Smartphones/Tablets

iPhone/Android

Week 6

Data Usage, WiFi, Storage, Security

Data Usage

- Data Usage
  - The amount of data used in a billing cycle (typically one month)
- How mobile data works
  - Mobile data allows your phone to access the Internet
- What uses data?
  - Browsing the Internet
  - Downloading and running apps
  - Checking email
  - Playing games
  - Watching videos

Data Usage – Types of Users

- Light user – “I use it every now and then.”
  - In a month, you occasionally browse through the Internet and send the odd email. You might check your Facebook every so often. But you never upload, download or stream any media. You’re likely to use your Internet for more than an hour a day. Recommended data allowance: 500Mb/month
- Medium user – “I browse when I’m bored.”
  - You browse the Internet every day and check your Facebook, Twitter and emails regularly. You use a few apps each month and like to watch videos or download some songs every now and then. Recommended data allowance: 1Gb/month
- Heavy user – “I use it for entertainment and work.”
  - You regularly browse the Internet, check Facebook, Twitter and emails. You use a number of your favorite apps, watch videos and download music for your phone several times a week. Recommended data allowance: 2Gb/month

WiFi

- What is WiFi?
  - Wi-Fi is a type of short-area wireless networking. It is commonly used in homes and offices to create a network that can be accessed by computers, smartphones, game consoles, home theatre devices, and other gadgets. This allows these devices to access the Internet without needing a wired connection.
  - Just about every smartphone has wifi capabilities
  - Wi-Fi can improve your connection to use the Internet, text or even make phone calls in areas where the cell connection is weak or spotty.
  - Using Wi-Fi can save money because you are not using any of your data allotment

WiFi - Public

- Two Types of Public WiFi – Unsecured and Secured
- An unsecured network can be connected to within range and without any type of security feature like a password or login.
- A secured network requires a user to agree to legal terms, register an account, or type in a password before connecting to the network. It may also require a fee or store purchase to gain access to the password or network.

WiFi – Dos & Don’ts

- **Do** connect to secured public networks whenever possible. In the event that you’re unable to connect to a secured network, using an unsecured network would be permissible if the connection requires some sort of login or registration.
- **Don't** access personal bank accounts, or sensitive personal data, on unsecured public networks. Even secured networks can be risky. Use your best judgment if you must access these accounts on public Wi-Fi.

WiFi – Dos & Don’ts

- **Don't** leave your laptop, tablet, or smartphone unattended in a public place. Even if you’re working on a secure Wi-Fi network, that won’t stop someone from taking your property or sneaking a peek at your device.
- **Don't** shop online when using public Wi-Fi. Sure, shopping doesn’t seem like it involves sensitive data, but making purchases online requires personal information that could include bank account and retailer login credentials. Shopping isn’t something you want to do on an unsecured Wi-Fi network.

WiFi – Dos & Don’ts

- **Do** turn off automatic connectivity. Most smartphones, laptops, and tablets have automatic connectivity settings, which allow you to seamlessly connect from one hotspot to the next. This is a convenient feature, but it can also connect your devices to networks you ordinarily would not use. Keep these settings turned off, especially when you’re traveling to unfamiliar places.
- **Do** monitor your Bluetooth connectivity. Bluetooth in the home is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can pose a huge risk to your cybersecurity. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked down when you leave your home, office, or similar secured area.

Cloud / Storage

- **Cloud** for the Android, **iCloud** for the iPhone
  - simply a service that keeps all your devices in sync. In other words, you can share information between your devices (iPhone/Android, iPad/tablet, iTouch/music player and a computer). The information on each device is automatically updated to make sure the most current information is available on all devices.

Cloud Uses

- Examples of Cloud Uses
  - Web-based emails (Yahoo, Gmail)
  - Backup (Google Photos, iCloud)
  - Social Media Sites (Facebook, Instagram, Pinterest)
  - Web based software (Google Docs)

Cloud


Documents. View and edit the same document from all your devices.

Smartphone Security

- Do smartphones and tablets need security?
  - Yes
    - Viruses can also infect smartphones and tablets
    - Viruses can be introduced to these devices much like they can on a computer through malicious software, or malware
  - How does the malware get onto the devices?
    - Through third-party apps stores (stores other than the iPhone/iPad's App Store or the Android's Google Play Store)
    - Or through visiting websites

Tips to Help Protect your Device

1. **Install and use security software.** Any device that connects to the internet should have security software. A good security suite will have a multitude of features that can help protect your devices and your data from online risks you may not be aware of.
2. **Always install software updates.** No matter what the device, don't delay when it comes to updating your software. These updates often help to patch the latest security holes and software vulnerabilities. Oftentimes, when there is a software update, it can add to or enhance security settings and reset your current settings. As a result, you'll also want to review your security settings on each device and make adjustments as needed.
3. **Be aware of the apps you install.** Use discretion when installing apps. Only source them from legitimate app stores, such as Google Play and the Apple App Store, and read app reviews and privacy policies before installing.
4. **Lock your device.** Lock-screen security is the first line of defense against having your information accessed by anybody who has your device. In the event of loss or theft, you'll rest easier knowing that all your information isn't suddenly public.
5. **Watch out for smishing.** It's not just emails you have to watch out for these days. SMS phishing scams are another concern. Whether an email or a text, trust your instincts. If a message seems suspicious, treat it that way. Better to be safe than to put your device — and your information — at risk.

info obtained from Norton.com

Smartphone Security

- Different Security Apps
  - Norton Mobile (www.us.norton.com)
  - McAfee Mobile Security (www.mcafee.com)