

## PROTECTING YOURSELF AGAINST PASSWORD LOSS

- ✓ DO NOT record your password on a post-it note stuck to your monitor or slid under your keyboard
- ✓ DO NOT use password-saving features, such as Microsoft's Auto Complete feature
- ✓ Do use a password-protected screen saver if you leave your computer, even for a few minutes
- ✓ DO Log off your computer at the end of the day

**If you think your password has been compromised, change it immediately**

## WRITING DOWN YOUR PASSWORD

Passwords should never be written down. Writing down a password increases the risk of it falling into the wrong hands. However, sometimes it is difficult to remember a complex password. If you must write down your password make sure it is stored in a secure place

White boards, sticky notes on your monitor, or hidden under your keyboard or mouse pad are not considered secure. Passwords should never be written down with your username.

### LINKS

**ITS Security Home Page**  
[http:// security.uwo.ca](http://security.uwo.ca)

Has Information on:  
Personal Computer Account  
Changing your Password  
Email help  
Antivirus Home Page  
Good Security Practices  
Acceptable Use Policy  
Reporting Violations  
Internet Safety

**P  
a  
s  
s  
w  
o  
r  
d  
s**

# Information Security



September 2004

**TREAT YOUR PASSWORD LIKE  
YOUR TOOTHBRUSH!**



## PASSWORD SECURITY

---

Passwords are a vital aspect of computer security. They are the defensive frontline that provides protection for your user account. A poorly chosen password is a weak frontline that can result in the theft of your user account! A stolen user account could then be used fraudulently on resources within the University. All UWO faculty, students, and staff (including contractors and vendors with access to UWO systems) are responsible for ensuring their accounts are protected by secure passwords.

## WHY WOULD I CARE ABOUT PASSWORD SECURITY?

---

Your unique name, or username, allows you to access the resources and services associated with the University of Western Ontario's network. Every time you connect to that network, you are challenged for a string of characters, known as your password, for validation purposes. If someone else has your password, they can assume your electronic identity. This means, this individual could have full access to your files, your e-mail, personal information, and more! The intruder could modify or destroy your files, send threats via e-mail in your name, or subscribe to unwanted services for which you would have to pay. In short, an insecure password can easily cause havoc in your life!



## PASSWORD RULES

---

- ✘ Passwords should not be shared or written down.
- ✘ Treat your password like your toothbrush and don't give it away or loan it to someone else to use!
- ✘ Passwords should not be a word in a dictionary, even a foreign dictionary.
- ✘ Passwords should not contain any form of your name or user-name.
- ✘ Don't use passwords like "password", "guest", "user", or "admin".
- ✘ Don't use personal information, like names of family members or pets, your date of birth, social insurance number, or any other similar information as part of a password. This information may be public, so you should not use it in a password.
- ✘ Don't use common words or acronyms even if they are spelled backwards.

## WHAT IS A STRONG PASSWORD?

---

- ✓ It is 8 characters long, a mixture of upper and lower case letters, punctuation and numeric characters
- ✓ It is changed every three to six months like your toothbrush
- ✓ It is confidential
- ✓ It is original, like you!



## HOW TO REMEMBER COMPLEX PASSWORDS

---

It is possible to construct a password that is strong and easy to remember. The following are provided as examples only and should not be used; create your own password unique and memorable to yourself.

- ✓ Creating a "pass phrase" is one way that helps to memorize a complex password. An example of a valid and secure pass phrase might be "Tqbf^0t1D" which is based its on the old typing practice sentence "The Quick Brown Fox Jumped Over the Lazy Dog!" Substituting numeric or special characters adds to the complexity of the password making it much more difficult to crack.



- ✓ Use lines from a childhood verse:  
Verse Line: Yankee Doodle went to town  
Password: Ydw2#twm
- ✓ Foods disliked during childhood:  
Food: rice and raisin pudding  
Password: r1c&ra1P
- ✓ My license plate is "880 PTW". That's not an acceptable password; hackers know that people may use their license plate as a password so it's very easy to scan for passwords that are license plates. Try mixing it up a bit "88oh-PtW" is acceptable and is such a minor variation that you ought to be able to remember it.