Volume 7 (2007)

Interface: The Journal of Education, Community and Values

5-1-2007

How Much Protection is Enough?

Pat McGregor

How Much Protection is Enough?

How Much Protection is Enough?

Posted on **June 1, 2007** by **Editor**

By Pat McGregor <pat@nithaus.org>

This isn't a commercial about life insurance, nor is it about birth control or UV-blocking eyewear. But it will teach you some techniques you can use to make decisions about those things, if you want to. Mostly, however, we're going to figure out how to protect ourselves online and in other transactions where privacy may be compromised.

Acceptable Risk

Let me talk a bit about "acceptable risk." Acceptable Risk is figuring out just what things will seriously endanger you and putting plans in place to protect yourself.

For example, flood insurance is extra for many home insurance policies. If you live on the top of a plateau in the desert, you can reasonably assume that you don't need flood insurance. If you live 200 feet from the banks of a river, and the county says you live in a "five-year flood zone" (which means you likely will get flooded every five years), you'll be required by your lender to get flood insurance. Or you might choose another house! But you'll be making a decision on what's your acceptable level of risk and what kind of protection you need. (Keep that "five-year flood" notion in the back of your head for a minute — we're going to talk about how to come up with that number before we get done.)

But how do you decide what is an acceptable risk for all the kinds of situations we have to deal with these days? You do a risk assessment. Or, you use the assessment tools someone else has created for you.

If you watch any commercial television, you've seen examples of tools people have created for you. Those commercials suggesting you get a checklist and fill it out, and then ask your doctor if you have Condition X — those are risk assessment tools. Another good one is by the Harvard Center for Cancer Protection, called "What's your disease risk?" [1] Instead of ten questions, they ask a wider range of questions and come up with a good assessment, as well as some recommendations.

There are similar tools for other kinds of assessment: how well your house is protected from fire, available from many fire departments; how likely your child is to graduate from High School given his/her current level of achievement, and so on.

Assessing your personal risk

You can drive yourself crazy trying to keep all your personal information completely locked away. Different, strong passwords for every place you have to sign on, opting out of every service that you're offered, using several different email addresses to minimize the spam you receive. Making a decision on what amount of protection you need based on an acceptable level of risk lets you spend you time and money wisely. It might even reduce your anxiety level, which would help your general health, too!

Nobody but you can decide what the right level of protection is *for you*. You can get advice from others, but you have to decide how much you trust those advisors. If you buy extra insurance based on a commercial or "infomercial" on TV, you are deciding to trust what the actors or salesman says. If your long-time insurance agent suggests more insurance, you might decide to trust past experience with that agent more than the infomercial. You're making a risk assessment right there, even if you don't know it.

And, no matter what your advisors say, *you* eventually make the choice. Knowing how to do it, instead of feeling lost in the dark, is always a good thing.

Evaluating the risk involves figuring out how likely something is to happen. That floodplain number we were talking about earlier comes from someone doing the work of recording all the floods in that area and then doing the math to calculate how often, on average, that piece of property goes underwater.

Now, this is a very important step. Doing some research and getting information about how likely something is to happen is the part of making a risk assessment that lets you save resources protecting against everything.

For example, many people base their "how likely is this to happen" on early articles about the Internet and the danger of passwords being stolen. They haven't actually done any recent research on what is actually happening out there.

In point of fact, stealing your password as you log in or hacking a whole file of passwords from a site happens very rarely. More likely, if you don't have your anti-virus software up to date and protecting you against these things, you'll visit a site that will download a little program that will capture your passwords and userids. Then it will "phone home" and send all the info it's captured. But the biggest threat these days is that people fall for phishing email, and give away their passwords and information. [2] *Phishing* mail is when someone sends you a note saying, for example, that there is a potential breach at your bank, and you should log on and confirm your

records. They give you a link to click. The page it takes you to will look exactly like your bank, but instead of fixing a problem with your bank, they are recording your bank password and ID. The keys to the castle, as it were. [3]

So, you do your research, find out what the most likely threat is, and decide how to protect yourself and your passwords. Some people even do some math and score the risks.

How do I do it?

My assessment says that the NY Times crossword puzzles, the recipe vault at a diet site, etc. — [things that don't have money access or that would let people post things or use my name]— don't need passwords that get rotated regularly.

Sites where I have the ability to spend money or access my health records, etc., have a need for strong passwords. I don't use the same password on each site, nor the same userid I use on the other, less important accounts. I change the passwords fairly regularly, especially when I have gotten a phishing message pretending to be from that site.

We should talk about strong passwords

At one point, a test of hacking against passwords showed that almost half the passwords on any system were "password" or the same as the Userids. This is a Really Bad Idea. Equally bad is writing your password on a sticky and putting it under your keyboard. Make up a strong password and protect yourself.

The definition of a strong password is something that can't be easily broken by someone with a high-end machine using various techniques. "Easily" generally means in 90 days or less, although like flipping a coin, the crook can come up lucky first time out and break it right away.

The password itself is made of a combination of letters and numbers that the security experts say will have a low probability of being broken. Here it is:

First, your password should be 8 characters or more

Then, it should have mixed elements. You have 4 available to you:

- 26 lowercase letters: sdfoiwrnueroqkin and so on.
- 26 Uppercase letters: ATNORACFD, etc.
- Special characters: ($@#)_"^)#+ and the rest (note, not all Operating Systems accept all specials. Check the documentation.)
- Numerals: 1243098, etc.

A good, "strong" password has 8 or more characters and 3 of the 4 elements above.

