



# CALIFORNIA OFFICE OF INFORMATION SECURITY & PRIVACY PROTECTION



(916) 445-5239  
WWW.INFOSECURITY.CA.GOV

ACCESS CONTROL  
INFORMATION SHEET No. 8  
JANUARY 5, 2009

## Refresher Course on Password Use

Let's be honest, passwords are annoying and it seems like we need either a password or a Personal Identification Number (PIN) for everything these days. In fact, we have so many that we can't keep track of them all. We forget to update them; and when we do, it's difficult to come up with effective ones that we can still remember, so we procrastinate changing them for months, even years. We all know this is bad, but the alternative – the painful, irritating password creation and memorization process – is sometimes more than we can tolerate. There is hope! Passwords don't have to be complex. A few simple methods can help make living with passwords a little easier.

While annoying and even taken for granted, it's important to remember why passwords are important: they are usually the first, and often only, means of protecting our personal accounts from unauthorized intrusion. Quite simply, passwords protect our personal information – information we don't want anyone and everyone to know such as financial information, health data, and private documents. In a professional context, this may include anything important to the success of the organization: trade secrets, financial data, intellectual property, customer lists, etc.

The bottom line on why we have so many passwords is that they are simpler and cheaper than other, more secure forms of authentication like special key cards, fingerprint ID machines, and retinal scanners. They provide an easy and direct means of protecting a system or account. For this Information Sheet, we'll define a 'password' as a word, a phrase, or combination of miscellaneous characters that authenticates the identity of the user.

### Password Cracking

While passwords are a vital component of system security, they can be broken or "cracked" relatively easily. Password cracking is the process of figuring out or breaking passwords that then allows unauthorized users access to a system or account.

Passwords can be cracked in a variety of different ways and it's easier than most users think. The simplest method is called "brute force" and uses of a word list or dictionary program to compare lists of words or character combination against passwords until they find a match.

Other common methods for potential intruders to nab passwords are by physically obtaining the password off a Post-It from under someone's keyboard or through a process called "social

engineering”. An example of social engineering might be a bad guy pretending to be an IT technician working on a “network” problem and simply asking a user for their password or other personal information over the phone. Many users create passwords that can be guessed by learning a minimal amount of information about the person whose password is being sought.

A more technical way of learning passwords is through network sniffers, which look at the raw data transmitted across the network. It’s possible that someone out there has at least one of your passwords right now which is why it’s always a good idea to use different passwords on different accounts.

## **How to Choose a Good Password**

In creating strong, effective passwords it’s often helpful to keep in mind some of the methods by which they may be cracked, so let’s begin with what NOT to do when choosing passwords.

*No Dictionary Words, Proper Nouns, or Foreign Words.* As has already been mentioned, password cracking tools are very effective at processing large quantities of letter and number combinations until a match for the password is found. By the same token, users should also avoid regular words with numbers tacked onto the end and conventional words that are simply written backwards, such as ‘drowssap’.

*No Personal Information.* One of the frustrating things about passwords is that they need to be easy for users to remember. Since it is alarmingly easy for hackers to obtain personal information about prospective targets, it is strongly recommended that users not include such information in their passwords. This means that the password should not include anything remotely related to the user’s name, nickname, or the name of a family member or pet. Also, the password should not contain any easily recognizable numbers like phone numbers or addresses or other information that someone could guess by picking up your mail.

A strong, effective password requires a degree of complexity and three factors can help users develop this complexity: length, width & depth.

*Length* means that the longer a password, the more difficult it is to crack. Simply put, longer is better. It is generally recommended that passwords be between six and nine characters. Greater length is acceptable, as long as the user can remember the password.

*Width* is a way of describing the different types of characters that are used. Don’t just consider the alphabet. There are also numbers and special characters like ‘%’, and in most cases, upper and lower case letters are also known as different characters. As a general rule the following character sets should all be included in every password:

- Uppercase letters such as A, B, C;
- Lowercase letters such as a, b,c;
- Numerals such as 1, 2, 3;
- Special characters such as \$, ?, &; and
- Alt characters such as μ, £, Æ

*Depth* refers to choosing a password with a challenging meaning – something not easily guessable. Instead of thinking in terms of passwords, try thinking in terms of phrases. A good password is easy to remember, but hard to guess so mnemonic phrase allows the

creation of complex passwords that don't need to be written down. Examples of a mnemonic phrase may include a phrase spelled phonetically, such as:

- 'I'm a cat!' becomes 'Im@Kat!'
- 'the quick brown fox jumped over the lazy dog' becomes 'tqbfjotld'
- 'four score and seven years ago' becomes 4S@7ya

What may be most effective is for users to choose a phrase that is has personal meaning (for easy recollection), to take the initials of each of the words in that phrase, and to convert some of those letters into other characters (substituting the number '3' for the letter 'e' is a common example).

