Cyber Security Do’s & Don’ts

DO’S –

– Create strong passwords that are at least eight characters long, and including at least a numerical value and a symbol, such as #, to foil password-cracking software. Avoid common words, and never disclose a password online.

– Change your password every ninety days.

– Perform regular backups of important data.

– Create a password for your files in order to protect file sharing activities.

– Physically secure your laptop

– Delete any message that refers to groups or organizations that you are not a part of.

– Download and install software only from online sources you trust.

– Never click on a link from an untrusted source.

– Close windows containing pop-up ads or unexpected warnings by clicking on the ”X” button in the upper most right hand corner of that window, not by clicking within the window.

– Use antivirus software, and update it on a regular basis to recognize the latest threats. Heed ITR security alerts to download antidotes for newly circulating viruses and worms.

– Regularly update your operating system, Web browser, and other major software, using the manufacturers’ update features, preferably using the auto update functionality.

– Set Windows or Mac updates to auto-download.

– Save attachments to disk before opening them. McAfee “Auto-Protect” will automatically scan your attachments if you save them to disk.

DONT'S –

– Never write down your password. Especially on a Post-It note stuck to your computer!

– Never give out your password to anyone, whether you know them or not.

– Never select the “Remember My Password” option. Many applications do not store them securely.

– Never purchase anything promoted in a spam message. Even if the offer isn't a scam, you are only helping to finance and encourage spam.

– Please refrain from opening an e-mail attachment, even from someone you know well, unless you were expecting it.

– Avoid creating common passwords such as your name, social security, UNI, etcetera.

– Do not leave your laptop unattended, even for a few minutes.

– Never reply to e-mail(s) requesting financial or personal information.

– Avoid opening e-mail(s) or e-mail attachments from an unknown sender.

– Please refrain from clicking on the close button within pop-up ads.

– Under no circumstances should you install or use pirated copies of software.

– Do not install P2P file sharing programs which can illegally download copyrighted material.

– Never set your e-mail program to “auto-open” attachments.