

Guidelines for Choosing a Secure Password

Choosing good passwords is the most important thing you can do to secure your accounts and avoid the consequences of a security breach.

Why Should You Care About Password Security?

Your City of Tucson, Department of Transportation username and password(s) give you access to the City of Tucson's and TDOT's computer and network systems. Should someone else guess or steal your password, he or she can masquerade as you, which means the intruder would then have access to the City of Tucson's and TDOT's computer and network systems, and to your GroupWise® E-mail account if you use the same password for both accounts. This intruder would then have the power to modify or destroy any files you have been granted access to, as well as a platform to launch attacks against TDOT's, the City's and possibly other's computer and network systems. In short, an insecure password can easily wreak havoc in your life, as the above crimes will be traced back to the account used.

Background

Attacks on computer systems, especially systems connected to the Internet, are increasing exponentially and they are becoming much more sophisticated, even though you do not hear much about it from the main-stream media. Security experts at Carnegie Mellon University estimate that more than 1.5 million passwords have already been stolen on the Internet. The importance of choosing a secure password cannot be overemphasized, and protecting your password is one of the most important principles of computer system security

How Are Passwords Stolen?

A large portion of the blame for a security breach falls on the users themselves. Users willingly share their passwords. More importantly, users are too predictable in their choice of passwords. Left to their own devices, users often choose a password that is too short or too easy to guess.

Passwords are about identity. We tend to reveal ourselves in our passwords. When allowed complete freedom in choosing passwords, an astonishing number of people choose some variation of their own name.

Do not underestimate the ease with which a password can be compromised. There are many techniques available to do this. A simple and amazingly successful password theft technique for the Hacker (or more properly – Cracker) is *password guessing* based on information they can easily obtain about someone. People often choose the name or birth date of a loved one; they use their address, telephone number, or Social Security number or some variation of these; they use the name of a favorite artist, actor, or author. Or, if we are wise enough to avoid any personal references, we often choose a proper name – perhaps with a few numbers stuck on; a word spelled backward; a letter, number and/or keyboard sequence; or a word that can be found in a dictionary. Just because we think a foreign word is obscure doesn't mean that it isn't in a dictionary somewhere (more on this below). The point is, all of these types of words are easily discovered, which makes the job of password cracking straightforward (i.e. entering your username, and simply running through a relatively short list of what your password might be).

Your best line of defense against someone misusing your account is a secure password.

A quick tour of an organization's parking lot will usually yield a few vanity license plates, which often turn up as passwords. On one network, security analysts found that two users merely hit the return key when prompted to enter their passwords, which is about the worst thing you can do. When people can select their own passwords, they naturally opt for easily remembered constructions. This leads to two related problems: easily guessed passwords and the use of dictionary words.

Sophisticated intruders, recognizing these proclivities, try such passwords first when trying to break into a system. Experience shows that when uninformed personnel choose their own passwords, two-thirds or more of the passwords can be discovered by a program that tries obvious choices. Words do not become much harder to guess by merely changing a few letters in obvious ways (such as changing an i to a 1 or an o to a 0) or adding a number or two before or after the word. If simply guessing fails, determined Crackers will try every word in *multiple* dictionaries, including common misspellings and many other variations. This is not as difficult as it might sound because computers are easily programmed to perform this task. Crackers don't even have to write these programs themselves any more because many are readily available on bulletin boards known to the cracker community.

I have seen password cracking programs with dictionaries in English, Spanish, German, Japanese, Latin, Italian, Chinese, Norwegian, Swedish, Finnish, Yiddish, and Dutch; with common jargon from Biology, Physics and Computers; of common male and female names; names from cartoons, movies, television, sports, Shakespeare, religion, and mythology; as well as common and famous place names. It wouldn't surprise me to see dictionaries of Farsi or ancient Aramaic words, either. Avoid using words or names, regardless of the language.

Even if the passwords are encrypted, crackers will simply encrypt every word in their dictionaries, spelled forward and backward for good measure, and try them all. When a match is obtained, a cracker can easily recover the word he or she had to encrypt to get the match.

