



Federal Aviation
Administration

The Password Survival Guide

A User-Friendly Resource for Technical Operations



NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. This document does not constitute Federal Aviation Administration (FAA) certification policy. Consult your local FAA aircraft certification office as to its use.

This report is available at the FAA, William J. Hughes Technical Center's full-text Technical Reports Web site: <http://actlibrary.tc.faa.gov> in Adobe® Acrobat® portable document format (PDF).

Technical Report Documentation Page			
1. Report No. DOT/FAA/TC-06/26	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle The Password Survival Guide: A User-Friendly Resource for Technical Operations		5. Report Date December 2006	
		6. Performing Organization Code AJP-6110	
7. Author(s) Vicki Ahlstrom & Kenneth Allendoerfer		8. Performing Organization Report No.	
9. Performing Organization Name and Address Federal Aviation Administration Human Factors Team – Atlantic City William J. Hughes Technical Center Atlantic City International Airport, NJ 08405		10. Work Unit No. (TRAIS)	
		11. Contract or Grant No.	
12. Sponsoring Agency Name and Address Federal Aviation Administration Human Factors Research and Engineering Group 800 Independence Ave, S.W. Washington, DC 20591		13. Type of Report/Period Covered Technical Note	
		14. Sponsoring Agency Code HF R&E Group, ATO-P	
15. Supplementary Notes			
16. Abstract With security becoming increasingly important, users may be faced with 50 or more passwords. Human memory can store only limited amounts of information and can be overloaded by too many passwords. This guide is intended to help password users cope with the increasing number and complexity of passwords by providing strategies for reducing the memory load without compromising password complexity. We developed this document based on field research with Technical Operations personnel. The material is presented in a graphical cartoon format along with limited text narrative. The goal is to provide a number of easy-to-use strategies in a format that would motivate Technical Operations personnel to read it. The ideas covered are addressed to Technical Operations, but in many cases transcend Technical Operations and apply to passwords in general.			
17. Key Words Passwords Technical Operations Mnemonics		18. Distribution Statement This document is available to the public through the National Technical Information Service, Springfield, Virginia, 22161. A copy is retained for reference at the William J. Hughes Technical Center Library.	
19. Security Classification (of this report) Unclassified	20. Security Classification (of this report) Unclassified	22. Price 18	No. of Pages
Form DOT F 1700.7 (8-72)		Reproduction of completed page authorized	

The Password Survival Guide Reader Response Form

Instructions: Please copy or remove this form from the guide. Fill it out and mail it to the address at the bottom of this page. All responses will be kept confidential.

Please circle the one number that best summarizes your level of agreement with each of the following statements.

1. The Password Survival Guide is relevant to what happens in my facility.

Strongly Disagree 1 2 3 4 5 6 7 8 Strongly Agree

2. The graphics in the guide were appropriate for the concepts presented.

Strongly Disagree 1 2 3 4 5 6 7 8 Strongly Agree

3. The Password Survival Guide is a useful job aide.

Strongly Disagree 1 2 3 4 5 6 7 8 Strongly Agree

4. Please provide your overall evaluation of The Password Survival Guide.
Circle the number that best describes your evaluation from 1 (Very Poor) to 8 (Very Good).

Very Poor 1 2 3 4 5 6 7 8 Very Good

5. List any concepts that you would like to see covered in a future version of the guide or any comments you may have on the guide. Use additional sheets, if desired.

Mail to: Vicki Ahlstrom, Human Factors Team-Atlantic City, Bldg. 28, Atlantic City International Airport, NJ 08405

We are interested in knowing whether this booklet was useful to you.

Please feel free to email any suggestions and/or comments to:

Vicki.ahlstrom@faa.gov

INTRODUCTION

We wrote this booklet for technicians, system specialists, supervisors, and other personnel in the Federal Aviation Administration (FAA) Technical Operations domain, but the advice applies broadly. We hope it will help you manage your passwords more easily and securely. We developed this advice by interviewing many Technical Operations specialists about their experiences and reviewing articles and research on how to make system security user-friendly, but effective.

Long, random passwords may be the most difficult to crack by brute force (i.e., trying all possible combinations). However, from a human factors perspective, long, random passwords are extremely difficult for people to generate and remember. This can lead to decreased productivity and numerous help desk calls from people who forgot their passwords. We believe that techniques, such as those described in this booklet, that help people create stronger, yet more memorable passwords will improve information security of the FAA overall.



