Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Passwords again - why we can't leave well enough alone

I just tried to login to my bank account, and surprise surprise, US Bank now requires that, in order to access my bank account, I must provide them still more personal information, including answers to questions about my personal history, family, and world view. When I called them up, they told me "it's for your protection", but in fact, it doesn't protect me at all. At best, it protects them; and it probably doesn't even do that. I'm going to ask a simple question:

If you can't protect my password, how can you protect even more private information?

The problem is simple. If you can protect my password, you don't need the additional information. If you cannot protect my password, you cannot protect the additional information. The net effect is that my account is no more secure, but more people have more access to more personal information.

When will the foolishness end?

To me, this foolishness represents the ongoing lack of rational decision-making with regard to one of the simplest and most effective protection mechanisms that has ever been found. For some unfathomable reason, after thousands of years of the use of passwords, people still seem to think that they can improve on them. The fact is, passwords can be, and often are, a highly effective protection mechanism, when used properly. Augmenting them with additional passwords, is almost never a sensible idea, unless the augmentation is used as an additional authentication to grant additional privileges. And then, we really have two passwords for two different functions. In my case, I will do everything I can to use the same password for each and every one of their protective functions, because to do otherwise makes my life less convenient, and adds no risk whatsoever to me. On the other hand, every time I provide another password, I have to write it down or put it in a file somewhere, or use a variation on the same password I use somewhere else. The net effect is a proliferation of poor quality passwords, reused in place after place, making the protection of the each and every one of these systems and facilities weaker, without improving my protection in any way. It is, quite literally, the worst of all worlds. I get less protection, less convenience, and they get less protection, higher costs, and lose me as a customer.

Back to the future again...

All of this is nothing new. Others have written about it for many years, and I've written about it, at least since the 1980s. I find myself, again and again, referring people to a simple piece that I wrote ten or more years ago, and I end up doing this for so-called security experts, several times a year. This demonstrates both the lack of attention to the issues by these so-called experts, and the lack of the most fundamental review of the open literature by people who are supposed to be acting in a responsible manner for large enterprises, such as banks, financial institutions, governments, and so forth. When will the foolishness end? My guess is - never.

