Stay Updated!

To kick off section 3 with a pretty easy start, let's talk about security vulnerabilities and why keeping your programs, apps, and operating systems up to date is important.

But not as important as this message:

Promotional Spot

*At the Black Hat Conference in 2017, security researchers found a vulnerability on all Android devices called The 'Toast Overlay' attack, * Have Plate of Toast **
which was able to deceive users into installing malware by *overlaying unsuspecting images users interacted with.* So the person thought they were pressing buttons related to an app, when they were invisibly giving the app the ability to infect the device. The only version of Android at the time that wasn't at risk was the latest one, *Android Oreo.*

BlueBorne is another vulnerability, which exploited Bluetooth in Android, Linux, iOS, MacOS, Windows, and it led to the possibility of man-in-the-middle attacks, letting hackers hijack the device. Vendors immediately started rolling out patches, which required an update to install.

**Hold bag of sugar ** *Crack....no no. KRACK* exploits vulnerabilities in the *WPA2 security protocol on routers and allowed hackers to eavesdrop on any device hooked up to a wifi network.* This affected all major operating systems, and vendors like Microsoft and Android rolled out their own patches.

These all happened in 2017, and they reveal a very small portion of the exploits out there. Something interesting though was that there was one similarity in all of these attacks: they were all patched and fixed by updates rolled out by a manufacturer. Every program and operating system you have on your devices can be used as an avenue for attack. Now, minimalism in itself is already a great defender against exploits, since there is a smaller likelihood of a program being utilized for wrongdoing. But, one of the best things you can do is to make sure your programs, apps, and operating systems are fully up to date! That way you're receiving the latest security patches, and quite honestly your device should run smoother with the newest features (assuming the developer behind the update is doing it properly)

Some tips: it's pretty frequent nowadays for *programs, apps, and operating systems to update themselves automatically in the background*, which is great for

our security. However, this can be increasingly frustrating. *Windows is well-known to reboot and go through updates at the worst possible times, and automatic app updates on your phones don't allow you to easily see what's being changed in the app by showing a changelog.* Personally, I go through all of my devices and update everything manually once a week, because I can't stand automatic updates--I like having control over the update process and I enjoy reading the changes developers are including in the update. But, for most users out there, I do recommend you leave automatic updates enabled to receive security patches at the fastest possible rate.

Queue Outro Promos

So that's the first lesson and probably the easiest of section 3. Keep your programs, apps, and operating systems up-to-date, and your future self will thank you later. The next lesson is going to dive into the more complex topics, beginning with *permissions and settings.* Thank you for watching, and I'll see you there!