Observer

Different Questions Produce Different Longevity Answers

How long you expect to live depends on how the question is asked. That's the conclusion of a team of researchers in a Columbia School of Business research paper. The authors suggest that beliefs about longevity are constructed at the moment a respondent is asked. Answers are influenced not only by the individual's age, gender, and health, but also by the way the question is framed.

Over the course of three studies, respondents were asked how likely they were to survive to age 85. The answer: 55 percent. But when individuals were instead asked the likelihood of their dying by age 85, they answered 68 percent. The estimated mean life expectancies ranged from 7.29 to 9.17 years longer for those who responded to the "live-to" question, compared to those who were given the "die-by" framing.

The authors compared estimated life expectancies to the Social Security Administration life tables and discovered that the expectations of individuals in the live-to frame more closely reflected the actual life expectancies for ages 65 and 75. By contrast, respondents to the die-by question were more accurate for older ages, such as 95. The authors found that the framing effect on judgments is partly influenced by the relative number of thoughts in favor of being alive at that age. The research also established a correlation between respondents' life expectations and their varying preferences for life annuities.

How Secure Is Your Password?

This year, more than 90 percent of user-generated passwords—even those your IT department considers "strong"—could be compromised by hackers, according to Deloitte.

A popular misconception is that hackers work by first discovering a username, then going to a login page and guessing the password. But most websites freeze an account after a few unsuccessful attempts. More commonly, organizations store usernames and passwords in encrypted master files, which can be leaked or stolen. Hardware and software for hacking and decryption have become more sophisticated and less expensive.

A password containing at least eight characters, with upper and lower case letters, at least one number, and one non-alphanumeric symbol, has long been the standard. Longer passwords would be more secure, but computer users find it difficult to memorize a series of more than seven numbers. Complex passwords also are hard to enter on smartphones.

Consequently, users often create passwords containing common names or words, using very few symbols. These tendencies weaken password effectiveness. Even worse, individuals reuse passwords for multiple accounts. A security breach on a less secure game site or social network can give hackers access to the user's high-security financial account.

To boost security, examine your firm's rules regarding password expiration, minimum length, use of the full symbol set, and password resets. Don't store unencrypted usernames and passwords. Password vaults and new software can make passwords harder to hack. Avoid obvious passwords that use names, common words, and number/letter sequences. Avoid obvious password reset clues, such as "mother's maiden name."

Expect many technology and telecommunication companies to implement multifactor authentication, augmenting the security of account names and passwords with fingerprints, iris scans, USB plug-ins, and other features.