Be cyber safe when working remotely

The Office of Information Technology (OIT) wants to remind staff who are working remotely to be diligent in their cybersecurity precautions. Bad actors are aware that people are both distracted, and extremely vulnerable to emails, phone calls, and texts offering COVID-19 information and they are taking advantage when opportunity presents itself.

Here is information that you may not know about protections that travel with you from SIU.

- SIUC uses Office365, which is cloud-based, so using SIU email on or off campus is essentially the same. Email that is sent within the @siu.edu domain, SIU staff to SIU staff, is secure. Office365 requires a secure login from on campus or remotely. The primary security issues are with access and vulnerability to phishing, social engineering, forwarding emails, shoulder surfing, and compromised accounts. For these reasons, OIT discourages and recommends that **sensitive information not be sent via email**. Our Data Loss Prevention (DLP) tool runs constantly and detects sensitive information in emails and alerts staff who are sharing it via email. To send sensitive information safely, use MOVEit to send confidential information. Files can also be shared securely using OneDrive or Teams.

- SIU protects campus resources to remote access via the Virtual Private Network (VPN). The VPN encrypts communication between remote workers' machines and the campus. Continue to store your daily work on an SIU server, if you have access to it via VPN. Other safe options are OneDrive or Teams (which do not require VPN access). Saving to any of these locations provides a secure backup of your work.

- SIU is protected by a tool called Proofpoint, which vets suspicious URLs, and eliminates malicious email to protect employees. Nonetheless, users must still be cautious about opening attachments, clicking links, or interacting with unsolicited email.

- SIU protections are not in place if you send emails or files using your personal email account. This is tempting, when working from a personal (versus a SIU) device. Conducting SIU business via personal email is a violation of SIU policy and leaves you, the SIU network, your colleagues, and University assets at risk.

Here are precautions you should take when using personal devices (including a home network)

- Patch your personal devices. Out of date software is a security risk. Software and app providers distribute patches regularly—apply them to your computers and phones. **NOTE:** Illegal/pirated software cannot be patched; remove illegal software from your devices.

- Do not save sensitive information to your personal device at home. SIU does not have appropriate toolsets in place to manage personal devices used remotely.

- Secure your home network. This is a basic precaution, but there are people living remotely who leave their in-home network open. Lock your network down with a password!

- Log out of browsers and apps used to access online content, and remove saved login credentials (turn off cookies and autofill if possible).

- Change old passwords, use different passwords for SIU access and personal accounts. Consider using a password manager if you don't use one already.

- Delete apps you no longer use.

OIT has compiled a list of FAQs and resources regarding using technology from remote locations. You can also call SalukiTech at (618) 453-5155, or contact them at salukitech@siu.edu if you need assistance; they will work with you as able, but there may be a limit to their knowledge and ability to help with personal equipment and software.