Dear GSU Community,

As we continue to observe Information Security Awareness Month, I want to draw attention to our mobile devices. These gadgets, whether smartphones or tablets, have become indispensable to our daily lives.

Keep Mobile Devices Updated
Dismissing notifications to update your device's software is easy, however these updates often contain patches for known vulnerabilities. Make it a habit to keep your devices updated with the latest software versions.

Dangers of Downloading from Unverified Sources
It's crucial to download apps only from reputable sources. Malicious apps can compromise your device's security and steal personal data. Always double-check app permissions and reviews before downloading.

The Rise of Malicious QR Codes
Unknown or suspicious QR codes can lead you to malicious websites or download harmful software. Always ensure the legitimacy of a QR code before scanning, especially if its source is unknown.

Using Strong Passcodes
A passcode is an effective barrier against unauthorized access. Follow these guidelines to ensure optimal security:

- Opt for a passcode that's at least six digits long. Alphanumeric combinations, where possible, add extra layers of security.
- Steer clear of easily guessable sequences like "123456" or "abcdef."
- Update your passcode periodically and avoid sharing it. Even temporary access can lead to vulnerabilities.

Remote Wipe Capabilities
For College-Owned Devices:
Should your college-provided device get lost or compromised, be aware that the university can remotely wipe it to protect sensitive data. This action ensures our collective digital safety.

For Personal Devices:
Apple Devices: The "Find My" feature through iCloud allows you to track, lock, or erase your device remotely. Ensure its enabled and familiarize yourself with its functions.
Android Devices: Android's "Find My Device" service offers similar protective measures. Regularly check its activation status on your device.

Additional Best Practices
Utilize biometric features like fingerprint or facial recognition for added security. Also, back up your device data securely and avoid using public Wi-Fi networks without a VPN, to prevent exposing your data.

Stay vigilant, stay informed, and remember - our knowledge and practices are our strongest assets in digital security.

Warm regards,
Jay Ellis
CIO

Grambling State University
Information Technology Center
Jacob T Stewart Hall |Room 139
403 Main Street |Box 4220 |Grambling, LA 71245
itc@gram.edu