Perfect Passwords

SELECTION, PROTECTION, AUTHENTICATION

Create Password Policies That Baffle the Bad Guys, Not Your Users

- Master the 20 Pointers for Perfect Passwords
- Build Password Policies That Won't Be Ignored
- Check Out the 500 Worst Passwords of All Time

"DUDE, THIS IS PRETTY COOL STUFF."
—JESPER M. JOHANSSON
MICROSOFT CORPORATION

Mark Burnett
Dave Kleiman Technical Editor

Chapter 7

Living with Passwords

Solutions in this chapter:

- **Making Passwords Convenient**

Making Passwords Convenient

Let's face it; passwords aren't going away anytime soon. Because no matter how much the world's authentication technology advances, chances are it will in some way always depend on a secret that only you know. Meanwhile, password-cracking methodologies will advance, and computers will become increasingly more powerful. You really won't be able to get away with your *cupcake55* or *beachbum* passwords for much longer. You need to learn how to build strong passwords that you can conveniently live with. By convenience, I mean a password that you can easily remember and type easily and quickly.

Remembering Passwords

When my youngest son was five years old, he had a 15-character password for our computer. He had to because that was my policy—even on my home network. Sure, that seems rather extreme for a home network, but I am a security consultant, so it is my job to keep up with the best security practices, even if it is at home. I am not worried about anyone cracking my son's password; it's just my policy, and everyone follows it. My family may hate it, but they follow it.

My son remembered his password just fine and had no trouble typing it in to the computer. What was his password? It was the letter *O* typed 15 times. He happened to like the letter *O,* and he could count to 15 so that was his password. The point is that he found a password that met my policy requirements yet it was something even he could remember. This is what can make passwords so easy to remember: we can build them based on our own experience. We remember the passwords that mean something to us.

Psychologists, scientists, educators, and others have developed many techniques for improving our ability to memorize information. We have all learned techniques such as mnemonics and association. All these techniques are based on the assumption that we are memorizing information that we did not choose. The advantage of memorizing passwords is that you get to choose what you are memorizing. So rather than worrying about how to memorize the passwords you select, you just have to select passwords that you can already memorize.

Several years ago, I set out to create Pafwert, a software application that would randomly generate strong passwords that are easy to remember. The biggest challenge was trying to find out what types of passwords people found most memorable. I based many of my original attempts on well-known memorization techniques, but it turned out that these were not the most effective.

As humans we have different parts of the brain that are tuned for certain tasks. When we memorize something, we may use different parts of our brains. For example, a visual memory, such as remembering someone's face, may be handled by one part of the brain, whereas a memory of a process, such as driving a vehicle, is handled in a completely different manner. The information we remember might contain images, colors, shapes, sounds, smells, tastes, touch, positions, emotions, meaning, knowledge, context, time, and elements of language. The words in a password have some meaning to us, and the letters and characters may form some pattern. The words in a password make a certain sound as we say them in our heads, and typing the password is a kinesthetic process.

I found that the most memorable passwords were those that spread out the work across our brain, making use of various memorization techniques. This combination of techniques makes the password meaningful to us, and therefore, it is easy to remember.

We see this happen all the time with songs. We get some phrase of a song stuck in our heads while we cannot seem to remember other parts of the song (in which case we make up our own words or use the words *blah blah blah* in place of the real words). Why do some parts of the song stick in our heads, while other parts don't? Moreover, why do the most annoying songs seem to be the only ones that become stuck in our heads? That might actually be part of the answer—the fact that a song annoys us might give it meaning for us and therefore make it easier for us to remember.

In the following sections, we discuss some elements that you can use to make your passwords easier to remember.

Rhyming

Do you know what year Columbus sailed the ocean blue? If you know that answer, you probably know it because of a rhyme. Rhyming is a wonderful device that makes a password much easier to remember. Our minds seem to grasp rhymes in such a way that we instantly remember them with little or no effort. An entire phrase becomes a single piece of information in our minds that sometimes has a poetic or musical quality.

To show how much of a difference rhyming makes, consider the rhyming English spelling rule *I before E except after C.* This is a simple rule that Englishspeaking children learn at a very young age. What makes the rule so simple is that it rhymes. If the rule were *I before R except after H,* it would have nowhere near the rhythmic echo as the real rule.

Here are some examples of passwords that use rhymes:

- Poor-white-dog-bite
- Icecream2extreme
- Teary/weary chicken theory
- Thick, thick Rick

Repetition

Like rhyming, repetition adds a sort of rhythmic echo to our passwords that our minds can easily recall. When used correctly, repetition can create tempo and rhythm in our passwords, thereby making them very easy to remember. And most important, repeating means your password is longer, but there's nothing new to memorize. Remember to integrate repetition into sounds, meanings, and other aspects of your password.

Here are some examples of repetition:

- Chicky-chicky running
- 2bitter@2bitter.com
- C:\files\myfiles\newfiles\
- Purple, purple pineapple

Visualization

Visualization can be a fun device for remembering passwords. We all use visual memories to a varying degree, but it is so much easier to remember a password that we can see in our mind. It doesn't have to be a single image; it can also be a journey or a process that we visualize. The more senses we involve, the easier it will be for us to remember. Here are some examples:

