

ISSUE #28 – 2nd Quarter 2009

Protecting Your Passwords from Thieves

Protect Your Passwords from Hackers and Identity Thieves

Do you stash your spare house key underneath the front doormat? Do you leave your car keys tucked behind the visor? We hope not-- these common hiding places are usually the first place thieves choose to look. So why are so many people careless with their online passwords?

According to a 2007 survey conducted by McAfee, the computer security firm, people who use the same password for online accounts are increasingly at risk from online fraud and identity theft. As many as 16 percent of people surveyed used the same password for online accounts, while 41 percent never changed their passwords.

Since most users choose passwords based on their hometown, birthday, school, or name of pet, clever hackers can data-mine social network sites like Facebook for valuable clues. This was probably how a twenty-something French hacker broke into several Twitter employees' e-mail accounts to gain access to confidential business documents.

Let's face facts: passwords aren't very secure because most people don't bother writing them down, so they tend to use the same one across a broad range of sites-- banking, shopping, and social networking sites.

Who wants to bother remembering a bunch of difficult passwords? So the human default mode is to stick with the same old password, and thus simplifying life for shady individuals trafficking in online identity theft.

Eric Thompson, founder of AccessData, a technology forensics company that makes password-guessing software, recently told Slate.com "that most passwords follow a pattern. First, people choose a readable word as a base for the password--not necessarily something in Webster's {dictionary} but something that is pronounceable in English. Then, when pressed to add a numeral or symbol to make the password more secure, most people add a 1 or ! to the end of that word."

Slate's technology columnist Farhad Manjoo has a great idea on how to quickly fix your passwords in less than five minutes. He says it "a foolproof technique to secure your computer, e-mail, and bank account."

Here's Manjoo's elegant little brainstorm: create a made-up phrase that combines easy-to-remember random sentence fragments. For example, "the moon is made of cheese" and "I love croissants." Turn your phrase into an acronym but try to use some numbers and symbols and capital letters, when appropriate. In this specific case, the mnemonic password is TmiMocilC.

Beth Givens, of the Privacy Rights Clearinghouse, writes that "the strength of a password is a measurement of its effectiveness in resisting guessing and attacks." It would be hard to see how someone could guess "TmiMocilC,"

Because there's password-decoding software, which, according to Slate.com "uses a brute-force technique that tries thousands of passwords until it guesses yours correctly {and it can also} incorporate your computer's web history in its algorithm--all your ramblings on Twitter, Facebook, and elsewhere," you should be extra vigilant about your passwords.

In addition to creating a password acronym, as Manjoo suggests, Givens offers a few more tough-to-crack passwords pointers:

- ✓ Don't use personal information like any part of your name, birthday, and Social Security number.
- ✓ Passwords become harder to steal with each character that you add, so longer passwords are better than shorter ones. A brute-force attack can easily defeat a password with seven or fewer characters.
- ✓ Create different passwords for different accounts and applications. That way, if one password is breached, your other accounts won't be put at risk too.

The first step in thwarting identity theft when it comes to password protection is realizing the growing enormity of the problem. A 2008 survey by Accenture found that nearly half the Internet users queried said they use just one password for all their online accounts. Accenture's report said that many computer users underestimate the potential of this cyber threat. Organized cyber criminals can reap big profits from selling stolen identities.

"There's a lot of confusion out there - a lot of people don't think there's a problem," says Robert Dyson, a senior executive in Accenture's global security practice. "There's still the kind of head-in-the-sand situation: 'My identity hasn't been stolen. I don't know anybody who's had their identity stolen. So it must not be happening.'"

But it *is* happening. Take the necessary precaution so you won't be an identity-theft victim. Start with your passwords.

If you think you are a victim of identity theft, please contact Identity Fraud, Inc. at:

**1-866-4-IDFRAUD
(1-866-443-3728)**