

Information Services

TOP FIVE THINGS TO REMEMBER

Secure your desktop and account!

- Always lock your workstation when stepping out of your office.
- Remind your students to **LOGOUT** of Windows® when finished using any workstations here on campus.
- **NEVER** write your passwords down on a **Post-It**® or piece of paper and leave out in the open.
- Also, you should always secure USB Flash/Thumb drives before leaving a classroom and/or office.



Change your password!

MAKE IT SECURE & UNIQUE

- Passwords should be at least 8 characters long.
- Should contain CaSe ChAnGes
- Should contain numbers and symbols: P@\$\$w0rD

USE A PASSWORD GENERATOR

Check out:

<http://passwordsgenerator.net/>



Beware of PHISHING

- Information Services will **NEVER** ask you to send your password to us in an e-mail.
- We will not contact you regarding E-mail Quota's via e-mail.
- If in doubt always send suspect e-mail to:
helpdesk@mctc.edu





Ransomware

–A form of malware that covertly installs itself on a computer. The malware then either locks the system or encrypts the computers files, both cases then demand payment to unlock them.

The best defense against ransomware is to always have an updated backup of your files, this allows restoration of the computer to before it was infected.

One should also not download/install unknown programs or files as these may be infected.



- **BitTorrent** – A protocol for peer-to-peer file sharing which is used to distribute data over the internet. This is one of the most common protocols for transferring large files.
- BitTorrent does have many inherent dangers due to the unknown nature of the files. Many of the files contain malware and can open up PCs to be vulnerable to outside attacks. Many torrents are also of copyrighted material, this can lead to legal troubles if movies, music, or software are illegally downloaded.