Proskauer

A Moment of Privacy

May 2009

Welcome to “A Moment of Privacy,” a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

“A Moment of Privacy” addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

And now for this month’s question:

Q: What elementary school did you go to?

A: I don’t know, but I could probably find out.

There is an increasing amount of discussion within the information security industry about whether the use of “security questions” to unlock forgotten passwords is a sound practice. Many web sites ask users to answer personal questions upon registration, so that those questions and answers can be used in the future to authenticate users when they have forgotten their passwords. The problem is twofold:

(1) The answers to many of these questions can be relatively easily guessed by an unauthorized individual to gain access to the account.

(2) In many cases, the authorized user forgets the answer to the question when it is needed later to access the account.

A recent study conducted by researchers at Microsoft and Carnegie Mellon University (“It’s no secret: Measuring the security and reliability of authentication via ‘secret’ questions”) found that 17% of users’ security answers were guessed correctly by mere acquaintances, and 20% of the study participants forgot their answers within six months.

If your company uses security questions to authenticate users who have forgotten their passwords, there are a few things your company can do to make this feature more secure and reliable:

- Once the user answers the security question correctly, do not simply provide the user's password. Instead, e-mail it to the e-mail address you have on file for the user.
- Never ask for a user's birth date or mother's maiden name. (Having this type of information in your database triggers compliance obligations under state and federal laws.)
- Select your security questions wisely, steering away from:
- Questions that can be easily guessed by an acquaintance (e.g., Where did you grow up?)
- Questions for which there is a limited pool of possible responses (e.g., What color are your eyes?)
    - Questions that are likely to have statistically common answers (e.g., What is your favorite flower?)
- Questions the answer to which could be found by doing online research (e.g., What was your high school mascot?)

See http://www.guanotronic.com/~serge/papers/oakland09.pdf to see how specific questions fared in the study.

- Disable your forgotten password feature after a user has made two or three incorrect guesses, and refer the user to a customer support representative.
- Ask questions that relate to the user's account activity, such as "When did you last log in?" or "During what month did you last make a purchase?"
- Require the correct answer to more than one security question before providing the user's password.

Have a question? E-mail Kristen J. Mathews at kmathews@proskauer.com.

Related Professionals

- **Jeffrey D. Neuburger**