Another kind of very weak password is an obvious sequence, either alphabetically or based on keyboard layout (e.g. 98765432, hijklmno or mnbvcxz). Repetition, either of a single character or a sequence, may also make passwords easier to crack.

In general, anything derived from a meaningful word (in any language) can be cracked using publicly available password cracking software.

Recommendations for choosing secure passwords

The most secure type of password would be a randomly generated one, but a random-generated password is difficult to remember. This compromises security because people write down hard to remember passwords, and ***you should avoid writing your password(s) down.***

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what your password is, but is one that you can learn. Note – I did not say, "remember." **Good passwords are created and learned**, not "chosen and remembered." (How to do this is described in detail below.) This leaves the Cracker no alternative but a brute-force search, trying every possible combination of letters, numbers, and symbols. Using this method, it could take years to crack a good password (unless you have the supercomputer resources of the CIA).

Choosing a suitable password entails selecting between eight and fifteen characters that are a mix of upper and lowercase letters, numbers, and symbols. Adding numbers, symbols (punctuation marks), and random capitalization will always improve a password, but do not use a blank space (this is a technical limitation of many computer systems). Choosing a suitable password is not a difficult task, though it will involve some careful thought.

Listed below is a (very long) checklist of "Don'ts" followed by recommendations and examples.

What NOT to Use

DO NOT use these as your password! If you just use any of the following, it's only a matter of time before your account is cracked. All of the examples below have been used before – and cracked.

- Your password should not be a word found in any dictionary of any language - current or dead -- including Klingon and Elvish!

This includes names –

any part or form of your name, your user name, your initials or those of anyone close to you, or any proper names (in any language) including nicknames, (don't attempt to be clever and make your password a simple derivation, this is - reversed, shifted by a few characters, a simple substitution code, randomly capitalized, abbreviated, doubled, etc.) ESPECIALLY the names of anyone in your immediate or extended family, pet names, boat names, etc.

DO NOT use coworkers or friends names, sports figures or teams, names of films, film stars, celebrities, TV shows, character names, or other famous or infamous folk,

DO NOT use the name of your house, street, city, home country, holiday location or any other geographic location – here on Earth or elsewhere.

- Do not just use all, part, or combinations of, any information which someone could readily obtain about you or those close to you

This includes birth dates and ages, telephone numbers, social security number, student ID number, credit card numbers, PIN numbers, mother's maiden name, home town, favorite sayings, mottos, what it says on your favorite tee shirt; the brand or model name of your computer, anything to do with your car(s), such as make, model, registration (VIN) or license plate numbers, anything to do with your hobbies or their terminology, your education, alma mater, major, licenses or certifications. (I'm constantly amazed how many people will just give you this information if you simply ask for it.)

- Do not use passwords you have used in the past or are using on other systems, particularly passwords you use for Internet sites and online shopping. If these are cracked or stolen they will be tried on other systems. Select a unique password. (The final section of this article has suggestions on dealing with multiple passwords.)
- Do not use months of the year or days of the week
- Do not use sports phrases, catch phrases, terms, or buzzwords and so forth from any sport, movie, book, or other popular media without using applied transformation techniques (details in next section).
- Do not just use Acronyms (the first letter of each word) of any of the above
- Do not just use standard abbreviations in any language
- Do not just use common misspellings of dictionary words (including replacing "l" with "1" and the like)

TDOT Information Services

City of Tucson • Department of Transportation

- Do not just use
any of the above, with a typical number substitution –i.e. "p@ssw0rd", "j3nn1fer"

any of the above spelled backwards

any of the above only preceded or followed by one or two digits
- Do not use passwords that are easy to spot while you're typing them in. Passwords like 12345, qwerty (i.e., all keys right next to each other), should be avoided
- Do not use a password of all digits, or all the same letter like "aaaaa" or patterns like "aBcDeFg" or "a1b2c3d4". This significantly decreases the search time for a Cracking program
- Do not just add just one or two characters before or after a word (!horrible or horrible!)
- Do not just randomly capitalize parts of a word (HOrrible)
- Do not just double a word (horriblehorrible)
- Do not just spell a word backwards (elbirroh)
- Do not just remove the vowels (hrrbl)
- Your password must not appear systematic (e.g. abc123)
- Do not use all uppercase or all lowercase passwords
- Do not use a password shorter than eight characters!
(also, some systems have a maximum length limit of 15 characters)

These are all very easily cracked with the powerful password cracking software now available.

