increasingly sophisticated, employing social engineering tactics that can deceive even the most vigilant individuals. The focus should not be on blaming the victim but on understanding the tactics employed by cybercriminals and empowering individuals with knowledge and skills to stay safe online.

An ideal world without fraud shame would be a more secure world. Victims would no longer hide and, instead, would [report all cybercrime](#). Families and friends would stand united and support each other, even if someone is victimized. More law enforcement personnel would understand that cybercrime is real crime, not just a civil matter. By changing our attitudes, we can help make this a reality!

## What you can do to fight “fraud shame”?

**If someone close to you tells you they are the victim of a fraud, don’t blame them.** Instead, help them reach out to the authorities. Teach them how to better identify phishing attempts and adopt other simple cybersecurity behaviors.

**If you are the victim of cybercrime, [report it!](#)** It doesn’t matter if you feel ashamed about it, you are a victim and you deserve help. Losing money and data is not the price of admission for the internet.



The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.