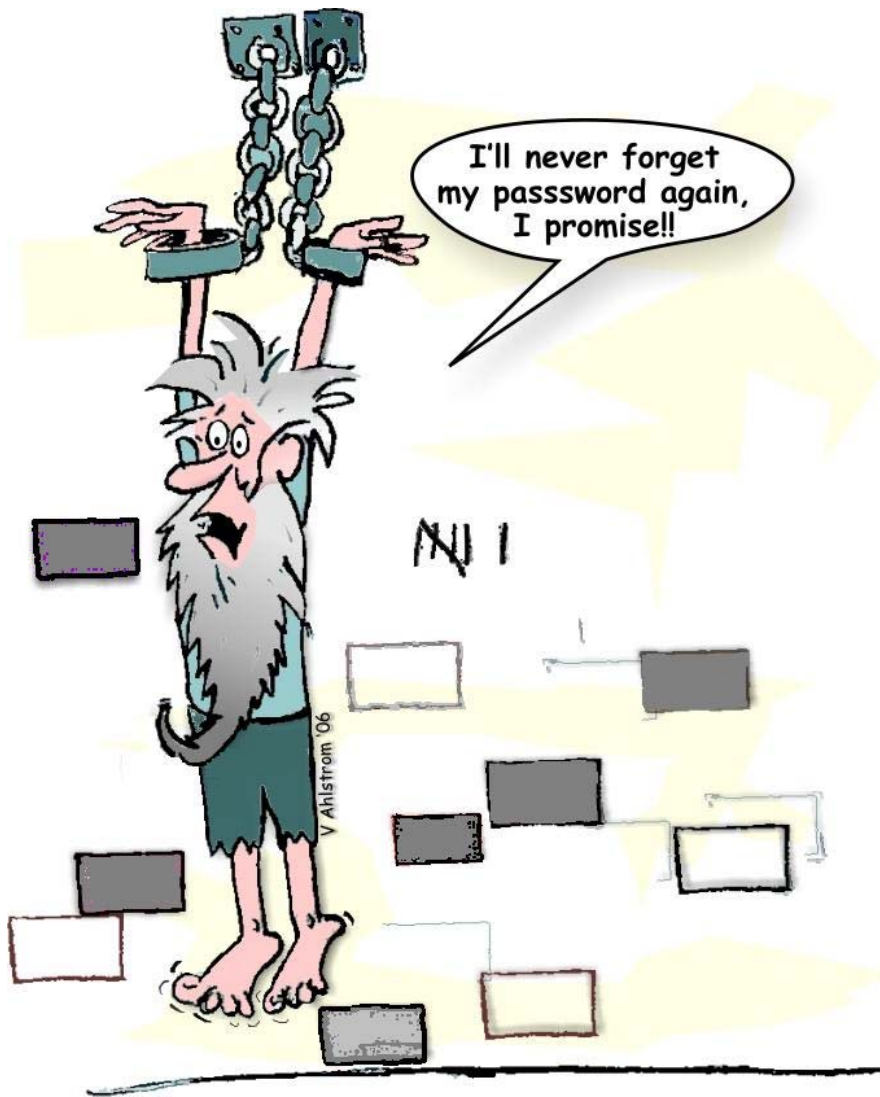
Carl Genna

Written by:
Vicki Ahlstrom & Kenneth Allendoerfer
Federal Aviation Administration
Human Factors Team-Atlantic City, ATO-P
Sponsored by Human Factors R & E Group

