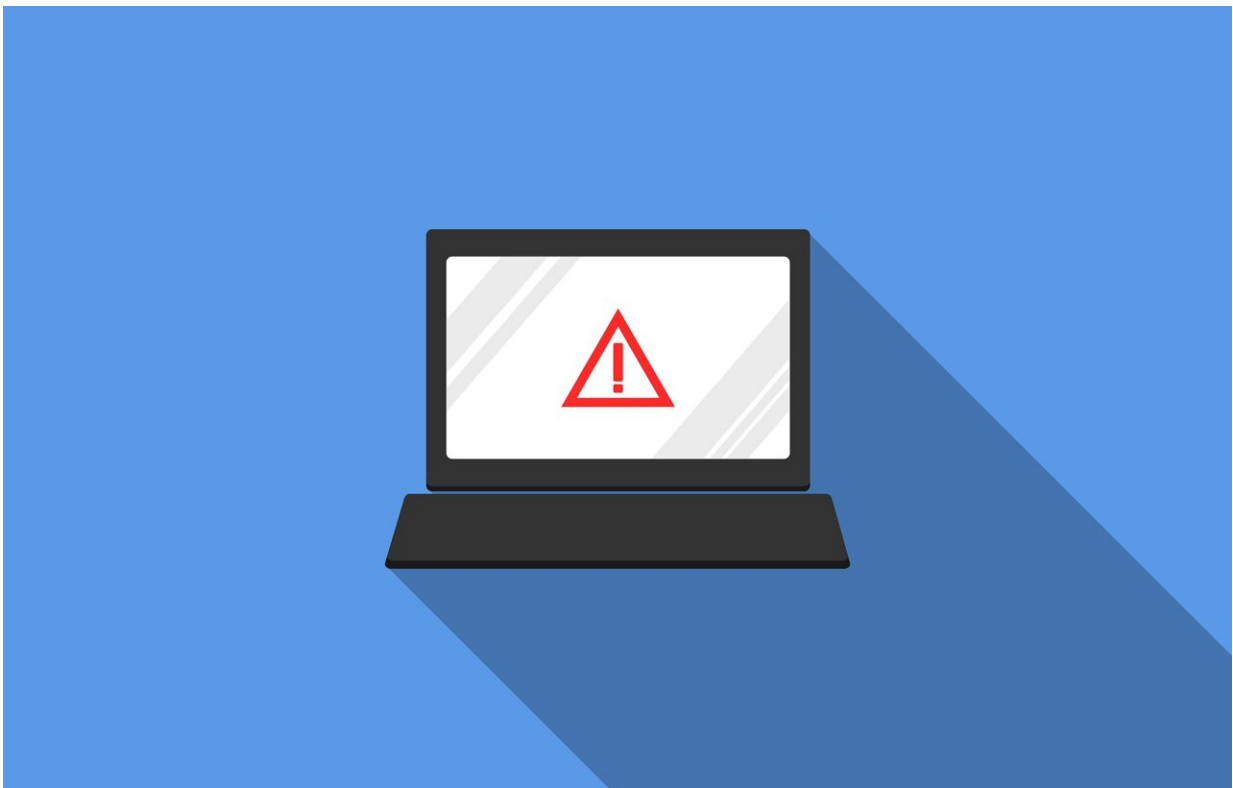# Fear trumps anger when it comes to data breaches, says researcher

June 22 2023, by Rajendran Murthy

Credit: Pixabay/CC0 Public Domain

When a person is notified of a data breach involving their personal information, if they react with a feeling of fear—as opposed to anger—they're more likely to stop using the site.

That was the main finding of [a study I conducted](#) with three co-authors that examined which emotions lead customers to change their behavior after a breach. We found that angry customers, on the other hand, are more likely to vent on different social media platforms but then return to the breached site.

We surveyed 208 U.S. consumers, ages 18 to 60, and asked them to describe their feelings after being informed of a data breach on their favorite and frequently used website. Subscription websites, such as Netflix and Xbox Live, and free-to-use websites, such as Facebook and Snapchat, were considered. We then asked the participants to explain, in their own words, what actions they took in response.

We found that [positive attitudes](#) toward the website before the breach did not meaningfully affect whether consumers reengaged with the website after the breach, as some [prior research](#) has indicated. Instead, the emotional response of fear, in particular, weighed heavily on customers.

Fearful customers appeared to stop using the breached site to reduce their feelings of stress and vulnerability. Other customers resorted to providing false biographical details or removing credit card data, name and date of birth from the [website](#) as they continued using it.

In 2022 alone, U.S. [customer data was compromised](#) in over 1,800 incidents, affecting over 400 million individuals.

Much of the prior research has focused on [customer anger](#) in the wake of a data breach and the need for companies to placate angry customers or manage negative media coverage. To do so, companies may [engage crisis managers to contain the damage](#), [partner with identity protection services](#), [pay fines or settlements](#), or try to lure back customers with [free services](#).

However, our research shows that companies need to address fearful customers differently after a data breach has occurred—if they want to avoid customer loss. To do this, companies can work with their IT departments to identify customers who are no longer active after a breach and then reach out to them directly to assuage their fears.

It is not yet known how companies should react in the aftermath of a data breach. It isn't clear why customers return. One likely explanation is privacy fatigue—when customers believe keeping their online data secure is futile.

In our study we found one-third of customers returned after a breach without even changing their passwords. More than half returned after making some changes, such as removing their credit card data, changing their passwords or removing personal information.

This may be why researchers cannot provide reliable recommendations for handling data breaches. From a company's standpoint, if customers will return anyway, there is little incentive to do more than the bare minimum to address a breach.

We are now studying the behavior of people who have experienced multiple data breaches in the past year. We want to know how these customers change their behaviors, as well as how they judge the recovery efforts of the companies whose sites were breached.

Recent regulations, such as the EU's 2018 data protection law and newly introduced state bills in the U.S.—along with updates to the California Consumer Privacy Act—will force companies and data brokers to think more seriously about the kinds of data being collected and stored. Health care, retail, finance, social networking and other websites will need to make significant changes in how they inform customers of—and compensate them for—such data breaches.

Citation: Fear trumps anger when it comes to data breaches, says researcher (2023, June 22) retrieved 28 April 2024 from https://techxplore.com/news/2023-06-trumps-anger-breaches.html