MeHI MassCyberCenter

Monthly Cyber Call

Mobile Device Universe

- Phone
  - IOS
  - Android
- Tablet
  - IOS
  - Android
- Watch
- IOT devices

Threats

- Vishing
- Smishing
- Malware
- Zero Day vulnerabilities
- N day Vulnerabilities
- Snooping/Attacker in the middle

Utilize setting to minimize Risk

- Device protection – anti-malware
- Screen lock
- Use Multifactor Authentication and biometrics
- Backup mobile devices
- Update software regularly
- Minimize bloatware
- Use trusted cables and chargers
- If corporate, implement a hardware lifecycle

Mitigate Risk through Avoidance

- Public WiFi
- Viligance clicking on links
- Avoid Jailbroken phones and untrusted app stores.

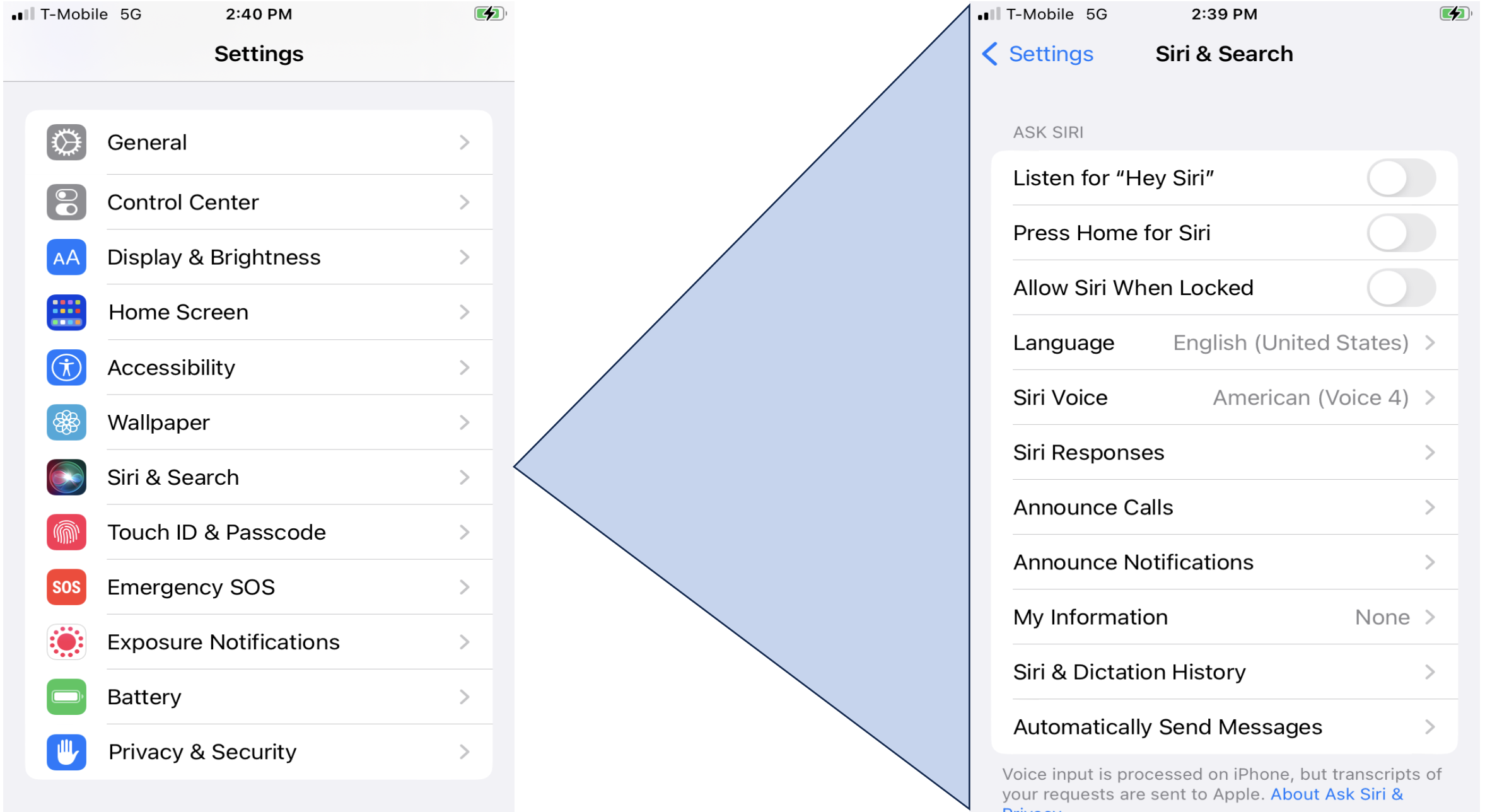
Acceptable Use Policy

- Delineate acceptable policies for work vs personal devices
  - Antivirus
  - Social media
  - Terms of use
  - Apps for work
- Network and password protocols for mobile devices
  - Guest network
  - Reporting lost or stolen devices
  - Password Sharing
  - Out of band communication

IOS Security

- Minimize Siri learning your actions
- Use only app store applications
- Screen lock
- Consider lockdown mode
- Manually forget your Wi-Fi connections

