Mobile/Smart Phone Security Do’s and Don’ts

Our phones now contain more computing power than most computers we used mere years ago. This month, our CISOs share some tips on phone and mobile device security.

Dos
- Enable security access.
- ONLY give your number out to people you know and trust.
- Use caller ID to block names and numbers of individuals you do not want to contact you.
- Delete emails that contain confidential or internal use information from your phone.
- If your phone is lost or stolen, report it to your local police station, your service provider, and campus IT immediately.
- If your phone is stolen, also use a remote wipe feature or location services.
- Treat your mobile device like you treat your wallet or purse.

Don’ts
- Do NOT store confidential information on the phone, such as PIN numbers and credit card numbers.
- Be aware of emails on your mobile or smart phone that may contain confidential information.
- Do NOT take pictures or videos of anyone with your phone, or allow them to be taken of you, without permission.
- Never reply to text messages from people you don’t know and avoid in-person meetings with someone you know only through text messaging.
- Beware of the GPS location tracking feature in your mobile device.

To access current and past IT Risk Bulletins, go to the “Office of Risk Management” page on www.uasystem.ua.edu.