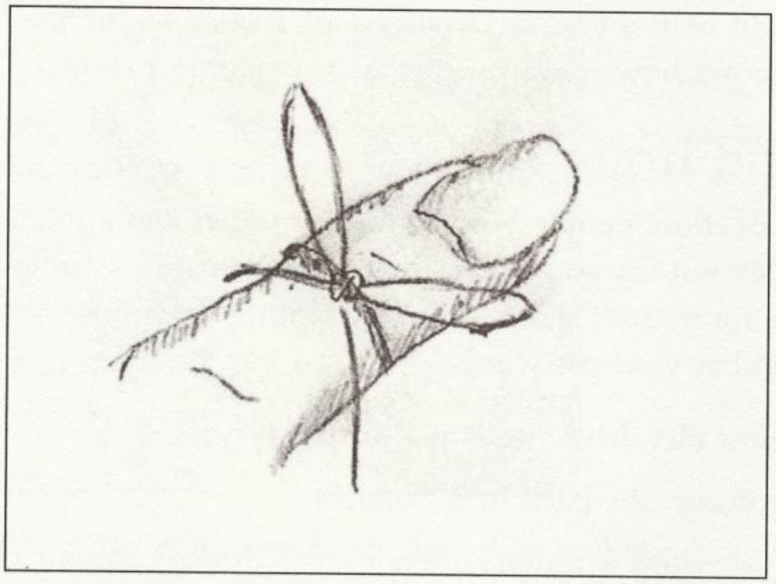
- Jabba the Hut doing the Cha-Cha
- Paquito sat on the apple!
- Frozen banana in my shoe

- Bun-mustard-hot dog-pickles
- Popping packing poppers

Association

It is sometimes intriguing how our minds wander from one thought to another, each thought triggered by an association from a previous thought. After a few minutes of our minds wandering, we marvel how we went from thinking about key lime pie to thinking about a mistake we made on our 1999 tax return. Our minds build complex and often nonsensical associations that trigger our memories. The interesting thing is that the association does not have to be a logical relationship. For example, we can remember a dentist appointment by tying a string around our finger. We see the string and remember our appointment through association (see Figure 7.1).

Figure 7.1 Tying a String on Your Finger As a Reminder



Several years ago, I was traveling for work and purchased a new notebook computer. That night I sat in my hotel room, installed Windows, and set a very strong administrator password. I then created a power user account that I could use daily. While traveling again about a year later, I happened to be in that very same city and at the very same hotel. I had a problem with my laptop and needed to log in to the administrator account to fix it.

I then realized that I had not used that password the entire year and could not remember what I had set. I did not have that password recorded and faced a big problem. I stared around the room contemplating possible solutions. I looked at the furniture. I looked at the coffee pot on the desk. I looked at the curtains. Suddenly, I remembered my password that I had not used in about a year.

How did I remember it? I was sitting in that very same hotel staring at the same furniture, the same coffee pot, and the same curtains when I first set the password. Being back in that environment was enough for my mind to associate these items with my long-forgotten password.

Sure, it might help if your associations are related to the password itself, but this story shows how powerful mental associations can be.

Humor and Irony

If you are one of those people who can never remember a joke, this technique is probably not for you. Nevertheless, we remember things that stand out for us. And funny stuff stands out. Any amount of humor and irony will help you remember your passwords:

- Was Jimi Hendrix's modem a purple Hayes?
- Gone crazy…be back in 5 minutes.
- Your password is unique—like everyone else's we put the "K" in "Kwality."
- Had a handle on security… but it broke.
- A dyslexic man walks into a bra...
- A fish with no eyes is a f sh.
- My reality check just bounced.

Chunking

Chunking has been used for a long time as a memory technique to help people remember things such as phone numbers. A simple fact is that remembering two or three small chunks of information is easier than recalling one large chunk. Research has shown that humans have the capacity to memorize five to nine items at a time. However, we can bypass this limitation by splitting things into smaller chunks and memorizing the chunks.

Here are some ways to use chunking in your passwords:

- Xzr--FFF--8888
- GgggH123-->software
- C51..D45..R22
- Explor+ation+vaca+tion

Exaggeration

Exaggeration is a fun technique that I sometimes use to make memorable passwords. Exaggeration is the technique of extending visual images or facts beyond their expected physical or logical bounds. Here are some examples:

- 43 o'clock
- December 322, 2005
- I Kicked the back of my neck

Offensiveness

Offensive words certainly do stand out. And they will stand out in your minds if you use them in your passwords. Offensive words includes swear words, gross words, slang, racial and religious slurs, crude behaviors, putdowns, insults, alternate words for sexual organs, and so on. If it offends you, or you know it will offend someone else, chances are you will remember it. Here are some examples (Warning: some might be offended).

- brutus@wrinkly-penis.gov
- OK well, just use your imagination…

Gripes

Finally, if something really bugs you, use that for a password:

- It says 10 items or fewer!
- Why is it so hard for you to merge?
- Honk if you ARE Jesus
- Justfindanotherparkingspottheyaren'tgoingtopulloutyoulasyslob

Other Memorization Tips

Despite all these techniques, remembering complex passwords still requires some mental activity. Never try to remember a password in a rush or while you are distracted with other concerns. Don't set a new password right before a weekend or holiday. Relax and think about your password for a few minutes and process it into your mind. Try teaching yourself your password or explaining to yourself the steps you followed to remember the password.

Typing Passwords

When you build a password, you should also consider how you type the password. Before setting a password, I give it a trial run on the keyboard. Some passwords are just harder to type and some passwords are prone to typing mistakes. If your password doesn't flow on the keyboard, just pick something else. Watch out for passwords that force you to type slowly or make obvious movements such as holding down shift to type a punctuation symbol or moving your hand to the number pad to type a long sequence of numbers.

Another thing to consider is how your password sounds when you type it. You can easily tell when someone's password is the same as their username because you hear the same exact typing sounds twice in a row. Some keys, such as the spacebar, make a distinct sound when pressed. Sometimes keyboard sequences, such as QWERTY have a distinct sound to them once you train yourself to hear it. The way a password sounds obviously isn't a huge risk for most people, but it certainly is something to think about.