The Top Ten Ways to Secure Mobile Devices

BYOD = It’s Yours
– Your Device: Your Responsibility
– Your LIABILITY
– UTHSC cannot be responsible for how you handle PHI on your device

Mobile Devices are . . . MOBILE
✓ The FCC is setting up a national database to track REPORTED stolen phones
✓ Nearly half of all robberies in San Francisco this year are cell-phone related
  - Sunday, Oct. 21, The Commercial Appeal

Mobile users are more likely to click on dangerous/malicious links

Need-To-Know

Configure

• Enable:
  – Auto-lock
  – Remote wipe
  – Browser Security Settings
  – SSL Protection, if available
  – Your PHI transmission habits as protocols
  – Password protection with strong password
Your Secret Formula

Vlh10*2)

Vicki Is Happy 10*2)

(Middle Name, U/lc, day you adopted your pet, random symbols)

Passwords

No matter how strong they are, used ones eventually have to be thrown away

Passwords are like a toothbrush because:

You don’t Share them with anyone else!

② Connect ONLY to:

✓ Secure Networks
✓ Disable Wi-Fi and Bluetooth when not in use

① Configure

② Secure Connect/Disconnect

③ Update

✓ Frequently
✓ Often
✓ Whenever possible

Auto Update
1. Use Anti-Virus tools

- Easy to find
- Free
- Critical for Health Care Professionals

2. Secure Connect/Disconnect

3. Update Often

4. Use Anti-Virus tools

5. Encrypt PHI

Encrypt PHI in Word Documents

6. Use Digital Certificates

- A digital certificate allows a sender to email an encrypted message to the recipient.
- The recipient uses the digital certificate’s Public Key function to access the encrypted information.
- The digital certificate verifies the identity of the sender and allows only the receiver(s) with the Public Key to open the message.

Digital Certificates: C. A.

- Digital Certificates are obtained through Certificate Authority vendors.

Interested in a CA? Google it. (Some are free.)
Top Ten Ways to Secure Mobile Devices

1. Configure
2. Secure Connect/Disconnect
3. Update Often
4. Use Anti-Virus tools
5. Encrypt PHI
6. Use Digital Certificates
7. Prevent Theft/Enable Recovery
8. Sanitize/Delete/Dispose
9. Policies and Procedures
10. Keep track of your stuff

Prevent Theft/Enable Recovery

- Never leave your device unattended.
- Report lost or stolen devices
- Lock up your laptop/device
- Back up your data and leave your backup someplace safe!

Keep track of your stuff

- Use tracking and tracing software
  - Computrace
  - Lookout
  - Find iPhone (in OS)
  - STOP
- Use Smart Owner Smart Phone Protocols

Sanitize/Delete/Dispose

- Delete all stored information before donating, exchanging, or discarding a mobile device.

Policies and Procedures

- UTHSC website: access to policies, procedures, standards, guidelines, recommendations, technical information.
- Policies include FERPA, HIPAA, FISMA, HITECH, FIPS, NIST, & ARRA compliance, to name a few.
  - See www.uthsc.edu/its for compliance guidelines.
  - Ignorance is not a valid legal strategy.
Sophisticated Spoofing

Change is constant

Questions?

- UTHSC website
- Frank Davison, IT Security Office
  448-1260 / fdavison@uthsc.edu

First and Third Tuesdays
910 Madison
IT Awareness Table in Lobby

Sophisticated Spoofing

Remember these museum pieces?

Stay informed about the latest news about hacking, phishing, target phishing, spoofing.

Be wary of unknown links, phone numbers, or contact names.

Beyond Nigerian Princes

Stay in informed about the latest news about hacking, phishing, target phishing, spoofing.

Be wary of unknown links, phone numbers, or contact names.

Configure

Secure Connect/Disconnect

Update Often

Use Anti-Virus tools

Encrypt PHI

Use Digital Certificates

Prevent Theft/Enable Recovery

Sanitize/Delete Dispose

Policies and Procedures

Continuous Education

1. Configure
2. Secure Connect/Disconnect
3. Update Often
4. Use Anti-Virus tools
5. Encrypt PHI
6. Use Digital Certificates
7. Prevent Theft/Enable Recovery
8. Sanitize/Delete Dispose
9. Policies and Procedures
10. Continuous Education

Questions?

- UTHSC website
- Frank Davison, IT Security Office
  448-1260 / fdavison@uthsc.edu

First and Third Tuesdays
910 Madison
IT Awareness Table in Lobby