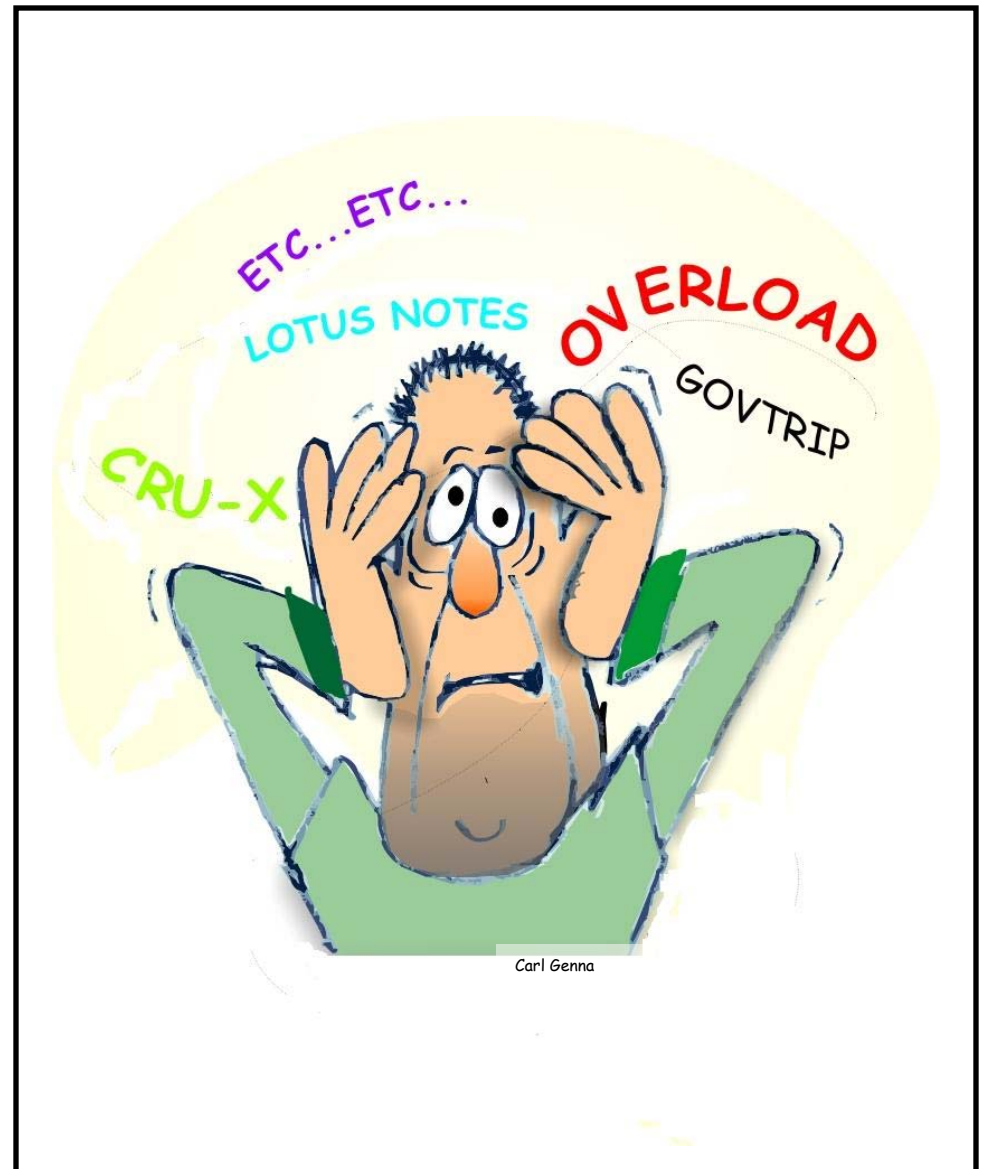
Illustrated by:
Vicki Ahlstrom & Carl Genna
Colorized by:
Larry Cole & Vicki Ahlstrom

Reference & Further Reading

- Allendoerfer, K., & Pai, S. (2005). *Human factors considerations for passwords and other user identification technique - Part 1: Literature review & analysis* (DOT/FAA/CT-05/20). Atlantic City International Airport, NJ: Federal Aviation Administration, William J. Hughes Technical Center.
- Allendoerfer, K., & Pai, S. (2006). *Human factors considerations for passwords and other user identification techniques -Part 2: Field study, results, and analysis* (DOT/FAA/TC-06/09). Atlantic City International Airport, NJ: Federal Aviation Administration, William J. Hughes Technical Center.
- Allendoerfer, K., Pai, S., & Ahlstrom, V. (2005). *Human factors considerations for user identification on air traffic control systems*. Symposium on Usable Privacy and Security, July 6-8, 2005, Pittsburgh, PA.
- Quote from Clifford Stoll available on the internet at:
http://www.brainyquote.com/quotes/authors/c/clifford_stoll.html



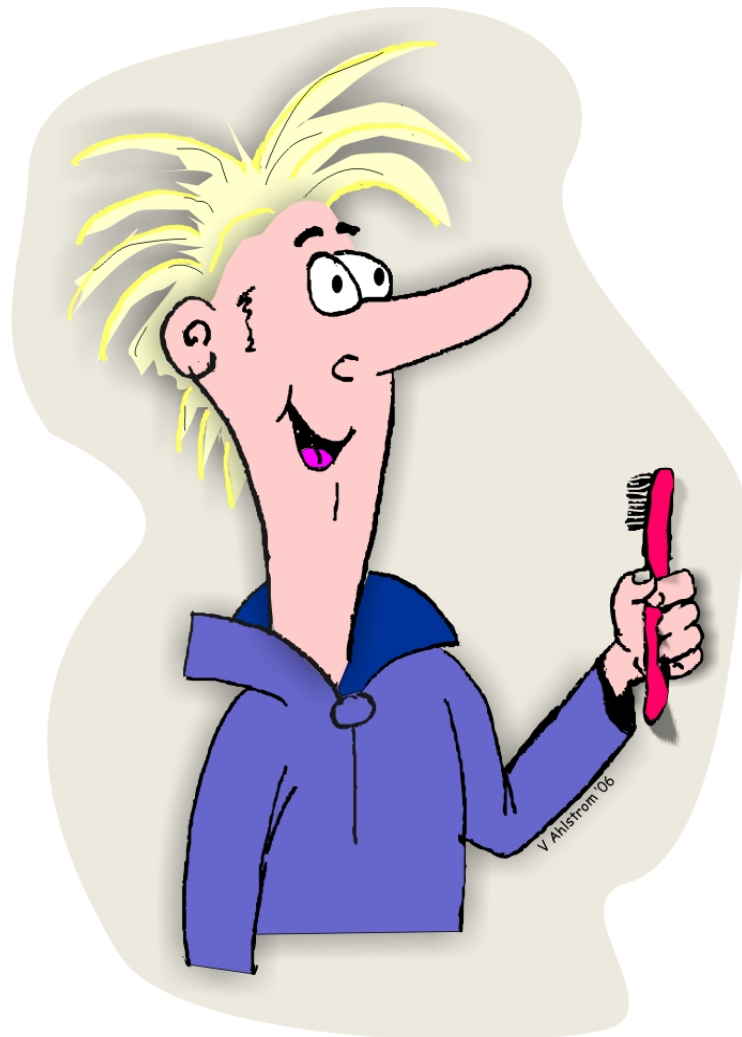
We have presented several strategies for creating memorable passwords. We recommend combining several of the strategies that are contained in this booklet to find the strategy that works well for you.



