Mobile/Smart Phone Security

Things to Do

The following are safe practices when using your mobile device:

• 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
• Enable security access (alpha/numeric if possible) to unlock the screen and turn on the option to reset the phone to factory settings if the security access is missed too many times
• Delete e-mails that contain UA confidential or internal use only information
• If your phone is lost or stolen, report it to your local police station and your service provider immediately
• Treat your mobile device like you treat your wallet or purse
Mobile/Smart Phone Security

Things Not to Do

Take the following precautions when using your mobile or smart phone:

• Do NOT store confidential information on the phone, such as PIN numbers and credit card numbers
• Be aware of e-mails on your mobile or smart phone that may contain UA confidential information
• Do NOT share anyone’s number without asking them first
• 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