The following table provides some examples of different characters and character sets that can be substituted for letters:

A	B	C	D	E	F	G	H	I	J	K	L	M
4 ^ @	3 6 ]3	< [ (	>  ) )	3 (-)	Ph  =	& 9 6	-  # ]~	1 !   ][	] _	< {	1  _ #  _	^^ ]V[
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
/ /  N	0 ( <> []	]>  *  0	(.) 0	2  ^	5 \$	7 +	_  ( v	\/ ^	Vv \^ / UU	>< %	\  /'	2 7_

### Extra Protection

There are also certain behaviors that users should practice to maximize the effectiveness of their passwords. Users should avoid using the same password on multiple accounts. Doing this creates a single point of failure, which means that if an intruder gains access to one account, they will have access to all of the user's accounts.

Users should never disclose their passwords to anybody unless they know them to be authorized (i.e., systems administrators). Even then, passwords should only be disclosed in person (not over the phone or by e-mail) to a known, trusted source.

Ideally, users should choose passwords that they will be able to remember – not an easy task given the complexity required of strong, effective passwords. The more complex and numerous the passwords, the more likely it is that the user will forget them. And whether it's a best practice or not, some people will take the path of least resistance and write down their passwords. So, if you do write your passwords down, write them on a small piece of paper and carry that piece of paper with you at all times. You might include some misleading, dummy passwords or other information that obscures the length or nature of the password, so at least someone who finds your list wouldn't know which ones are the actual passwords or which of your accounts they are associated with.. Guard this list with the same importance that you guard your credit cards with.

Users should resist the temptation to write down passwords on Post-It notes stuck to their monitors or hidden under their keyboards. That's always one of the first places someone will look and stories of hackers obtaining passwords through shoulder-surfing and dumpster diving

are not urban myths, they are real. Never store your list on any document you keep in your computer. An obscured hint might be okay, but never the actual password or even an encrypted version.

Users will sometimes store their passwords and PINs, authentication codes and sensitive information on their personal digital assistants (PDAs). If you do decide to store such sensitive information on your PDA, make sure to protect the device with a strong password and encryption.

### **Changing and Storing Passwords and PINs**

In order to ensure their effectiveness, passwords and PINs should be changed on a regular basis and how often you change them really depends on the account. Online financial accounts should be changed every month or two. Changing a password is relatively quick and painless compared to the irritating and expensive process of coping with the aftermath of identity theft. Just use good judgment and don't be lazy.

Obviously, passwords are just one piece of the puzzle. There are other technologies that provide more in-depth protection, but in areas where the only method of control users have is a PIN or password, the best thing we can do is be aware of security risks and keep up with their password controls.

### **Resources**

- Cliff, A.: "Password Crackers - Ensuring the Security of Your Password", Security Focus, Feb. 19, 2001. <http://online.securityfocus.com/infocus/1192>
- Donovan, Craig: "Strong Passwords," SANS Institute, June 2, 2000. <http://www.sans.org/infosecFAQ/policy/password.htm>
- MacGregor, Tina: "Password Auditing and Password Filtering to Improve Network Security", SANS Institute, May 13, 2001. <http://rr.sans.org/authentic/improve.php>
- Federal Communications Commission: "Creating Strong Passwords," July 2002. [http://csrc.nist.gov/groups/SMA/fasp/documents/id\\_auth/July2002.pdf](http://csrc.nist.gov/groups/SMA/fasp/documents/id_auth/July2002.pdf)
- University of Maine at Fort Kent, *Your Password, Your Identity, Your Privacy* - <http://www.umfk.maine.edu/password/password.ppt#256.1>

### **Acknowledgement**

The OISPP thanks the California Department of Education for allowing us to share the information they developed for their employees as the basis for this Information Sheet.