

# Drinking From The Firehose — Too Many Passwords, Too Little Time

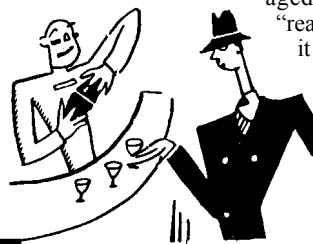
Column Editor: **Eleanor I. Cook** (Appalachian State University, Boone, NC) <cookei@appstate.edu>

The number of passwords that the average librarian must have at his or her fingertips has grown by leaps and bounds in recent years and there is no end in sight. This is a fact of life and we must find a way to manage them better. I suspect there are many people in other professions facing a similar challenge. IT system administrators and bank managers and well, just about anyone who shops or pays bills online with any regularity will find themselves collecting a hodgepodge of passwords to recall.

The experts often say that you should never write down passwords. Excuse me? As of this writing, I have 97 unique (almost) passwords — 34 of them are for travel and shopping sites, 23 of them are for credit cards and other personal finance and ID purposes, and 40 of them are specifically library work-related. To this latter category I add regularly as we increase the number of databases and e-journal platforms. Therefore, that advice is completely unhelpful to me, as there is no way on this earth I could possibly keep up with this many secret codes, no matter

what. The only personal codes I don't have to write down to remember are: My social security number, my home and work telephone numbers, and my ATM PIN. I also can usually recall my main email user name and password and my library ILS username and password but I use these everyday and I have these written down in the same place I have all the other codes I'll never remember, because I believe it is my responsibility to make sure that if something bad happens to me, that someone can get in there if necessary.

As a librarian and faculty member at a university, I am not held to the same strict security standards as people who work in the private sector. I have heard some interesting stories about how strictly passwords are managed out there in the "real" world and while it makes me shudder (and wonder); I can respect their need for more security in some cases. But so often, companies are moving the liability back onto the individual, so not to have to take the heat.



With identity theft such a serious problem, what are we to do? In order to explore this topic with more rigor, I decided to do a little research. I found a number of articles in the popular literature about the way passwords are developed and what the best practices are, but this did not satisfy me completely because some of the advice was the same old thing — don't write them down, and make them unique and hard to crack.<sup>1</sup> Ok, I sort of know this intuitively, but it is too difficult to do this, right? We are all lazy about the way we develop our passwords, but does it really matter?

But then, I met someone who changed my thinking entirely. A colleague of mine at **Appalachian State University** has done some really interesting research that captures the essence of the problems we face with the world of passwords. **Dr. Joseph Cazier** has several scholarly articles already published concerning password security issues and in his most recent study he has demonstrated some disturbing trends in the behavior of every-day citizens that points to the real need we all have for being more careful about how we construct the passwords that serve as barriers to our most sensitive personal information — our bank records, our email accounts, our financial and health records, and so on.

**Dr. Cazier** is certainly not the first person to explain this to me, least my systems colleagues at the Library feel slighted for essentially telling my coworkers and me the same thing. It's not that I didn't already know that

the best passwords are the hardest to remember or figure out — it's rather that **Dr. Cazier** has actually demonstrated this in an empirical way that can't be ignored.

In one study, **Joseph Cazier** and **Dawn Medlin** used a real data set of customer passwords from an e-commerce system to analyze the strength of the passwords. They were able to crack a majority of the passwords in a relatively short period of time.<sup>2</sup> In another study by the same authors, password choices were analyzed by gender and trends for password development were discussed.<sup>3</sup>

If you think you are alone in using your children, grandchildren or pet names as passwords, think again. Apparently the most popular constructs for password creation include these categories: family names; fan names, such as sports teams or entertainment characters; fantasy aspects, including sexual allusions (remember the commercial with the guy on the train trying to quietly tell the person on the other end that his password is "big boy"? ) and then finally, cryptic combinations, which is what is considered the best practice for development of passwords. In addition, the categories of "Faith," "Place," and "Numbers" figure prominently in the way people develop passwords.<sup>4</sup>

Why is it a problem to use these kinds of passwords? They are easy to guess and the people trying to guess them are using many clever ways to get at your passwords. Besides running software programs looking for common passwords (which is one method) another disturbing but growing method is referred to as "social engineering." Social engineering is the term used when sensitive information is obtained simply by asking for it — sometimes directly but other times under the guise of some other inquiry for which the victim doesn't understand the real purpose.