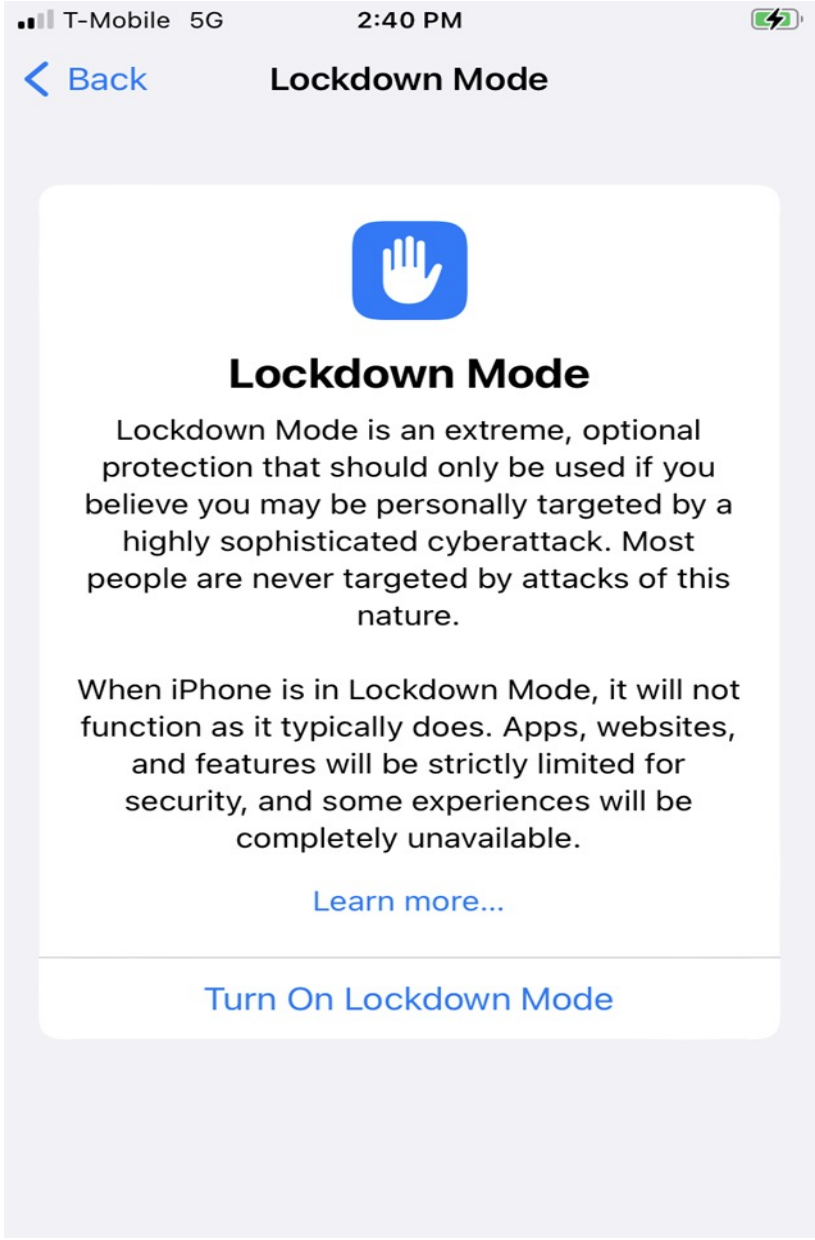
Siri and Search settings in each App



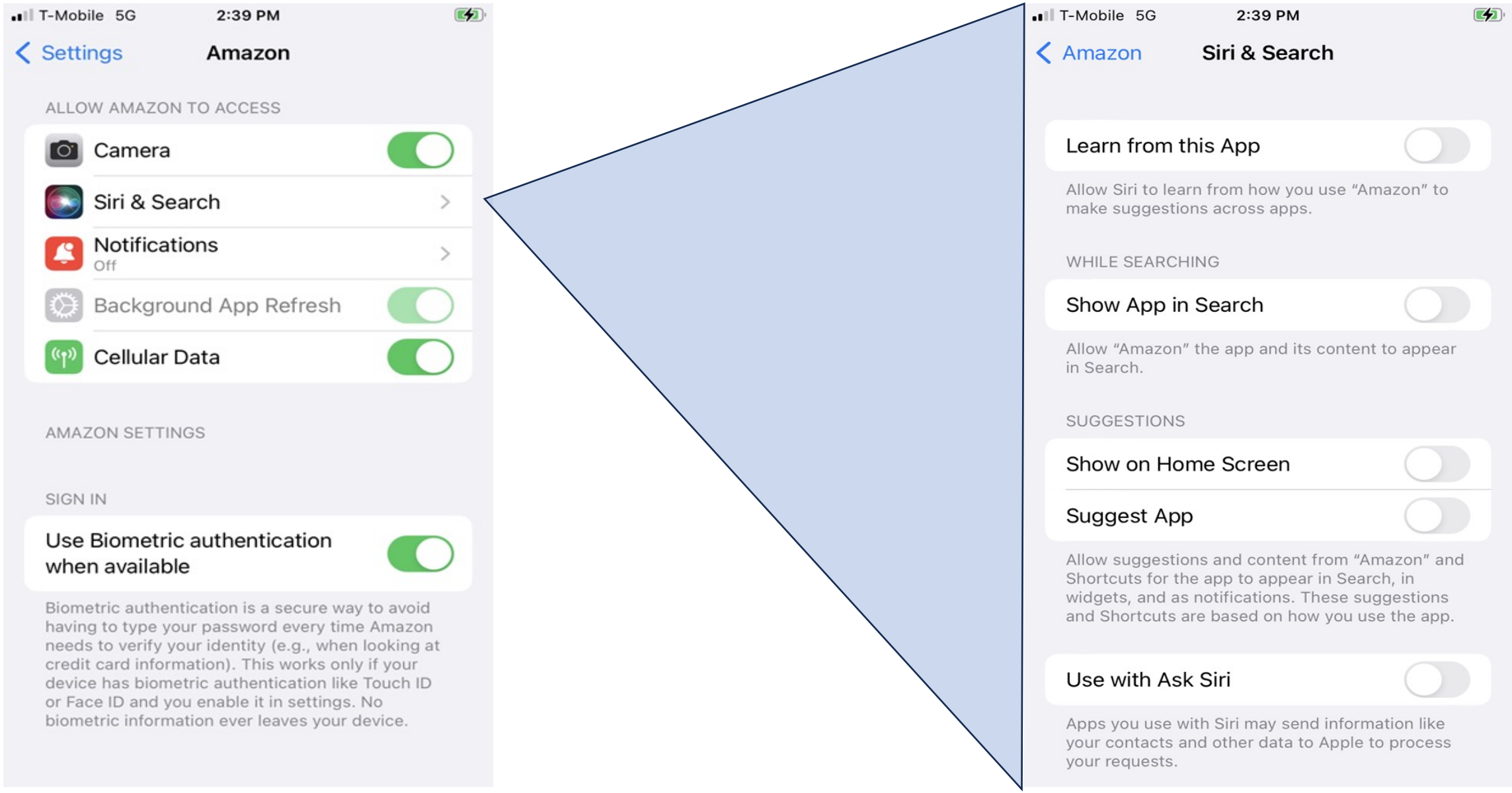
Siri and Search settings in each App

Lockdown Mode

- Protects against no-click attacks
- Executives and Security specialists
- Limits Containers from sharing data
- Can’t receive text message and add into app



Siri and Search settings in each App



Android Mobile Device Security Considerations

John Danahey
Managing Partner (Systems)
Digital Tech Partners
jdanahey@digitaltechpartners.com
339.204.5435

Android Operating Systems – Overview

1. Different Than Apple Products
2. Many Different Hardware Manufacturers
3. Many Different Components
4. Differing Terminologies

Android Operating Systems Security Features

1. Google Play Protect – Verifies that the app you are downloading or using on your phone has been inspected by Google and passes their “security” validation.

2. Find My Device – Being able to locate a lost or stolen device is important, being able to “de-identify” the device, and wipe the data remotely are critical to protecting information.

3. Device Encryption – Storing regulated data encrypted at rest and in transmission is required.