If you consider all your passwords between work and home, you might have 50 or more logins. Almost no one can reliably remember that many different complex passwords over a long period of time. This booklet contains a number of memory techniques that can help you create memorable, yet secure passwords.



There is no such thing as a completely secure username or password. The best we have are passwords that are secure *enough*. The reason for complex password rules is to increase password security. However, there is always a chance that even a very complex password could be hacked or stolen. Therefore, it is important that you don't use the same passwords for work as you do on non-work websites.



“Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every (3)^{*} months.” (Even if the system doesn't require it.)

Quote from Clifford Stoll – Author of “The Cuckoo's Egg-Tracking a spy through the maze of computer espionage”

^{*} Original quote said six months. We changed it to three months to comply with FAA recommendations.



Don't assume you know the motivations or abilities of potential intruders. There are many types of intruders with many different reasons for breaking into systems. Some are sophisticated. Some are very crude. You cannot assume that you are safe just because you're a "small fish" or because you don't work with sensitive information.



The FAA is moving toward common rules for passwords. Some of the rules that passwords will have to comply with include the following:

- Must contain characters from three of the four following types:
 - English upper-case characters (A-Z),
 - English lower-case characters (a-z),
 - Numerical digits (0-9), and
 - Non-alphanumeric characters (for example, !, &, \$)
- Must have a minimum length of eight characters
- Must not contain the user's account name (for example, Joe FAA should not use Joe1234, FAA1234, or JoeFAA1 as his password).
- Must not contain multiple characters in succession (for example, Aaaa1111 is not a good password)

To create a strong password, it is best to avoid words that can be found in the dictionary, common names, common pet names, or the names of sports teams, unless they are altered in some way.



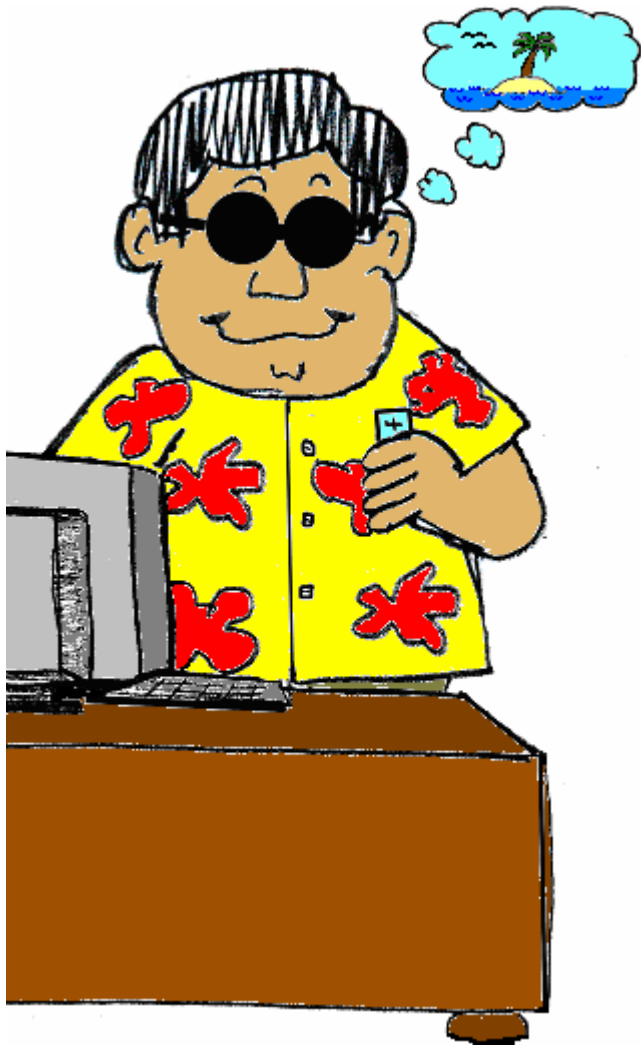
People often use the names of family members as a password. These names might be easy to remember, but they're also much easier for a potential hacker to guess. It's best to avoid using common names in your password.

