

Joseph Carrigan

Senior Security Engineer, Johns Hopkins University Information Security Institute

Recently, The Maryland Cybersecurity Council, The Johns Hopkins University Information Security Institute, and the National Cryptologic Foundation collaborated in conducting a study of the cybersecurity awareness and practices of Maryland residents. The result of the study that I found most shocking was that approximately 25 percent of the respondents indicated that they have been the victim of an online scam where they lost money.

We asked respondents to quantify their losses. The largest group of losses was under \$100, But there were responses as high as \$100,000, with a surprising number of responses in the range of thousands of dollars and 10s of thousands of dollars.

\$100,000 may seem like an outlier but there is no shortage of people who have lost amounts of this size. For example, a recent [story](#) from WMAR's Mallory Sofastaii reported that 7 Marylanders lost a total of 3.8 million between May and December of last year. That's an average of over half a million dollars each. These statistics come from the FBI's Internet Crime Complaint center.

These scams are elaborate. They play on people's ignorance of banking and law enforcement systems. SB0834 will be a good first step to filling the knowledge gap that leads to these kinds of losses. Informing people of the tactics used in these and other scams protects people by allowing them to identify a scam at the beginning. An awareness program could let people know that it's okay to just hang up or that law enforcement will never ask for payment in gold, cryptocurrency, or gift cards. I ask for a favorable finding for SB0834.

Link:

<https://www.wmar2news.com/matterformallory/elaborate-scam-involves-gold-bars-and-couriers-cost-a-maryland-woman-2-million>