How repeated questions could put you at risk of cyber crime

March 27 2023

Credit: CC0 Public Domain

People reveal more personal information when you ask them the same questions a second time, according to new research from the University of East Anglia.

A new study published today reveals how simple repetition can make people disclose too much, and potentially put themselves at risk of identity theft and cyber crime. The research team says that understanding why people disclose personal data could help inform measures to address the problem.

"Tell Me More, Tell Me More: Repeated Personal Data Requests Increase Disclosure" is published in the *Journal of Cybersecurity*.

From subscribing to online newspapers to completing customer surveys, our personal data is being mined continuously; the world's most valuable resource is no longer oil, but data. But for consumers who provide their personal data, doing so comes with potential costs and security risks.

Lead researcher Dr. Piers Fleming, from UEA's School of Psychology, said, "We're constantly being asked to give up our personal details, whether it's being asked to subscribe to a newspaper, turn off an adblocker, or complete customer surveys."

"You may have received an email asking for a small increase in your monthly charity donation, or if you log in to social media, it may ask you for a little more profile data like adding your school or workplace," he continued. "This can lead to minor inconveniences such as junk emails or more disruptive potential consequences such as identity theft. We wanted to know more about why people share large amounts of personal information, particularly over social networks, without protecting that information from unintended recipients. Advertisers, marketers and social media gurus believe that repeated requests will lead to increased compliance. So we wanted to find out how these repeated requests change our behavior, and whether they can lead us to do things, like sharing personal information, that we otherwise would not do."

The research team asked 27 study participants for a range of personal

information online including their height, weight and [phone number](#) as well as their opinions on topics including immigration, abortion, and politics.

The participants then ordered the questions from least to most intrusive and were asked how much of their personal information they would "sell" to be made available on a purpose-built website for two weeks.

They then asked them again how much information they would sell—to appear for a further two weeks—for a chance of even more money.

In a second larger online study, 132 participants were asked how much information they would sell at two time points, as well as a range of personality questions.

Dr. Fleming said, "Our first study showed that asking for real personal data led to increased information disclosure when asked again. Our second study replicated this effect and found no change in people's associated concerns about their privacy—people change their behavior but not their view. This demonstrates that simple repetition can make people over-disclose, compared to their existing, and unchanged concern."

"This pattern of asking for increasing amounts of user information over time mimics a classic compliance technique known as the 'foot-in-the-door' effect. This is a compliance tactic that aims at getting a person to agree to a large request by having them agree to a modest request first. It is commonplace in consumer behavior and charitable giving," Dr. Fleming continued. "This study is important because if we better understand why people share [personal data](#), we can encourage greater sharing when it is mutually beneficial but protect against over-sharing when it might lead to harm."

The research team suggests ways for businesses and consumers to encourage an acceptable level of disclosure to match personal beliefs for mutual benefit.

"For example, we suggest practical measures, such as forewarning people to protect their privacy across repeated requests should be effective at reducing this effect," added Dr. Fleming.

More information: Piers Fleming et al, 'Tell Me More, Tell Me More: Repeated Personal Data Requests Increase Disclosure', *Journal of Cybersecurity* (2023).

Provided by University of East Anglia