If you do want to include personal information in your password, use information that is old, outdated, and more difficult to obtain or guess, or modify the information in some way.

For example, say your kids are named Marsha and Greg and they are 16 and 18 respectively. Instead of using "Marsha16" or "Greg18" you could use the first two letters and age of each combined with a symbol to create a password of "Ma16&Gr18". Or instead of using your phone number, you could substitute letters from the phone pad such as "TMP-5309" instead of "867-5309".



Know the process for obtaining a new password for every system you access, especially if you access safety-critical systems. If a maintenance action was suddenly needed on a system and you forgot your password, would you know what to do or whom to call? Is your contact available 24/7 or only during business hours? If you maintain a list of your passwords, store the system contact information separately because if you lose your passwords, you would lose the contact information, too.



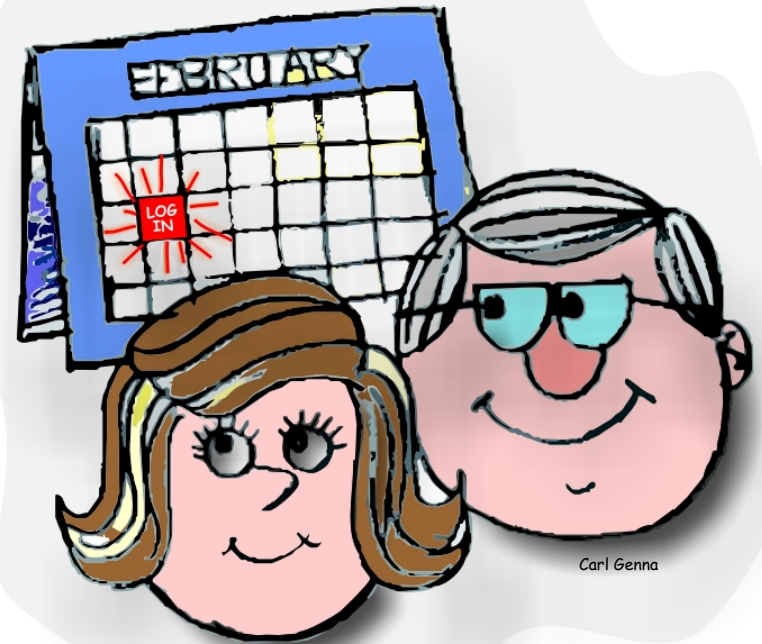
People often forget their passwords while they're on vacation or away from the facility for training. On your last day before leaving, take a few minutes and log in to all your systems. If necessary, write down the passwords, and store the list in a secure location. If any passwords are about to expire, renew them before you leave.



Intruders will try anything to get you to reveal your login information. Don't fall for it! A common trick is for the intruder to pretend to be someone trustworthy, like an FAA supervisor or system administrator. The intruder may ask for your password for a seemingly legitimate purpose like "network maintenance." These requests often come through email, known as "phishing," and on fraudulent websites, known as "spoofing." Emails looking like a legitimate organization such as a bank, may ask you to follow a link and "update your information". Don't click on links that come through email. Though more rare, these tricks also can come over the phone or in person. If someone asks for your username or password, even if it seems like a legitimate reason, politely refuse to provide it and notify your supervisor.



Hide your list! Sometimes the only way to remember all of your usernames and passwords is to write them down, but doing so makes them much easier to steal. If you must write them down, try to encode it and keep the list locked up in a place known or accessible only by you.

