epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 8, 2022

The Honorable Dolores G. Kelley, Chair
Senate Finance Committee
Maryland General Assembly
3 East
Miller Senate Office Building
Annapolis, MD 21401

Dear Chair Davis and Members of the Committee:

EPIC writes in support of Senate Bill 639 regarding financial institutions' security questions and measures. SB639 would help protect Marylanders from identity theft by requiring financial institutions who choose to use security questions to provide customers with more than one security question option.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has long advocated for cybersecurity safeguards for consumer information held by financial and commercial organizations. EPIC has previously testified before Congress on the need for financial institutions and companies to protect consumers against data breaches.[1]

Security Questions are a Poor Security Measure

We're all familiar with the situation: you create an online account, set a password, and the site asks you to answer one or more "security questions" in case you need to reset your password or verify your identity. The problem? The answer to many of those security questions is not secret. Yet many financial institutions are using these questions as a critical identity verification method that gives access to an account. But there are much more secure authentication techniques now widely available. And the use of a weak security question undermines complex password requirements and other security precautions. The requirement that your password contain one uppercase letter, one lowercase letter, one symbol, and one number is meaningless if all that is required to bypass that password is your mother's maiden name.

[1] *See, e.g., Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the H. Comm. on Financial Services*, 115th Cong. (2018) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf; *Consumer Data Security and the Credit Bureaus: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. (2017) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/testimony/congress/EPIC-Testimony-SBC-10-17.pdf; *Cybersecurity and Data Protection in the Financial Services Sector: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 112th Cong. (2011) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.

During the 2008 U.S. Presidential election campaign, Vice Presidential candidate Sarah Palin's personal Yahoo email account was hacked by a 20-year-old college student who looked up the answers to her security questions—such as her birthdate and high school—and subsequently changed her password and gained access to her e-mail account.[2] In 2005, Paris Hilton's T-Mobile account was improperly accessed by a teenager who did a quick online search for "Paris Hilton Chihuahua" and therefore could answer the "secret question" of "what is your favorite pet's name."[3] These so-called "social engineering" attacks pose a significant risk to accounts that do not have strong verification standards.

The question of "what is your mother's maiden name?" is possibly the least secure of all security question options. Your mother's maiden name may in fact be your last name. But even if it is not, it is easily discoverable through an internet search, listed in obituaries, wedding and birth announcements, and social media posts.[4] Financial institutions should not even offer this question as an option, but at minimum they must offer other options, as SB639 requires.

The weakness of security questions as an authenticator has been known for years. Sixteen years ago, renowned security expert and Lecturer in Public Policy at the Harvard Kennedy School Bruce Schneier wrote "The answer to the secret question is much easier to guess than a good password, and the information is much more public."[5] In June 2017, the National Institute of Standards and Technology ("NIST"), which operates under the U.S. Department of Commerce, updated its Digital Identity Guidelines and removed its previous recommendation for security questions as an authenticator.[6]

Best Practices for Authentication

There are plenty of alternative authentication methods available today. Financial institutions truly should no longer be using basic security questions. EPIC recommends that institutions should follow the best practices laid out in NIST's Digital Identity Guidelines.[7]

But if security questions are going to be used, institutions should ensure that multiple question options are given, and that users are permitted to answer the questions with randomly-generated password-like answers rather than factual, semantic answers. This allows users who use a password manager to store those answers with their account information and prevent hackers from guessing those answers.

---

[2] Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED (Sept. 2008), https://www.wired.com/2008/09/palin-e-mail-ha/.
[3] Anne Diebel, *Your Mother's Maiden Name is Not a Secret*, N.Y. Times (Dec. 28, 2017), https://www.nytimes.com/2017/12/28/opinion/sunday/internet-security-questions.html.
[4] *Id.*
[5] Bruce Schneier, *The Curse of the Secret Question* (2005), https://www.schneier.com/essays/archives/2005/02/the_curse_of_the_sec.html.
[6] Nat'l Institute of Standards and Tech., U.S. Dept. of Commerce, *NIST Special Publication 800-63B: Digital Identity Guidelines* (June 2017), *available at* https://pages.nist.gov/800-63-3/sp800-63b.html#sec5; Lily Hay Newman, *Time to Kill Security Questions—or Answer Them With Lies*, WIRED (Sept. 28, 2016), https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/.
[7] *Id.*

By requiring that financial institutions who choose to use security questions to provide customers with more than one security question option, SB639 is a step in the right direction in protecting Marylanders against identity theft. The Committee should give SB639 a favorable report.

If EPIC can be of any assistance to the Committee, please contact EPIC Deputy Director Caitriona Fitzgerald at fitzgerald@epic.org.

Sincerely,

Caitriona Fitzgerald
EPIC Deputy Director