DO NOT use a password that is so difficult for you to learn (remember) that you will forget it if you don't write it down! Don't write your password down!

OK, So What Can I Use ? !!

- A system that works for many people is to make up a phrase and use the first letter of each word, and include numbers and punctuation. The more unique or fanciful the better.

In this way, your password is really a "pass phrase." (For example, "Do you know the way to San Jose?" could be D!Y!KtwTSJ?). Intersperse punctuation marks or symbols such as #, \$, %, etc. Do not use a blank space. Always use a mixture of upper and lowercase characters.

However, be very careful about using common sayings, proverbs or published phrases. For example, say you like Star Trek, so you think that WnohgB4 would be a great password - it's random, right? A mixture of letters and numbers, upper and lower case, right? Wrong, it's a bad password - "Where No One Has Gone Before" -- it's been done, been cracked. Trust me. And if you're famous (or infamous!) for always using a certain phrase, then that would obviously be a bad choice.

TDOT Information Services

City of Tucson • Department of Transportation

Once you've decided on the phrase, choose the first (or last, or the second, or whatever) letter from each word. Include all the punctuation. Use a mixture of upper and lowercase characters. This will improve the security of the password. Your password should be a nice, long password with a good mixture of characters.

As an example, if our nonsensical sentence (okay, it isn't even a complete sentence -- all the better) were "fiery swans, joined ends", the password "fiSw%edds" could easily be remembered, all that needs to be remembered are the sentence and that the first two letters of the two first words were used and the last letters of the second two. Additionally, an arbitrary character (in this case, a %) has been inserted between the two logical components of the password and one letter has been capitalized. This way, even if you forget the password (and before you actually learn to remember it directly), you could think about how it was generated.

The result can be more secure and still easy to remember if you replace one of the letters or words with a digit that sounds like the letter or word.

Examples:

- "won" => 1
- "none" => n1,
- "to / too / true" => 2
- "tree / tea / tee" => 3
- "for / floor" => 4
- "before" => b4
- "fever" => 5r
- "sick / sticks / sex" => 6
- "ate" => 8
- "late" => l8
- "benign" => b9
- "oh / owe" => 0
- "no" => n0.

You can also use stylized spellings to turn ordinarily bad passwords into reasonably good ones.

Use letter substitutions such as the following:

1=i, 3=e, 4=a, 5=s, 7=t, 0=O (zero = the letter 'O')

Use 'z' instead of 's' for plurals, and use 'ph' instead of 'f'

Examples:

"Artichoke" = "4r71ch0k3"

"Freaks" = "Phr34kz"

Combine all three techniques to give an intruder a real headache.

Example: 07wh2p1:p1." = "The only thing we have to fear is: fear itself."
(Remember, 'p' is short for the 'ph' substitution for 'f').

TDOT Information Services
City of Tucson • Department of Transportation

Another example:

"I hated doing Shakespeare for English at school"

If we take the first letter of each word we get the letters: I.H.D.S.F.E.A.S.

However we can be more cryptic - let us replace some letters with characters that look like the letter or sound like the word. Let us change:

I to 1 because it looks like an I,
H to 8 because hated sounds a bit like eight,

F to 4 because for sounds like four,
A to @ because @ in web URL means at.

So we now have [with CAPS LOCK off ;-)] → 18ds4e@s

We could improve this further by shifting some of those characters. If we use the [SHIFT] key on the first four characters we get:

!*DS4e@s

which you will agree is total gibberish to others but may still have a meaning to me.
Obviously DO NOT USE THIS EXAMPLE!!!!

More examples:

Pass-phrase: "Four score and seven years ago, our fathers..."
Password: Fs&7yAoF

Pass-phrase: "My Son is 5 years old"
Password: Msi5!Yold

Pass-phrase: I have lived in California for 5 years
Password: IhliCf5#y

The password is derived by choosing the first letter from each word, using mixed case letters, and using a non-alphabetic character and a number.