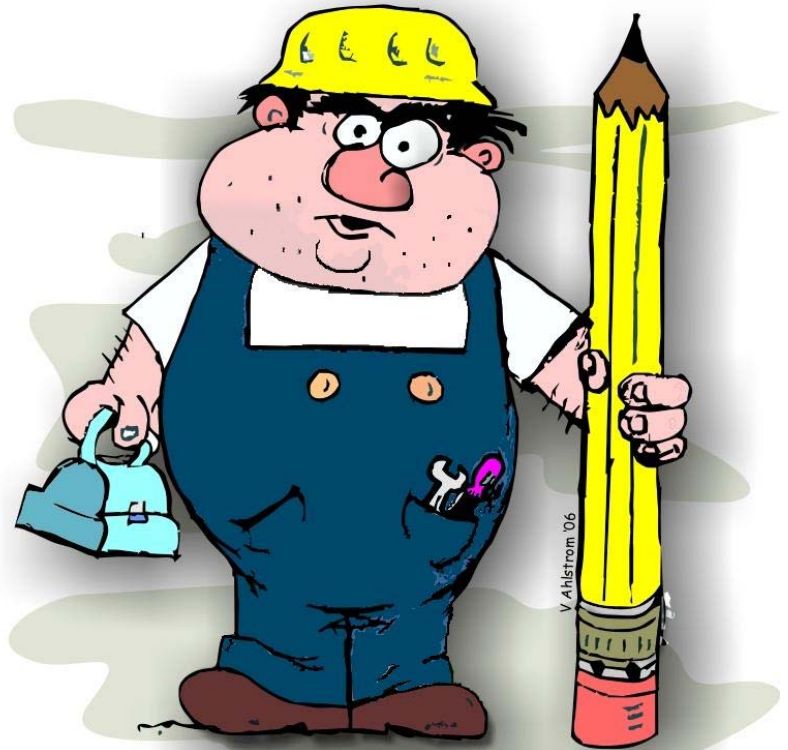


Use it or lose it. People naturally forget things when they don't use them. Logging in to your systems at least once a month will help keep your memory for usernames and passwords fresh. If you haven't used your password in the past 3 months, there's a good chance you've forgotten it or it has expired.

Super-secret
decoder ring



Become a minor-league cryptographer. If you must write your usernames and passwords down write them using a code or system known only to you. If you store your usernames and passwords on a computer file or PDA, the file must be encrypted. If someone steals your password list or accesses your file but doesn't know the code, it will be much harder for them to access your accounts.



Construct your own personal password method, apply the method to each system, and don't tell anyone. For example, your method might be a short sequence of letters in lowercase, such as four sequential keys on the keyboard (e.g., hjkl), followed by the first two letters of the name of the system in uppercase (e.g., LN for Lotus Notes), and the current two-digit month (06 for June). In the example, the password would be hjklLN06, which is a difficult password to crack without knowing the method.

By applying your personal method, you can usually derive your password even if you forget it.

How do I
spell "racecar"
backward?



Backwards. No doubt about it, words are easier to remember than random letters, but they are also easier to guess. A familiar word written backward (DrawkcaB) can still be easy to remember, but is harder to hack. By combining this strategy with other strategies or just capitalizing the first and last letter and adding a number on either end of the word (1DrawkcaB1), you can create a password that is easy to remember but complies with current rules.

Remember your sixth-grade science teacher? She taught you "Kings Play Chess On Fancy Glass Stools" as a way to remember Kingdom, Phylum, Class, Order, Family, Genus, Species. Think up a phrase or a rhyme to help you remember. This sort of technique is called a *mnemonic*. Use a similar technique to remember your username or password. For example, "tznMw2s2f1t" can become "The Zookeeper Named Moe Was Too Sleepy To Feed One Tiger."




Rehearse your passwords aloud in your car on the way home. Make your passwords rhyme, such as “Dis1Tis1Wis1,” or sing the password in your head to the tune of your favorite song. Songs are very memorable and can help you remember a password. You might feel a bit weird doing these sorts of things, but you’ll remember your passwords much better. Just remember not to sing your password in public (even if you have a great voice).



Carl Genna



Move over one key. If you have a password that works well for you and you need to change it, try moving your hands one key to the left or right, up or down. Using this technique, a weak password such as “Password1” can become a much stronger password “{sddeptf2.”



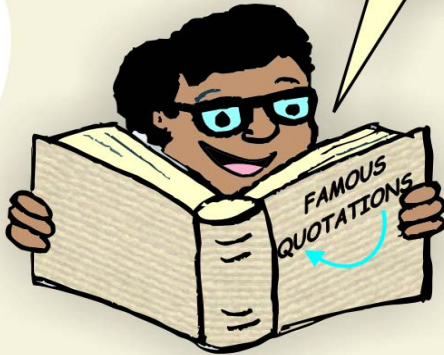
Should I use the serial number on my phone, or the model number on my keyboard or...

V Ahlstrom '06

Use a physical reminder. If you always use your password at the same location, you can use something (i.e., serial numbers, model numbers, or barcodes) around you to create a unique, memorable, and difficult-to-guess password. Changing your password can then become as simple as moving in a certain direction around your workspace to pick new objects.

Passphrases are similar to passwords but are often longer and may use regular words. Passphrases are hard to crack by brute force and can be easier to remember than short random passwords. Not all systems, however, accommodate passphrases. If you can use a passphrase, don't choose a famous quote without modifying it. For example, "Ask not what your country can do for you" is a bad passphrase because it would be included in any book of familiar quotations. However, "Ask not what your trycoun can do for you" is still easy to remember and much more difficult to guess. In this example, "country" is modified by inverting the order of the syllables.

