CITE
CENTER FOR INFORMATION TECHNOLOGY EXCELLENCE

The following guidance is provided by PVAMU to educate students on how to secure themselves and keep their information safe.

Remote Learning Guidance for Students

Video Conferencing

- Only use PVAMU approved software & tools to host, initiate & schedule meetings.
- Be wary of links sent by unfamiliar address, & never click on a link to a meeting sent by a suspicious sender.
- Do not share a link to a meeting on an unrestricted, publicly available or social media post.
- Do not provide links to meetings, meeting IDs, or meeting passwords to anyone outside of PVAMU.
- Do not share passwords with anyone.
- Do not share student credentials or links with strangers who may use them to disrupt class or steal information.
- Check to see if the meeting came from a known professor or other PVAMU employee.
- Hover the mouse cursor over links in an email to ensure the domain is legitimate.

Securing a Personal Device/Environment

If using a personal device for work from home:

- Require a strong password to log into the device.
- Close all other, non-school related windows & applications before & while using the personal equipment for work.
- Keep the operating systems & all relevant applications up-to-date, & fully patched.
- Turn on automatic patching & run antivirus software.
- Check & update your home network.
- Change default network settings & use complex passwords.
- Change the generic name for your home Wi-Fi network to avoid identifying who it belongs to or the equipment manufacturer.

Protecting Sensitive Data/Information

- Consider the sensitivity of data before exposing it (via screen share or upload) to video conferences.
- When sharing a screen, ensure only information that needs to be shared is visible.
- Use common sense - do not discuss content you would not discuss over the telephone.
- When having sensitive discussions, ensure all attendees are the intended participants.
- Ensure your visual & audio surroundings are secure.
- Confirm that roommates or family are not within earshot of sensitive conversations.
- Consider using headphones to avoid eavesdroppers.
- Use backgrounds or blur options in video calls/meetings.
- Turn off home security cameras & virtual assistants to avoid inadvertently recording sensitive information.