- Another system is to choose two short words and concatenate them together with a punctuation character between them. It's not very secure, but it is easier to remember if you want a throw away password to use temporarily on some Internet site.

For example: ``dog;rain," ``book+mug," ``kid?goat."

Even better is to combine a few pronounceable "nonsense" words with punctuation.

For example: nuit+Pog=tWi.

In this example we have combined together the nonsense words in a way that is similar to an arithmetic formula, which makes it easier to remember. You may want to use other punctuation for similar reasons. Read the nonsense word forwards and backwards to verify it is not a sequence of one or more words found in a dictionary.

TDOT Information Services

City of Tucson • Department of Transportation

- Other strategies for choosing a good password include:

Using lines from a childhood verse (and using substitutions and transformations):

Verse Line: Yankee Doodle went to town

Password: Ydw2#t0wn

Expressions inspired by the name of a city:

City Expression: I love Paris in the springtime

Password: Il!p_itST.

City Expression: Chicago is my kind of town

Password: CismYKot!.

Foods disliked during childhood:

Food: rice and raisin pudding

Password: ricNraiPudng

Food: boiled broccoli

Password: boi%Brocc

Transformation techniques:

Technique: Transliteration

Illustrative Expression: photographic

Password: foTOgrafik

Technique: Interweaving of characters in successive words

Illustrative Expression: iron horse

Password: ihrOrnSe

Illustrative Expression: file drawer

Password: FdirLawer

Technique: Substitution of synonyms

Illustrative Expression: coffee break

Password: jaVa*rest

Technique: Substitution of antonyms

Illustrative Expression: stoplight

Password: st_aRt!dark

Remember to use both upper and lower case characters and replace a few letters with numbers or symbols.

Whatever your system, don't tell it to anyone!

Don't write it down!

And, of course, don't use any of these examples!

- ✓ **DO use a password with mixed-case alphabetic characters.**

- ✓ **DO use a password with non-alphabetic characters -**
e.g., digits (numbers) and symbols (punctuation).

- ✓ **DO use a password that is easy to learn, so you don't have to write it down.**

- ✓ **DO use a password that you can type quickly, without having to look at the keyboard.**
(This makes it harder for someone to steal your password by watching over your shoulder.)

Additional Password Protection Tips

- 1.) DON'T GIVE OUT YOUR PASSWORD TO ANYONE. DON'T SHARE YOUR ACCOUNT WITH ANYONE OR LET ANYONE ELSE USE YOUR ACCOUNT.

- 2.) DO NOT STORE YOUR PASSWORD IN AN INSECURE PLACE!
 - In your wallet, in a file (especially one labeled "passwords"), under your keyboard or on a sticky note on your monitor (really, I've seen all these). These are all terrible places to keep your "secure" password. **The most secure place to keep your password is in your head.** If you must write it down though, put it in a place that will be locked up, and difficult to find. And keep the password and username, and info on what system it's for, separate!

 - Never store your password on a computer or in a program, such as in a dialup PPP script or control panel. Many e-mail clients, web browsers, and web services will offer to store your password for you so that you don't need to type it in each time you want to use it. This is a bad idea -- it is generally trivial for Crackers to recover your password from inside one of these programs if they have access to your computer (and sometimes even if they don't). It is also possible for some computer viruses or "Trojan horses" to recover your password from such locations and e-mail them to their creator or to people in your address book. Such viruses may even distribute the password before anti-virus software is able to locate and remove the virus.

- 3.) MAKE IT HARDER FOR SOMEONE TO STEAL YOUR PASSWORD.
 - Don't let anyone see you type in your password.

 - Stop typing if you notice someone watching you.