Some phrases are short enough to be used on current systems. For example, "ILuv2Fly!" or "ILuvMy12Cats!" are phrases that could be easily remembered; yet comply with many system requirements.



"Ask not what your trycoun can do for you..."

"A nypen saved is a nypen earned..."

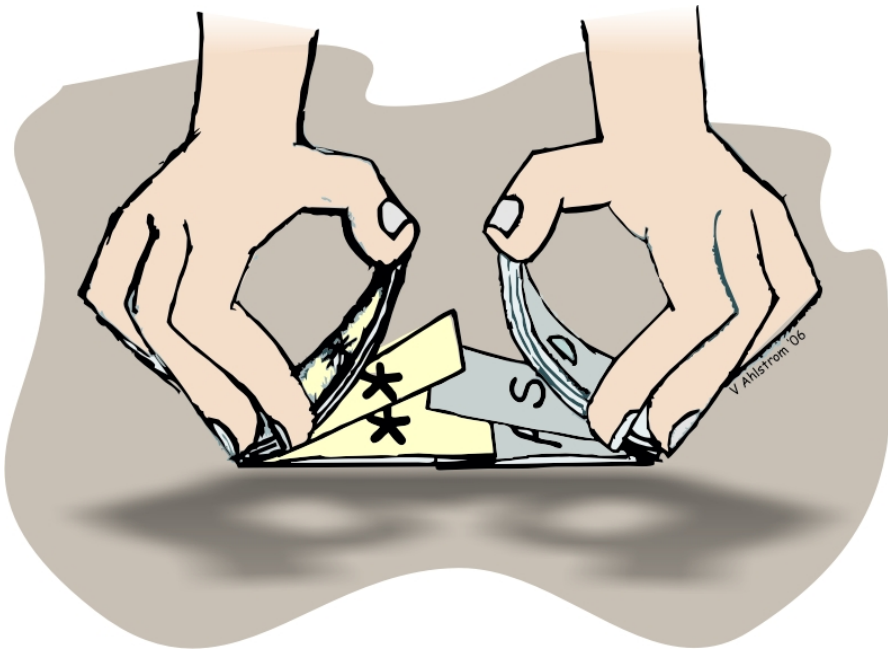


Use “shocking nonsense” to create your password or passphrase. That is, use words or images that create strong visual or emotional impact (and are therefore easy to remember) but make little logical sense. For example the passphrase, “Four rude blue mollusks are eating my hair!” (or password: 4Rbmaemh!) is very unlikely to be guessed. Concrete words tend to be easier to remember because they are associated with an image. Funny or peculiar images are easier to remember than normal ones. In addition, people are less likely to share nonsensical passphrases because they may be bizarre or embarrassing.

