BASIC SECURITY PRACTICES

As our world becomes increasingly digital, we need everyone to pitch in to help protect our University’s resources. By following a few simple steps and developing good security habits, you can minimize opportunities to inadvertently expose sensitive data or information.

What is sensitive data? “Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.” For example: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, government passport number, employer or taxpayer identification number, unique electronic identification number or a routing code.

Review Acceptable Use Policy: www.stritch.edu/policy

Good habit: Do not store sensitive information such as student records, credit card numbers or social security numbers on your computer unless it is absolutely required by your job. If required, contact the Office of Information Technology (OIT) for assistance with properly safeguarding the information. Do not share sensitive data via email at any time, and be particularly careful on the internet to make sure a site is secure by looking for a url that begins with ‘https’ or look for a logo such as:

Email: Email, chats, instant messengers, Facebook, etc. are not secure and should never be used to send any information you do not want exposed to the public. Social networking sites are playgrounds for criminals. Limit what information you share. Avoid email with embedded links and attachments from sources you don’t recognize. Many email messages and viruses look like valid messages. Be aware of phishing which is a high-tech scam that either asks for your credit card, bank account, passwords, or social security numbers OR leads you to a web site that looks official and asks for the same type of information.

Good habit: If you can’t post the information comfortably on the closest billboard, think before sending it via email. If you don’t recognize the sender, delete it—they will send the message again if it is real or call instead.

Passwords: A password is the first line of defense. Choose ‘strong’ passwords with at least eight characters, using a combination of numbers, upper and lowercase letters and at least one special character (!@^%*). Remember to change your passwords frequently. Remember, OIT will never request your log in, password, birth date, etc. via email.

Good habit: Do not share your password with others and do not post it in an obvious place (like a post it on the computer or in the top drawer of your desk).

Back up your work: You have just spent a significant portion of your time creating a lesson plan, lecture notes, preparing a grant, writing an article.....remember to save it and go one step further – back up all of your personal work on a weekly basis to a CD or other external media.

Good habit: Set aside a portion of time each Friday to back up your work and clean up your email. Once you have your data backed up, be sure to test it to ensure it can be retrieved. Store your back ups in a safe location.
Love your computer: Log off or use the keyboard locking function when stepping away from your computer. If you don’t, others can easily access your email or other documents. If you are using a laptop, run a virus check before connecting it to the Stritch network. Make sure your computer is always up to date with security patches and virus protection.

Good habit: Learn how to run the virus check if you have a laptop—if you need help, call x4600. If your computer starts acting ‘funny’ – call before trying to fix it yourself unless you have good computer troubleshooting and diagnostic skills.

and finally…

Shred your documents: Remember to shred sensitive documents in the office and at home. People with a malicious intent will search through trash to get what they want.

Good habit: Share your good habits with others and Stay safe!!!