

Transcript:

## Security Questions: What is your pet's name?

---

**Speaker:** Kristen J. Mathews – Partner, Proskauer

*(Words slide in from top): Security Questions: What is your pet's name?*

**Mathews:** Rethinking customer authentication methods. What is your pet's name? Some of you may have read my blogging on this recently, because I, I have felt that these security questions ha– are weak. I thought that they've been weak for as long as they've existed, but I've always felt that I'm the only one who seems to feel this way.

We have a study, um, that supports this view to some degree. Uh, it was done by Microsoft in collaboration with Carnegie Mellon University. Carnegie Mellon – Mellon University is doing a lot of these studies, I'm finding. Uh, 17 percent of users' security answers were guessed correctly by mere acquaintances. Um, that doesn't really surprise me. A lot of these questions are "What is your pet's name?", "What city were you born in?", "What high school did you go to?" It would be pretty easy for an acquaintance to know the answers to those questions. 20 percent of the participants forgot the answers, and that also doesn't surprise me at all. Um, and you can find out more about this study at this URL. In particular, they have specific questions and how those questions fared in this study, and I think that would be important to anyone who is using security questions in your business. You should try to steer away from the ones that didn't do very well. And we'll go into this more.

Um, in particular, you may have read – it got a lot of press – that there was a Twitter hack, and corporate Twitter documents were disclosed. If you read carefully, and it didn't really – wasn't that broadly conveyed in the media – the underlying method of that breach was, um, a weakness in a security question feature on a web-based e-mail service that enabled the hacker to first get into a Twitter employee's, um, personal web-based e-mail account, and from there, as you may or may not know, once you do that, once a hacker achieves that, the hacker is easily able to get into your other accounts. Because if you think about it, once your web-based e-mail account is hacked into, it can be used to leverage the "forget my password" features on other websites, because all you have to do is look at all of the spam, if you will forgive me, that's in the e-mail box, and you see all of the advertisements from all of the merchants that you've purchased things at, you know that you ha– they, they can from that derive that you must have or you may have an account with those merchants, so you go to the merchant website, you say, "I forgot my password," it gets sent to the e-mail address that you hacked into.

Um, so in any event, security pass– security questions really are important, and they can be used in ways that could hurt your customers and also you.

Um, you may also know that Sarah Palin's personal e-mail was hacked into, also because of weak security questions.

Some tips if you use security questions. Um, once the user answers the question, don't just give them the password. Rather, um, e-mail it to their address on file. Um, I think most companies do do this. Of course, that is relying on the security of the e-mail account in the first place, so it's not the only thing that you should be doing.

Um, do not ask for birth date or mother's maiden name in a security question. I see this a lot. It's not a good idea for a number of reasons. Um, first of all, you don't want that information, in, in particular, mother's maiden name, you don't even want that information in your database because if it gets hacked, um, it – that triggers breach notification laws in at least one or two states. Date of birth is another thing that you don't want to ask for for – unless you're asking for it for, and that you've, and you've figured out how to comply for other reasons, because we have COPA issues if you're asking for date of birth. Um, also, again, some of the breach notification laws cover date of birth, so if there's not a good reason and if it's not well thought out, you really ought not be asking for that information.

Um, let – disable the forgotten password feature after the user makes a few incorrect guesses. Now, I know you're saying to yourself, "Okay, then what do we do? How do we let the person get their new password?" And it does present customer service issues for you, because somehow you're still going to have to speak with or communicate with somehow, that, that individual. Um, so I'm not dismissing the problem, I'm presenting, um, some possible solutions.

And also you can think about security questions that are not likely to be known by acquaintances, uh, such as, "When did you last log in?", "During what month did you last make a purchase?" These are not perfect, I know, because I personally wouldn't be able to answer, for example, necessarily, when did I last log in, but if you can come up with security questions that are a little more safe, do so.

Um, require the correct answer to more than one. That's one easy thing you can do that would at least statistically increase the, um, effectiveness of these questions.

And steer away from questions that didn't do well, for example, on that survey that I mentioned by Carnegie Mellon and Microsoft. For example, questions that could be easily guessed – "Where did you grow up?" – um, questions for which there is a limited pool of possible responses. This is something a lot of people don't think about, but if the question is, "What color of your – are your eyes?", I think there's four possible answers to that question. "What's your favorite flower?", I think, essentially, there's three an– typical answers to that question. Don't ask me what they are, or ask me on the break, and I'll tell you what they are.

Um, and also, don't ask questions the answers to which are easily found on online research. For example, Facebook, Reunion.com, Classmate.com.