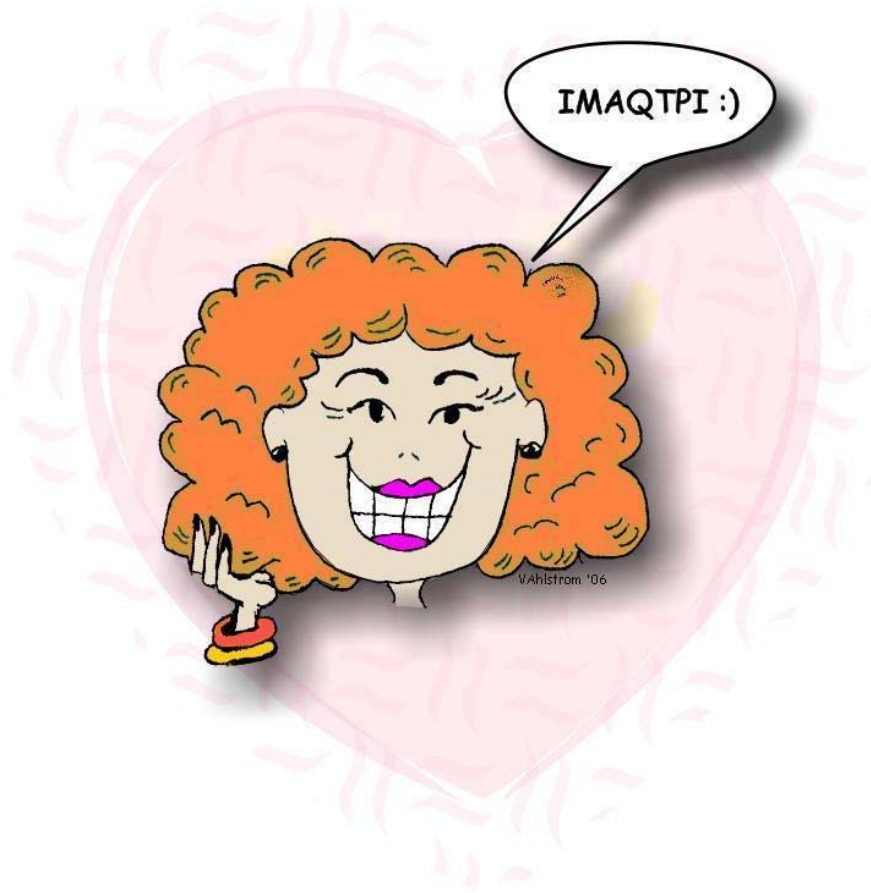


Switch letters. Try picking a password that you can easily remember and replacing or switching the first letter or letters. For example, “MyPassword1,” which is very easy to guess, becomes “PyMassword1.” Similarly, your dog’s name and year of birth “Fido2004,” becomes “Qido2004” by replacing the first letter, “F,” with the first letter on the top left of the keyboard.

Interleave a word and symbols or two words. "P*a*s*s*w*o*r*d" is harder to hack than "Password" but still easy to remember, and "Keylock" as a password is much easier to hack than if you interleave the words KEY and lock: "lKoEcYk." This type of strategy is also useful for incrementing passwords. For example, you could start with P*a*s*s*w*o*r*d, and then change the * to another character by applying some rule, such as replacing the * with the next character to the left on the keyboard; making the new password "P&a&s&s&w&o&r&d." (We use the word Password for example only! Please use a different word than password if you try this technique!!!).



Be shifty. Pick a password or phrase that you can easily remember and hold down the shift key while typing the numbers; "2Bornot2B" becomes "@Bornot@B." If you want to get even more complex, you can replace the letter o with the number 0 to get "@B0rn0t@B".

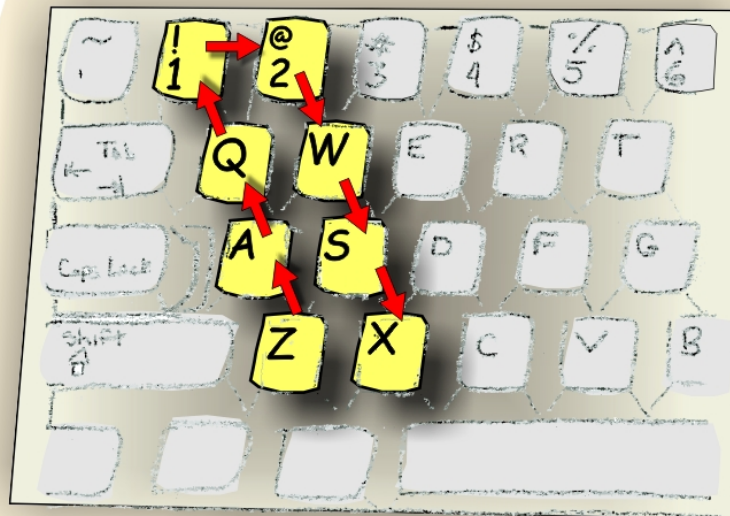


Emoticons. Emoticons are facial expressions made up by a series of keystrokes, such as a colon and parentheses as a smile :) or frown : (. Because they present a graphic image, they may be easier to remember than a meaningless character. For example, "Thisis2fun:)." These can be combined with other strategies, such as texting language, to create very complex but memorable passwords, such as lmaQTPi:) (I am a cutie pie smile face) or w/oUIMblu:((without you I am blue sad face).



If you know a foreign language (or even pig latin), try using words in that language in combination with the other password techniques. This interferes with hacker techniques that use dictionaries and the frequencies of words to guess passwords. For example, "1lgpayAtinlay" is harder to hack than "1PigLatin."

Instead of using a memorable word for your password, you can use a physical pattern on the keyboard to create a pattern. For example, if you start at the bottom left of the keyboard (pressing the shift key), move up, over, and then move down again (pressing the shift key again), you have “Zaq12wsX,” a password that would be hard to hack but would be easy to remember by applying a simple rule.



ZAQ12WSX



Replacing words or syllables with numbers and symbols or abbreviations in your passwords can help create memorable passwords that are difficult to guess.

This type of code is often used in text messaging and on vanity license plates. Some examples of replacing words with single letters include replacing *be* with *b*, *see* with *c*, *are* with *r*, *you* with *u*, and *why* with *y*. Removing vowels from a word also makes it memorable but harder to guess (between = btwn). Similarly, digits and symbols can be used to replace words or syllables: replace *ate* with *8* (great = gr8 or ate = 8); *to*, *two*, or *to* with *2*; *for* or *fore* with *4* (before = b4); and *at* with *@* (that = th@).

This could result in a complex, yet memorable passwords or passphrases, such as “Every1nosth@URgr8”¹, “ImDaB0\$\$0U”² or even U+Me=BFF(2tru)³.

¹Everyone knows that you are great ²I am the boss of you ³You and me equal Best Friends forever too true