It's YOUR Info. Keep it that Way.

Personal information is like money. Value it. Protect it.

Your mobile devices contain significant information about you. Your friends. Your family. Think about the contact numbers, photos and so much more stored on your device.

- ✓ Back up your files – don't keep the only copy on your mobile device.
- ✓ Keep your device with you – mobile devices are so portable that one of the biggest threats is loss or theft.
- ✓ Think twice – be thoughtful about the information stored on your device and how it may be collected through apps you download and websites you visit.
- ✓ Erase your mobile device before disposing of it whether you are donating, reselling or recycling it. Check the device's user guide for instructions on erasing data.
- ✓ Own your Online Presence – use security and privacy settings on websites and apps to manage what is shared about you and who sees it.

Additional Help & Info

Support Center

The Information Technology Services Support Center offers services to help you set up your mobile devices and make sure they are secure.

Contact them at 828-262-TECH (8324) option 2 or stop by the Support Center.

They are located on the bottom floor of Anne Belk Hall directly across from Rankin Science.

Support hours for the Fall 2015 Semester are:

- Monday – Thursday, 8 AM – 11 PM
- Friday, 8 AM – 5 PM
- Sunday, 1 PM – 11 PM

Summary

- ✓ Long passwords are good
- ✓ Change your passwords regularly
- ✓ Be aware of where you are
- ✓ Be aware of where your device is
- ✓ Update your software

http://security.appstate.edu

Follow us on Twitter @ appinfosec

Appalachian State University
BOONE, NORTH CAROLINA 28608
Information Technology Services
Office of Information Security

Information Security

Mobile Devices

Securing Your Mobile Device

Your smartphone. Your tablet. Your laptop. These are all mobile devices and need to be protected. Here are a few simple tips to help keep them that way:

- ✓ Secure your devices – use strong passwords, passcodes, passphrases or other features such as touch identification to lock your devices.
- ✓ Encryption – enable it!
- ✓ Keep Security Software Current – having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.
- ✓ Delete apps you no longer use or no longer are of interest to you.
- ✓ Disable WiFi and Bluetooth when not in use. - Some stores, restaurants and other locations look for devices with WiFi or Bluetooth turned on to track your movements while you are within range.

Still Securing Your Mobile Device

- ✓ Limit Public WiFi usage – public wireless networks are not secure. What that means is anyone could potentially see what you are doing on your laptop, tablet or smartphone while connected to their network.
- ✓ Use VPN (virtual private network) for a more secure connection.
- ✓ Understand App Permissions – when you grant application access you are granting access to your personal information and access to perform functions on your device.
- ✓ KeePass – If you store passwords on your phone, protect them in a password vault like KeePass.
- ✓ Don't Know, Don't Answer – fraudulent text messages, call and voicemails are on the rise. If you received something from someone you don't know or it's from someone you know but looks suspicious, don't reply. Email and mobile requests for personal data or immediate action are almost always scams.

Securing Specific Mobile Platforms

You can install security apps that enable remote location and wiping. Some are installed such as Find My iPhone on Apple devices while others need to be downloaded. Downloading security apps for a Android or Windows Mobile device are generally safe provided the apps are from a legitimate app market such as Android Market or Google Play.

Security apps must be set up before the phone is lost or stolen.

Risks of rooting your phone:

- Your smartphone can become a brick or at least as useless as one.
- Your warranty will be void…immediately.
- Malware can easily breach your mobile security.