

Passwords stacking up? / Courier News
by Michael Danahey

February 22, 2007

There was a time in the not-too-distant past when the only digits you might need to remember to get through the day were your telephone number, your driver's license number and Social Security number -- and maybe the combination to your gym locker.

These days, in addition to those, Alice Hutson of Lake in the Hills has a key code to open the front door at the Dundee Township Park District Recreation and Fitness Center in Carpentersville, where she works the front desk; passwords for her computers at home and at the office; and passwords for her voice mail systems at work, home and for a cell phone. Her car has a password entry, too, but Hutson opts for the remote button key.

"I didn't ever realize I needed that many," said Hutson.

Hutson's need for numbers pales in comparison to John Bussert of Swift Technologies in Elgin. He needs 50 passwords for the various devices and Web sites he might have to access on any given day, while Joe Tokarski, Chicago region IT manager for Comcast, lives a life requiring about 300 such secret codes.

Of course, Bussert and Tokarski work in computer-related jobs, meaning they have a better handle on dealing with keeping their Internet Age dealings secure.

Still, Bussert admitted that all too often he's forgotten passwords, having to go through the hassles the rest of us do, either resetting ones for Web sites or in some cases registering again to get access.

Tokarski said it's common for someone to have about 20 passwords these days, and there is evidence to back up his claim. Research conducted by East Coast-based RSA Security found that people use between six and 12 passwords just at the office, while a study conducted by the Software Usability Research Laboratory at Wichita State University found that the students there averaged more than eight passwords.

Further, the college research showed that although the students knew they should take steps to keep their access safe, they were not following through with such measures. For example, more than half the respondents said they never change passwords unless required to do so.

Another potential source of trouble is that many people "pick common names and words for passwords. That makes it relatively easy for a hacker to find, given there is software that basically scans through a dictionary's worth of terms in about an hour," said Tokarski. And too many people also use their own name and/or birth date as their password, another combination that is easy to uncover.

People also tend to use the same passwords for work as at home, Bussert noted. Further, they should not have the same password for the Web places they visit for financial matters, shopping and sites they like to visit that might require registration, such as newspapers, MySpace and You Tube.

You should change your passwords every couple of months, which can add to the confusion. Bussert noted an Internet discussion group where that topic came up for businesses. That task obviously can add to the workload, but "it can really force you to have a way to keep track of (passwords)," said Bussert.

While you might have to access dozens of devices and/or Web sites with passwords, that doesn't mean you need to have that many different ones. Tokarski recommended coming up with a few common passwords, which should be changed at regular intervals, and making them complex.

"Take the name of someone you know and write it backwards, making some of the letters small case and others upper case. Throw in some numbers for good measure, and throw in some keyboard symbols to make it extra tough, as those are harder for hackers to crack," Tokarski said.

Both men strongly suggested making each password at least eight characters long, too, and Bussert suggested using a phrase instead of a name or single word.

Also remember, "never to give anyone your password, including representatives from companies that call you," Bussert said. "The only time you have to give them their password is when you initially create a password or when you want to change it. So watch for phishing e-mails that ask for passwords. Companies do not ask for passwords. They don't need them. They have them already, or an encrypted version of them.

"Instruct your children never to give out passwords, and continue to remind them to not do so. Kids have a hard time keeping a secret when they know they are supposed to keep it and it is important," he added.

You also should be careful when using a laptop computer in public, shielding password entry much like you would your PIN number at the store, Bussert said.

Some people write down their passwords in notebooks tucked away for safe keeping. However, Tokarski said he memorizes the passwords he uses, while Bussert uses Password Safe, shareware from the Internet that encrypts a database with all the passwords you might want to store in it. Of course, you'll need to recall a password to access your secured ones.

As for how things might be getting safer, some Web sites and devices have "two factor" authentication, Bussert said. Tokarski mentioned one such system in the eToken line from Aladdin, a software digital rights management business with its U.S. headquarters in Arlington Heights. Tokarski also mentions .NET Passport from Microsoft in which Windows XP users set up a single name and password for certain services and Web sites.

Bussert said that other security-related technologies are in various states of development. Those include access through fingerprints; iris, facial, palm and retinal scans; voice prints; signature dynamics; and even keyboard dynamics, which can ID you by the tendencies you have when you type.

Anecdotally, at least, Bussert said he has noticed consumer resistance to using such options.

"I asked one of the cashiers at Jewel a few weeks ago about how many people really use the fingerprint reader," Bussert said, "and she told me almost no one uses it, even though it is safe and secure."