SWCP Portal
January 2013

New Years Security Issue

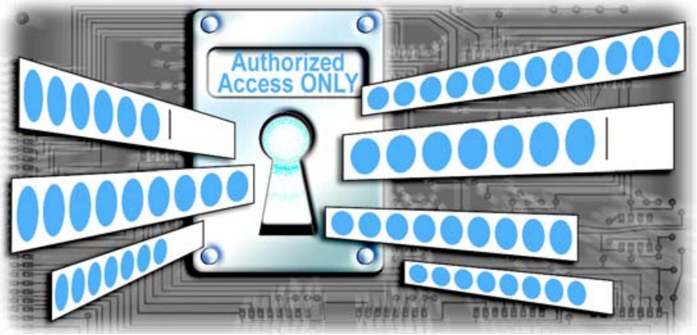
Protection beyond passwords

Passwords are essential keys to online existence. They are the main line of protection for privacy and security, the magic "open sesame" that allows entry to messages, services, wealth, and worlds online. Without them, the Internet would be even more of a dark, forbidding, cyberjungle where obscurity is the only defense against anonymous marauders.

Unfortunately, passwords are also a major pain – and might not be all that effective, either. There are many problems inherent in their use. They can be lost, stolen, guessed, forgotten or misremembered. Much of the advice from "experts" is contradictory or difficult. Users are solemnly told to make up unique usernames and long, unmanageable, confusing strings of unique characters for every account. Never write them down but don't forget to change them every so often, either. No wonder some simply give up trying.

Millions of passwords have been leaked, more than enough to get a good idea of how they are used. The most frequent password is "**123456**" while the next most common is "**password**" and the hundredth is "**please**" and so on. Oddly enough, "**sesame**" didn't make the worst 500 list. But easily obtainable software **password cracking programs** not only look for these but entire dictionaries. So people are told to mix numbers for letters, combine upper and lower case, and make them as long as possible – and try not to confuse themselves in the process.

Such rigamaroles seem necessary because anything done to make passwords easier benefits the bad guys almost as much as it does the rest of us. Life online has become an ongoing battle of wits. Empowered by ever more sophisticated social engineering techniques, those who wish us harm are only getting trickier. And passwords may no longer be enough to maintain both reasonable convenience and privacy.



Growing threats

Meanwhile, cyberspace is daily becoming scarier. There are constant news reports of major hacking attempts. Worse, the line between criminal attacks and **cyberwarfare** has become a vague frontier at best, as nowadays state-backed hackers go after big banks and corporations while mafia gangs hack into public infrastructures to hold them up for ransom.

It's not just utilities being assaulted either but common users. **Ransomware** attacks have become much more frequent. In them, a user may find a splash screen suddenly appearing on his or her computer. Accompanied by the logo of the FBI or other law enforcement agency, it sternly informs victims that they have been caught doing something illegal or embarrassing, like downloading copyrighted materials or porn. They are told that the computer is now locked down – which it is – and given instructions on how to pay the "fine" to get their machine unlocked.

The terrified prey usually does indeed rush out to buy a pre-paid credit card to send the hackers cash. However, victims' computers will *never* be unlocked by the hackers because any compromised computer is still worth money in the criminal underworld.

Even if used only for email and websurfing with no banking, merchant, or any other online accounts, such zombified devices are still valuable to Internet mobsters. There are even online forums where access to hacked computers as well as the passwords and account information stolen from them are openly traded among criminals.

Just how vulnerable everyone is these days was amply shown last year when two noted tech writers for *WIRED*, Matt Honan and David Pogue, sophisticated but ordinary users, were hacked by a criminal gang of kids. Though both victims knew and used

Continued on back

Continued from front

good password practices, they were somehow tricked. Within an hour, all of Honan's accounts were disabled and all his files wiped out. Was it maliciously done for money or access to secrets? No, all the teens really wanted was to own his Twitter handle.

Dark clouds

Experiences like this point out modern vulnerabilities especially with **cloud computing**. The idea of the cloud is to have all services available anywhere, anytime, which means that good identification verification is absolutely vital. Yet meanwhile, all these accounts have become linked in a giant daisy chain, often by a single email address. Getting into one frequently now allows an easy way into a slew of others.

Other steps, such as a **pass phrase**, like your mother's maiden name or where you went to high school, may not help security but merely make penetration easier. Many times that information can be found online or guessed with a little knowledge of the target.

Such data might be sufficient to fool eager but naive tech support personnel to give out information or even reset passwords – thus locking out the rightful user and giving the hacker complete ownership. Thus SWCP takes certain steps to confirm your identity when you call, and we will *never* email critical account information outside our system.

Building a better password

Users are often advised that the best way to concoct complex passwords is by jumbling letters, numbers, and signs together. An easier way, some experts suggest, is **mashing up** a sentence or favorite quote as a string to make a memorable but hard to crack code. For pass phrases, a little creativity also helps. You don't have to be honest, just consistent with the answer you give, so use a wrong one that is easy to recall. Substitute your favorite sport for your mother's maiden name, for instance. Few hackers would think you actually called Mommy "`football`" – but the trick is remembering it yourself.

Password management programs are attractive and convenient, but since they live on your computer they could be vulnerable to hackers. Besides, you'd still need to come up with and recall a really good password to get into the application. Using **online password strength checkers** can show you ways to construct strong passwords, but caution's needed. And having your browser remember them for you is useful only if no else has access to your machine.

Faced with a constantly growing list of passwords and increasing memory glitches due to age, many people go old-school and just write all their site information in an address book and pray it doesn't go astray. It seems there's just no easy or simple solution to the problems with passwords.

Verification alternatives

Windows 8 can be accessed by passwords, 4-digit **PIN numbers**, or "**picture passwords**." The latter identifies users by having them draw simple patterns in 3 moves across chosen photos with a finger. While easily recalled, it might take several attempts to get in, and gestures are not something easily described or wrtten down, so passwords remain as back-up.

Other means of identification are based on **biometrics**, comparing measurements of physical details of users. However, these are not foolproof by any means. **Visual recognition schemes** can be confused by different glasses or hats or fooled by masks. **Fingerprints** can be easily lifted from the scanner's glass; not only that, but despite all the computerized instant identification on police shows, up to 20% of people have fingerprints that are naturally too fine, damaged, or blurry to be machine-read. Other biometric devices may not be able to compensate for physical changes, like a hoarse voice due to a cold.

Possibly the most foolproof systems would involve **RFID chips**, which would emit identification info when scanned. However, chips in a card or fob can be lost or stolen as easily as anything else, and the information could also be surreptitiously read or intercepted. Chips implanted within the human body raise serious medical concerns and have an old, very bad reputation. Two thousand years ago, their convenience and misuse were predicted in a vivid warning:

> *It also forced all people, great and small, rich and poor, free and slave, to receive a mark on their right hands or on their foreheads, so that they could not buy or sell unless they had the mark, which is the name of the beast or the number of its name.*
> (Rev. 13:16-17)

Maybe it might just be better if we continue to wrestle with passwords for a while more.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ⦿ **SWCP.com** ⦿ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**