Wish-It-Was Two-Factor 2007-09-20

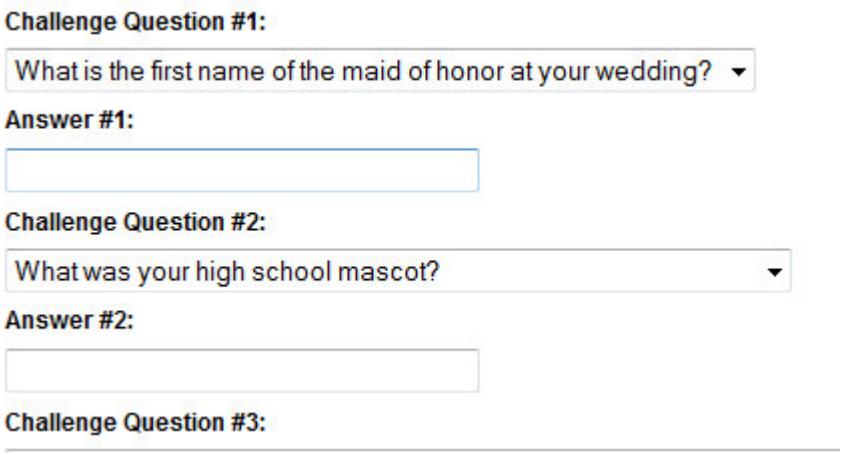
by Alex Papadimoulis in Feature Articles (187 Comments)

Unless you've just recently signed on to this whole Internet Thing, you've probably noticed an increasing trend in the World of Authentication. These days, when logging on to various websites, users are asked for a name, password, and the answer to one or more "secret questions." It's actually a new-fangled type of authentication called Wish-It-Was Two-Factor.

It all started way back in the year 2005, when the Federal Financial Institutions Examination Council issued a guideline entitled Authentication in an Internet Banking Environment. It's a rather exhilarating read if I do say so myself, especially if you're a fan of government banking regulations. And, really: who isn't? In a nutshell, the FFIEC mandated that internet banks utilize a Two-Factor approach to authentication by year-end 2006.

The idea behind Two-Factor authentication isn't too complicated. Simply (1) verify that a user knows something, and (2) verify that he physically has something. This could be done with a (1) name and password, and (2) one of those key fob things or even a print-out of one-time use codes.

Banks, however, weren't too happy with the requirement of implementing such "costly" changes and instead chose to invent the Wish-It-Was Two-Factor authentication. In this method of authentication, they (1) verify that a user knows something, and (1, again) verify that a user knows something else. For example, Charter One Bank's implementation of Wish-It-Was Two-Factor requires that customers create three "secret questions" as shown below:



Users are asked to pick from all sorts of different "secret questions," ranging from "In what city is your vacation home?" to "What is your second-favorite post-modernistic European novel?" And if they're lucky, users can actually *remember* what answers they gave *and* figure out *exactly* how they typed them in.

Unfortunately, this Wish-It-Was Two-Factor type of authentication has become an industry standard. A recent study reported that 96% of U.S. banks are failing to implement the recommended Two-Factor authentication, opting instead for "authentication methods that solicit confidential information from consumers." The problem with this, of course, is that industry standards are… well… standard. It's just the way things are supposed to be done.

Worse still, the Online Banking industry is perceived to be one of the most secure. Surely, if anyone knows how to do online security, it's the online banks, right? And if you want your web application to be extra secure, it should be modeled off of an online bank, right?

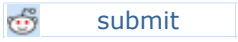
That's exactly what Russ's company figured. When the higher-ups learned how "unsecure" their web application was (it *only* asked for name and password), they directed development to implement "bank level" security. Development, figuring that online banks *must* know what they're doing when it comes to online security, went ahead and implemented their own version of Wish-It-Was Two-Factor authentication. After signing on, end users were required to select four questions from a selection of sixteen.

The users, however, weren't too thrilled with the change. One email from a disgruntled user reminded them just how wishfully secure their new authentication protocol was …

```
Dear -------.com,

Extra security, fine. I don't mind it. But let's get serious.

I never met my grandfather (he's been dead over sixty years). My parents
never talk about where they were born. I was never married. I didn't go to
college. High school mascot? Come on, I've been out of high school for decades!
And who has a favorite color?

Sure, I can make up answers, but since there's no way I'll remember my made up
```

```
answers, then I'm screwed. So I'll have to write them all down, but that doesn't
seem very secure. So, basically, I'm screwed.

Thank you,
---- ----------------
```

Share *Wish-It-Was Two-Factor*:



Digg submit

Trackbacks (URL)

The Mouse's Cord › Palin Exposes Security Flaw in Security Questions (09/18/2008)

187 Comments • Add Comment