4. App Permissions – Verify which permissions are appropriate for the applications running on your device. Location services, microphone, and contact access permissions should be granted on a case-by-case basis.

Android Operating Systems Security Features

5. Lock Screen Controls – High security controls features include password, and biometrics (face and / or fingerprints)

6. Emergency Contacts – Medical, Emergency Contacts, and SOS Messages should be enabled in the settings that are appropriate for you. Medical and Emergency contacts are available when the phone is locked.

7. Biometric Authentication – As mentioned before enabling this feature allows for unique identification, not foolproof and better than just a PIN.

8. Lockdown Mode – A feature that can temporarily disable biometric or Smart Lock features so that the device can only be accessed by you.

Android Operating Systems Security Features

9. Guest Mode – Enabling guest mode allows you to restrict access to your personal information (photos, files, etc.) when allowing others to use your phone.

10. Smart Lock – Enables your phone and your Chrome browser to work together to minimize the number of times you need to authenticate to your device.

11. Two Factor Authentication – Enabling this feature allows for a higher level of security and is a best practice for accessing sensitive personal information to include ePHI.

12. Google Security Checkup – Logging into your Google account and launching the security checkup feature enables you to understand the “big picture”. It reviews your accounts, saved passwords, known breach information, and device status.

Android Operating Systems Security Features

13. Google Activity Controls – No pun intended, if you “google” this subject, you’ll learn what information is stored about your account, enable you to select what you want to retain or delete, and otherwise change the “defaults” that Google provides when you sign up for the service.

14. Enhanced Safe Browsing – Again by “googling” this feature you can control what is saved in Chrome and how to remove unwanted ads or malware.

15. Autofill – Enables the sharing of your personal information to applications including password management applications. This feature presents opportunities and risks and should be understood before enablement.

BYOD Considerations for eMR / ePHI:

1. Mobile Device Management
2. Wireless Networks
3. Anti-Malware / VPN
4. Suspicious Activity
5. Reporting / Escalation

MeHI
MASSACHUSETTS eHEALTH INSTITUTE
at the MassTech Collaborative

MassCyberCenter
at the MassTech Collaborative

DIGITAL TECH PARTNERS

Questions?