TDOT Information Services

City of Tucson • Department of Transportation

- Use a password that you can type quickly, without having to look at the keyboard. (Some people add extra flourishes of their fingers and hands to obfuscate their movements over the keyboard for any non-casual observers.)
 - Be careful that you are typing your password in the password area, field or box, (not the username box) and that your password is not being displayed ["echoed"].
 - A password should roll off the fingers. It should be typed quickly and efficiently (and of course correctly). I sometimes will type a new password ten times quickly to generate the rhythm of it. Practice entering in your password, so you can type it in quickly, without looking at the keyboard.
 - Make sure you are not on a computer or terminal that is recording your keystrokes as you type in your password. You can usually get rid of such sneaky programs (called keystroke grabbers) by rebooting the computer (definitely recommended for Macintoshes). The safest act to perform upon walking up to a Windows PC is to give it the *three-fingered-salute* (pressing the 'control', 'alt' and 'delete' keys simultaneously) -- this will grab the attention of Windows 3.1 and 95 (allowing you to reboot them) and on Windows NT/2000/XP it will provide proof that you are performing a real NT domain login and not talking to a 'Trojan Horse' login program.
 - Be wary of any program or Web page that asks you for your username and/or password. If you have never previously seen a particular screen which is prompting you for a TDOT password, please contact the Department's I.T. staff to verify the authenticity of the request.
 - Secure TDOT web pages that would ask you for your user name and password will generally have URLs (Universal Resource Locators) that begin with "https://" and your browser should visually indicate that you are typing your password into a secure page (Browsers will display a solid key or a locked padlock symbol in a corner).
- 4.) **CHANGE YOUR PASSWORD REGULARLY!**
Many universities require passwords to be changed every 90 days.

How often should I change my password?

It is time to change your password if:

- Your password does not meet the criteria set out in the rules and recommendations listed above.
- You have had the same password for more than 6 months.
- You have told your password to anyone else.
- You suspect that some has, or is trying to, obtain your password.

Change your password immediately if you think it has been compromised. Also alert the Department's IT staff.

Handling Large Numbers of Passwords

In the modern Internet environment, people often find that almost every web site that they visit wants them to remember a password. In addition, most people have passwords to access one or more e-mail accounts and to provide access to all sorts of different Internet-based services that they wish to use. However, **using the same password in multiple locations is very dangerous**. If the password is stolen from any one of the places where it is used, it will be tried elsewhere as well.

Below are a few ideas on various ways to handle the increasing number of passwords that seem to be required these days while not making the passwords easy to guess.

- Consider what the password is protecting when choosing a password. Many passwords protect configuration settings rather than protecting access to sensitive data and/or access to e-mail or other network services. Use a single password for all such services. If the password is not protecting access to any personal or financial information *or does not allow other people to impersonate you* (for example, by sending e-mail as you), you probably don't need to keep it as secure. If you are not sure, always use a different password than you use on any other site.
- Consider your password as multiple parts, a central core of the password and a prefix and/or suffix that is specific to the service that is being protected.

For example, your core might be "gPw4", from "generic Password 4 (for)..."

If this password is to be a password for the New York Times Web Site, you might choose to add "NYt" to the beginning of the password and "n" (for "news") to the end. This would make your password: NYtgPw4n.

Your password for eBay might be eBgPw4A ("A" for "auctions").

- Choose a formula such as the ones described above for the passwords that are less important and typed infrequently, but for the most important passwords (i.e. business E-mail accounts or your most sensitive information) choose something that is in no way related to any of your other passwords.
- Don't reuse your passwords.
In one case, a stalker started a 24/7 password-cracking program against his victim. She routinely changed her password every month, but used only the same two passwords. The encrypted password that the stalker managed to obtain was cracked, but it was for the 'other' month. Fortunately, the stalker was caught (and his computer seized which is how this was discovered) before there was tragedy.

For questions or additional information contact TDOT Information Services at 791-4086

This article is based on publicly available, non-copyright, public domain information obtained from many sources and compiled and edited to present a comprehensive guide to password security for the benefit of the reader, and the general computing community at large. It shall not be reproduced with the intent of making a profit from it.

Many of the examples used in this article appear on multiple publicly available web sites. These examples were included only after determining that they were in the public domain and not copyrighted according to the web site(s) on which they were found. Oftentimes it was not possible to determine the original author. Many of these web sites are easily found by doing a web search for "password guidelines" or similar terms.

Article compiled by Casey Townsend.