In an article soon to be published,<sup>5</sup> **Cazier** and **Botelho** report on a study they conducted recently in a metropolitan area. They set up a table in front of a large financial institution in a downtown area. Presumably, individuals working at such a company would have received a modicum of security training concerning passwords and the like. The researchers did not hide where they were from or what they were doing — they identified themselves as university researchers and said that they were conducting a study about passwords. They asked people if they wished to fill out a survey and offered them candy, and also a chance to win a free dinner at a local restaurant for completing the survey. They then repeated the study in front of a major hospital (another institution where employees are assumed to have a higher than average understanding of security issues). They also repeated the study with a population of students.

*continued on page 83*

An amazing number of people actually shared their actual passwords with the researchers! In addition, most survey respondents freely shared other personal information with the researchers even if they did not actually give them their passwords — this information, such as their names, addresses (for the purposes of the drawing for a free restaurant meal) and other identifying information could have been easily used to guess at their passwords.

The fact that such information can be gleaned this easily made me pause when thinking about the way we manage our passwords. This has me seriously rethinking my approach to my password problem — it's true that there is no way I can remember them all, especially if I develop "strong" passwords that are hard to crack. For example, the password a!s@d#f\$g%h^ would certainly be harder to crack than fluffy999, for example. However, even a!s@d#f\$g%h has a pattern to it — it is a series of letters and symbols based on the standard keyboard and anyone could use it (which means a clever cracker could figure it out too). A colleague of mine suggested a method for developing passwords based on the LC classification system. You can use call numbers from your favorite books as passwords. This idea is intriguing because you could create a code for referencing your passwords without actually telling anyone the actual password. For example, if you have a list of passwords you could note: *Agony & Ecstasy* (for your Citibank credit card) but only you would know that the real password is PS3537.T669A38. This definitely appeals to the librarian in me! And of course if you are more comfortable with the **Dewey Decimal** system, you could use that too. And you could take this concept and apply it to other systems of numbers and letters, I suppose. The point being that you need to come up with something creative and hard to guess.

There are a number of Websites that provide random password assignment, but that will have to be another whole column to discuss these. In addition, there are a number of password management software packages out there. Again this needs further exploration. (And if you have come across something you like in either of these areas, contact me!)

Banks and other institutions collecting sensitive information about you (health care systems, insurance companies, etc.) continue to be challenged by these problems. Some of their solutions are not very helpful though. In some cases they build too much complexity into the system and make it even harder for normal people to access their accounts. A recent example: one of my credit card providers decided that they wanted to build another layer of security into their system and asked their customers to pick an image from a set of pictures to use as another layer of privacy. Apparently they concluded that such a system would be useful, especially to those people who are visually oriented. I totally rejected this system as unworkable for me — I am <not> visually oriented and found the pictures to

choose from completely ridiculous. But that's just me — maybe some people like this system. For this account, I pay my bill the old fashioned way — through the U.S. mail!

Another financial institution I use has built in a series of questions to serve as a security wall in the case that someone unauthorized tries to access your accounts. Besides the well-used question, "What's your mother's maiden name?" this institution also includes a set of three other questions — things that only you know, and they give you three choices at all three levels. For example, if asking my favorite color or favorite sports team means nothing to me, I can still say indicate the name of my elementary school. That question has an exact answer for me, although it might not for someone else who moved around a lot as a child. By giving three options for each of the three questions, it is more likely that at least one of the questions in each set will pertain to any given individual. This is complicated but also possible to manage.

As for where to write this stuff down — it's clear that we will have to start doing this, but how to manage that? It used to be if thieves broke into your home they might first go for the jewelry and appliances such as TVs and DVD players, the family silver or other valuables, but now they might be looking for bank records, social security numbers and the like. A crook might take the hard drive of your computer first nowadays. This seems to be a logical place to start in some cases. If you keep your list of passwords in a file on your computer, can spy ware or ad ware invasions get to it? Probably not, but that does not mean it's not vulnerable to theft. As the news media has shown, people all over the country are taking hard drives or laptops home with them that apparently have large files of sensitive information on them (Why? I have to wonder).