There are ways to make up a password that can't be cracked using a "dictionary" attack (trying to use all the words in a big electronic dictionary). For example, if you lived in Groton, CT, in 1976, you could make up a password like:

```
gro+oN-76
```

You substitute the T with a + (plus sign), Capitalize the N, and put the date at the end. You could also use

```
19Gr@ton76
```

Put the century (19) at the beginning, Capitalize the G, and substitute the @ (at sign) for the first "o" (OH). Then put the years (76) at the end.

These look hard, but if you do the substitutions and capitalization in a way that makes sense to you, they are easy to remember.

These passwords have a low probability of being cracked easily. When you change them, pick something equally easy for you to remember.

Other Controls: Pay Attention!

In security-speak, *"controls"* are things you use to protect against a possible attack or vulnerability. Your Userid and Password are controls. You have lots more.

My other controls are regular monitoring and change where compromise seems possible: I check my credit union reports regularly and monitor my bank accounts/charge accounts every day or so. This is safer than waiting to see what's going on by reading a paper statement only once a month. [4] In fact, a recent Javelin Research paper found that unsecured online transactions were responsible for fewer than 2.5 percent of identity theft cases. The report even recommends canceling paper bills and statements in order to reduce the risk of theft or loss. [5]

If I even *misplace* an ATM card or charge card for more than a couple of days and can't find it, I call and get it reissued.

And my credit card companies are more paranoid than I am — they call me if anything unusual shows up, and their thresholds are lower than I'd expected.

"Hi, this is Credit Card America. Can you tell me the last two charges on your account? Did you by any chance buy first class tickets to Hong Kong and a Lamborghini?"

Is my SSN out there?

Although we've been talking about passwords, I found this article while doing research, and thought it was valuable to share. Since using a Social Security Number is a valuable jumping-off point for identity theft, being able to do at least a first look seems very useful.

In February of 2007, the New York Times wrote an article about limiting the potential of your Social Security Number (SSN) being out there for people to use in identity fraud. [6]

http://www.nytimes.com/2007/02/24/business/24money.html?ex=1173844800&en=bb233458d0555671&ei=5070

For people wondering if they should be worried about the security of their own numbers, there is a new tool to help them.

TrustedID, a company that sells services to consumers to give them more control over who sees their credit reports, has compiled a database of compromised numbers that could already be traded or sold on the Internet.

It has created an online search tool, StolenIDSearch.com, where people can check at no cost to see if their number is one that is in a too-public domain.

Put on your armor and fight back

Clearly, there are things you can do to protect yourself, and tools out there to help you. Use passwords, and make them strong. Don't use the same password on less important sites as you do on your financial accounts. Check your credit rating; look for your SSN online, and read your bank account transactions and credit card transactions online every day or two. Be smart. Wear your armor. Fight Back.

Other References and Resources

Ellis, Steve. *Internet Banking: Safer Than You Think*. eWeek. 25 July 2005. Accessed 8 Mar 2007. http://www.eweek.com/article2/0,1895,1839262,00.asp

Special Report on Identity Management. eWeek.com Accessed 8 Mar 2007. http://www.eweek.com/category2/0,1874,1649818,00.asp Note: there are many articles on technologies, which are mostly useful for businesses. However, there are many articles on personal practices to protect your identity, and you should sort down the list of articles and find them.

Finding out if your SSN has been stolen. In February of 2007, the New York Times wrote an article about limiting the potential of your Social Security Number (SSN) being out there for people

to use in identity fraud. http://www.nytimes.com/2007/02/24/business/24money.html?ex=1173844800&en=bb233458d0555671&ei=5070

Notes

[1] Harvard Center for Cancer Protection. *What's your disease risk?* Last updated Nov 2006. Accessed 8 Mar 2007. http://www.yourdiseaserisk.harvard.edu/

[2] Emigh, Aaron. *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*. Radix Labs. 3 Oct 2005. Accessed 8 Mar 2007. http://www.antiphishing.org/Phishing-dhs-report.pdf

[3] Germain, Jack. *Protecting Yourself Against Online Identity Theft.* Newsfactor Network. 6 Feb 2007. Accessed 8 Mar 2007. http://www.newsfactor.com/story.xhtml?story_id=01300170BTPH&page=1

[4] Westin, Liz Pulliam. *Go paperless for safer banking.* MSN Money Online, Feb 2007. Accessed 9 Mar 2007. http://articles.moneycentral.msn.com/Banking/BetterBanking/GoPaperLessForSaferBanking.aspx

[5] Monahan, Mary T, Editor and Analyst. *2007 Identity Fraud Survey Report FULL VERSION — Identity Fraud Is Dropping, Continued Vigilance Necessary.* Issued Feb 2007. Accessed 9 Mar 2007. http://www.javelinstrategy.com/research/2 (Consumer version is also available.)

[6] Darlin, Damon *Think Your Social Security Number Is Secure? Think Again.* New York Times, 24 Feb 2007. Accessed 28 Feb 2007. http://www.nytimes.com/2007/02/24/business/24money.html?ex=1173844800&en=bb233458d0555671&ei=5070 (May require registration; I believe their privacy policy is acceptable.)

This entry was posted in Uncategorized by **Editor**. Bookmark the **permalink [http://bcis.pacificu.edu/interface/?p=3357]** .

ONE THOUGHT ON "HOW MUCH PROTECTION IS ENOUGH?"

Evonne Ahr
on **February 5, 2014 at 6:26 PM** said:

Aan al diegenen die niets in te brengen, maar schreeuwen naar de post te hebben, heb ik een offerte voor u uit Denis Thatcher: "Beter je mond te houden en worden gedacht een dwaas dan openen en verwijder alle twijfel."