9 TIPS TO
Stay Secure While Working Remotely

Lock down your home wireless network
Create a complex router password and limit access.

Secure your work devices
Use strong passwords or passcodes, and lock your laptop screen or put your device to sleep when not in use.
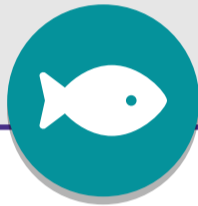
Control use of removable media
Do not allow family members or guests to plug personal devices or accessories into your work devices.

Protect institutional data
Keep institutional data exclusively on your work devices. Avoid transferring work-related files to personal devices.

Beware of phishing attempts
Do not click links or attachments from unknown senders, and be cautious about what you download.

Separate the personal and professional
Do not use personal computers or devices to conduct institutional work, and vice versa.

Only use authorized software
Never download unauthorized software on your work devices, and don't tamper with or disable authorized software or applications.

Share files securely
Always use email encryption or your institution's secure file-sharing services.

Report security concerns ASAP
If you see anything suspicious, contact your institution's infosec or IT team immediately.

ellucian.
www.ellucian.com