So if you need to list out your passwords somewhere where you can get to them, you need to do it in such a way where you can remember what it <really> is with some prompt, and use other tricks that no one knows (or maybe just one other person knows). At least one other person in your family you trust should know that these things can be found somewhere. After all, if you are hit by a hay truck or drop dead of a heart attack someone needs to know how to cancel your accounts. They might not need your passwords to do this, but they need to know where you even have accounts.

Another development that is on the horizon and is actually being used in some places is a fingerprint-based device. Known as "biometric identification," grocery stores and financial institutions have started using this to some degree. This eliminates the need to remember an actual password since bodily attributes identify you instead. Iris-scanning systems, reminiscent of the movie *Blade Runner* are not far behind. Since there are essentially three methods of multifaceted identification: Something you know (passwords); Something you have (a key, a pass card or other object); or Something you are (your finger print, the iris of your eye), some institutions trying to protect your privacy are implementing systems

*continued on page 84*

that use all three of these. Of course, whether this makes your life simpler or more complicated is a good question. These systems are Big-Brother like, and even now, with so much of our consumption happening through ATM cards and debit systems, anyone you do business with (and possibly the government) can track your every move.

Maybe I should get rid of all those passwords and just pay cash! Unfortunately, I still have to have all those work-related passwords so I can get into the staff side of the ILS, my email account, and the ever-increasing number of e-journal platforms and the like that demand I create a user name and password as an account administrator. Argh, no winning on that one, and no end in sight!

As my friend **Megan** says, we are overtaxing our syntactic memory (don't you just love that). But since organized crime is getting into identity theft schemes these days, not just bored teenaged hackers, it's time we take this seriously. Risk management is a big deal these days. In order to mitigate that risk, it's best not to travel into "bad" virtual neighborhoods — porn sites and other fly-by-night Websites considered risky in terms of viruses and other types of scams. If you are the unlucky victim

of personal item theft (wallet, handheld, etc.) you need to take immediate action. The better you protect your passwords by keeping them hard to crack and written down in safe and encrypted fashion, the less your life will be disrupted. More on this in a future column — for now, it's time to make those passwords more secure! 🐼

---

*Thanks to: Tom Bennett, Joe Cazier, Adam Jordan, Megan Johnson, and Janice Keim for their feedback on this article.*  
— EC

#### Endnotes

1. I looked at the following articles: **Harrison, Warren**. "Passwords and Passion," *IEEE Software*, July/Aug. 2006.
- Kandra, Anne**. "Manage Passwords Safely – and Simply," *PC World*, April 2003.
- Lewis, Peter**. "Let Your Fingers Do the Locking," *Fortune*, Jan. 24, 2005.
- Locke, John**. "Smarter Password Management: How to Handle Your Passwords Without Getting Lost," *Free Software Magazine*, 2/10/2005. [http://www.freesoftwaremagazine.com/articles/password\\_management/](http://www.freesoftwaremagazine.com/articles/password_management/)
- Metz, Cade**. "Password Managers & Form Fillers," *PC Magazine*, May 24, 2005.  
*Password Management Best Practices / M-Tech Identity Management Solutions* — <http://mtecht.com/docs/user-provisioning-best-practices.pdf>
- Regnier, Pat and Sahadi, Jeanne**. "Defend Your Virtual Home," *Money*, Dec. 2006.
2. **Cazier, Joseph A. and Medlin, B. Dawn**. "Password Security: an Empirical Investigation into E-Commerce Passwords and Their Crack Times," *Information Systems Security: The (ISC)2 Journal*, v.15, no.6, pp.45-55.
3. **Medlin, B. Dawn and Cazier, Joseph A.** "An Investigative Study: Consumer Password Choices on an E-Commerce Site," *Journal of Information Privacy & Security*, v.1, no.4, 2005, pp. 33-52.
4. **Medlin & Cazier**, *Ibid*, p.40.
5. **Cazier, Joseph A. and Botelho, Christopher M.** "Social Engineering's Threat to Public Privacy," to be given as a paper at the 6th Annual Security Conference, Las Vegas, NV, April 11, 2007, <http://www.security-conference.org/> and also has been submitted for publication.