Mobile Device Security

Securing Wireless Devices

Wi-Fi

Currently, that's WPA2 or Wi-Fi Protected Access Version 2.

This relies on the advanced encryption standard for its encryption algorithm, also known as AES.

Bluetooth

Well, by default, Bluetooth requires you to pair the device. And when you pair the device, the two devices will communicate via that shared link and give each other a shared link key. They use that key to encrypt their data.

Mobile Malware

1. Do not jailbreak or root your device. When you do that, you're bypassing the natural protections that your system has and that's going to make you more vulnerable to attack.
2. Don't use custom firmware or a custom ROM. When you're using a custom firmware or a custom ROM, this is specific to Android users, you're using an alternate version of the operating system. It's been forked off the original source code, so when Google has something that's been patched, it doesn't necessarily make its way into those custom firmwares or custom ROMs and so, you're still going to be vulnerable.

3. Also, only load official apps from the official stores. The reason for this, again, is because those have at least some quality control and some level of check before they're released into the public.
4. And finally, always update your phone's operating system. Any time there's an update or a patch for your operating system, or your applications, you want to make sure you're installing it because that's going to patch up the known vulnerabilities.

Sim Cloning & ID theft

SIM cloning allows two cellphones to utilize the same service and allows the attacker to gain access to the phone's personal data. So, if I'm cloning your SIM card, the towers think I'm you.
The first versions of SIM cards were very easy to clone, but the newer SIM version 2 cards are much, much harder. So, this gives us a lot more security.

If the attacker is able to take over your phone number, they can now pretend to be you and log into your bank, your Facebook, your Gmail, or whatever else you have for two-factor authentication.

Well, you can go and get a Google Voice number, or something of that nature, where you have a single phone number that people call and then nobody knows your actual cell phone number that's behind it.

Bluetooth

Bluejacking

Bluejacking is sending unsolicited messages to Bluetooth-enabled devices. This often happens by having somebody who will pair to your device and then send the data to you.

Bluesnarfing

This is unauthorized access of information from a wireless device over a Bluetooth connection.

BYOD

Bring Your Own Device is a policy that a lot of organizations have been adopting.

This means when you come to work, you can bring your own device and use it on their network.

Now, when you use Bring Your Own Device, it brings a lot of security issues for you to consider. If I have somebody's laptop that now gets plugged into my network, I'm also introducing all of the vulnerabilities that device had.

Now, on the flip side, a lot of companies really like Bring Your Own Device because it means they don't have to buy laptops, cellphones, and all those types of devices for their employees because the employee is bringing their own.

A lot of organizations that have adopted Bring Your Own Device will use storage segmentation. This will create a clear separation between personal, and company data on a single device.

I can install Mobile Device Management on it. That would allow me to have a centralized software solution for remote administration and configuration of your mobile device.

But when I do Bring Your Own Device, are you going to let me install Mobile Device Management on your system?
You might not.
And, so this is why a lot of companies are now switching from a Bring Your Own Device, because of all those security issues, into a Choose Your Own Device, or CYOD model.
CYOD gives the employee a choice of a couple of phones.

Hardening Mobile Devices

1. Number one, update your device to use the latest version of the software. Whether this is your operating system, your apps, or your firmware, you should always be updating it. By updating it, you're making sure that you have all known vulnerabilities patched and secured. Just like your desktop, most devices are hacked because they're not patched from a known vulnerability, So, when an update comes out, make sure you apply it.
2. Number two, install antivirus. A lot of people figure that it's a mobile device and it's not a computer so it doesn't need antivirus. But, just like a computer, your mobile devices do need to have antivirus and anti-malware installed.
3. Number three, train your users on proper security and use of the device. This includes showing them how to use social media appropriately, what sites are safe to browse, and what apps are allowed to be installed. Remember, these are all vulnerabilities that your employee, who's holding the device, can install and use on your device. You have a right to train them the correct way.
4. Next, number four, only install applications from the official mobile stores. At least if you've done that, they have malware checks and security checks and you're much less likely to have issues. Again, this is the App Store for Apple and the Google Play store for Android.
5. Number five, don't root or jailbreak your device. That's going to bypass the security and the built-in protections that Apple and Android have already put in there for you. If you do this, you're asking for trouble.
6. Number six, only use version two SIM cards with your devices. As we talked about in the SIM cloning lecture, version two is very hard to clone but version one is actually quite easy. So, you should always use version two SIM cards to help counter SIM cloning.
7. Next, we have number seven, turn off all unnecessary features. Whether this is Wi-Fi, Bluetooth, near-field communication, mobile hotspots, tethering, location tracking, and more. Turn it off if you're not going to use it. If you do have to use Bluetooth, make it undiscoverable.
8. Number eight, turn on encryption for your voice and data. This'll ensure things like Bluetooth, near-field communications, Wi-Fi, and others have encryption enabled whenever you're using them.
9. Number nine, use strong passwords or biometrics for log on. That means you shouldn't be using a four-digit PIN. You want to use things like a thumbprint, a face scan, or long, strong passwords, whichever of those three your device supports. Also, you should turn on Find My Phone, enable remote lockout, and remote wipe capabilities before you need them.
10. Number ten, don't allow BYOD. I know I talked about in the BYOD lecture, that you can allow your organization to make the choice, but let's just be honest: bringing your own device means bringing your own disaster. It introduces a ton of risk; if you use it, you need to ensure that you have storage segmentation and good mobile device management and having your

employees allow you to install it. It's much better to choose your own device or employer furnished devices where you control the device and you control what goes on on it. It's your data, after all, you have to protect it.

After you do all those 10 things you need to make sure your organization has a good security policy in place for mobile devices This will tell your employees what's expected of them and it'll tell your administrator what they have to secure too.