

## Password Tips

The College of Arts and Sciences technology support services at Western Michigan University offers the following tips to choose a good password.

Since very few systems have support for one-time tokens (dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. If a malicious user can get hold of or 'crack' your password, they can access the system with your identity and access rights.

## Password Composition

Passwords should contain three of the four character types:

- **Uppercase letters:** A-Z
- **Lowercase letters:** a-z
- **Numbers:** 0-9
- **Symbols:** ~`!@#\$%^&\*()\_+={[]| |:;'"<,>.?/

Do not use all letters or all numbers and do not use a dictionary word in any language or a permutation of such. Avoid using common words such as "Western" or "Bronco," your name, account name, common names of people or places, technical jargon, repeating sequences, and keyboard sequences. Do not base your password on any items of personal information such as your name, social security number, birthday, pet names, or family member, and do not use your account name as a password. Do not use computer terms, names, commands, sites, or company's software titles, and do not use word or number patterns like abcdefg, qazxsw, qwerty, or zxcvbn.

## Creating Strong Passwords

- **Use random, pronounceable syllables** to make up words that are easy to remember.
- **Use acronyms** for unusual phrases that you invent (e.g., "WCMPE120D" for "why change my password every 120 days" or "Tbontbtitq" for "To be or not to be that is the question" then substitute characters).

## Character Substitution

Character substitution is where you take a lowercase dictionary word and substitute in special characters, numbers, and uppercase letters to make them more complex. Examples of common substitutions are:

- \$, S or 5 for s
- 1, l or ! for i
- @ or A for a
- 7 or T for t
- 3 or E for e
- 9, G or 6 for g
- 0 or O for o
- 8 or B for b

“Tbontbtitq” for “To be or not to be that is the question” would become “7b0n7B7!7?”

### **Combining Words**

Make two separate words into one longer password. You will also need to do character substitution to ensure that the password meets complexity requirements.

#### **Examples:**

- internet explorer - 1nt3rN3TeXp70r3R
- happy days - hapPyDaY\$?
- good boy - 60odB0y!

### **Inserting Codes or Words**

Substitute codes or words into other words (insert numbers between the letters of the original word).

#### **Examples:**

- Internet with numbers doubling (e.g., 1,2,4,8,16 - I1n2T3e4R8n16E32t!)
- Today my favorite color is orange - t0oRdaaNyGe
- John’s favorite football team is the Tigers - Jt0iHgN3r\$

### **Phrases with Character Substitution**

Create a password from phrases with character substitution. Phrases can be statements, locations, lines from books, movies, etc.

#### **Examples:**

- The next generation is you. First and last letter from each word = Tentgnisyu - 73n79N!\$yU!

- 45 main street - First 2 letters in word with a number between. First letter of each word in capitals - Fo1Fi2Ma3St4 or Fo1F!2M@3St4
- I drive a holden commodore now - First letter of each word with the characters of my license plate between (assume license plate is ABC 123) = iAdBaCh1c2n3 or !AdB@Ch1c2n3!

### **Protecting Your Password**

Do not use the same password for Western Michigan University accounts as for non-Western Michigan University accounts (i.e., personal ISP accounts, brokerage accounts, benefit accounts). If one account password is compromised, all accounts may be compromised. Do not share your University password(s) with anyone, including administrative assistants, supervisors, secretaries, or co-workers. All passwords are to be treated as sensitive, confidential Western Michigan University information.

### **To Better Protect Your Passwords, Don't:**

- Reveal your password over the phone to anyone, including your computer support personnel. Support personnel should never initiate a call requesting a password.
- Talk about your password around others.
- Reveal a password on questionnaires.
- Share your password with co-workers while on vacation.
- Use the remember password feature on applications (e.g., Netscape Messenger, Outlook, Outlook Express, Eudora).
- Write passwords down or store them anywhere near your computer.
- Store passwords in a file on any computer system (including cell phones) without using strong encryption.

If you suspect your account or password has been compromised, report the event to the appropriate system administrator and the University information security administrator and change your password immediately.

If someone demands your password, refer them to your system administrator or the University security administrator in the Office of Information Technology.