WHY IT MATTERS	
Data is your most valuable digital asset. The pictures, documents, and files you create, use, and, rely upon everyday are difficult or impossible to replace if damaged or deleted. Personal information can cause significant harm if stolen or disclosed. Protecting your data involves the ability to backup data (protect from loss), verify the integrity of the data (protection from alteration), and maintain confidentiality (protect from disclosure). Advanced encryption techniques provide the maximum protection to prevent data theft and improper disclosure. Encrypting data makes it practically impossible to access data without proper authorization.	**A** **DATA** **WARNING:** The incorrect use of encryption techniques can cause permanent data loss. **Use with extreme caution.**

WHAT TO KNOW	
Encryption protects sensitive data by transforming the data into an unreadable scrambled form. When you authenticate using a PIN, password, pattern or key, the data is decrypted, returning it to the original form and making it understandable to the authorized user. Encryption protects the confidentiality and integrity of data. Encryption can be used for both data 'in transit', such as when it is being transferred from one system to another over a network, or stored data 'at rest' on a DVD, USB thumb drive, or other storage device.	
Encryption definition – Webopedia Encryption definition – Encyclopedia.com	http://www.webopedia.com/TERM/E/encryption.html http://www.encyclopedia.com/science-and-technology/mathematics/mathematics/encryption

WHAT TO DO	
Recognize proper SSL encryption - The complexities of the SSL protocol remain invisible to most users. Browsers provide users with a key indicator, the padlock icon, to let them know they are protected by an SSL encrypted session. Clicking on the lock icon displays details about the SSL Certificate. Learn to understand this information and recognize a valid certificate.	
"What is SSL?" - SSL.com	https://info.ssl.com/article.aspx?id=10241
Use file encryption - For especially sensitive files consider using a file encryption application, either a native version or 3rd party application. You can encrypt individual files or create encrypted containers for multiple files.	
Open source encryption – Veracrypt	https://veracrypt.codeplex.com/

HOW TO DO IT	
Android - Native Encryption	**iOS** - Native Encryption = FileVault
https://source.android.com/security/encryption/#full-disk	https://support.apple.com/en-us/HT204837
WARNING: Changes to device and application settings can have unintended consequences and may interfere with normal operation. Improper use of encryption and authentication can cause a loss of data and prevent access. Please do not attempt to apply any guidance that exceeds your level of knowledge and familiarity with your device or application. All guidance is provided "as-is" from referenced sources. User assumes responsibility for any changes made to their device and/or applications.	