



IT Security Tips

Password Rules

- Must contain at least eight (8) characters
- Passwords expire every 180 days
- Five unsuccessful login attempts will lock the account for 15 minutes
- Cannot use any of your previous 24 passwords
- Must include three of the four requirements
 - capital letter
 - lower case letter
 - number
 - special character (@,#,\$,%,&,*+,!,)

Password Tips

Use a passphrase. Rather than trying to remember a complex password, think of a memorable phrase and use the first letter of each word to compose your password.

Example:

I went to Lowell High School and graduated in 2010!

Passphrase: IwtLHSag2010!

Add punctuation and numbers to meet password requirements.

Don't share your password or leave it where others can find it. You'll risk giving access to all your personal data.

Never send your password via email! Disregard any emails asking you to verify your password.

UML IT WILL NEVER REQUEST YOUR PASSWORD VIA EMAIL!

Passwords can be changed by visiting <http://password.uml.edu>



Best Practices

Set your anti-virus software to update daily and scan your PC for viruses daily.

McAfee is available for students, faculty and staff.

Visit <http://www.uml.edu/it/shared/software/McAfee87i.exe> to download.

You'll need to supply your UML email address and password for access.

Securely backup your data. Faculty/staff should use secure network fileshares. Students should consider external USB drives to store non-sensitive data.

Remember to log out of ISIS and email when done.

Do not click on links in emails sent by strangers.

Respond immediately to potential security threats by contacting the Help Desk at x4357 or emailing itsecurity@uml.edu.

Ensure Windows is configured to update automatically.

Use a password-protected screen-saver.

Run anti-spyware software periodically. IT Security recommends MalwareBytes.

Downloading copyrighted material is illegal and UML IT will suspend Internet access upon receiving DMCA notices!

NEVER EMAIL YOUR PASSWORD TO ANYBODY!

Tips for Removing a Virus or Spyware

Take the following steps to help clean up your PC. If you're not sure about how to complete any of the steps outlined, Google can be your friend!

Delete all temporary files. Right click on your C drive, click Properties and do a disk cleanup.

Make sure your anti-virus is installed and up to date. McAfee is free on campus.

Install MalwareBytes. Visit www.malwarebytes.org for more info.

If your Internet access is affected, copy McAfee and MalwareBytes onto a USB drive from a working PC.

Disable System Restore.

Reboot into Safe Mode. Press F8 just before the Windows Splash Screen. Timing is everything!

Run a full anti-virus and MalwareBytes scan and delete all infected files.

Reboot. In most cases, the steps outlined should clean up all but the most serious infections.

Get your FREE McAfee Anti-Virus software!
Call the Help Desk or download it from the web.
Help Desk: x4357