Beware "Juice Jacking" - Avoid Public Phone Chargers

Your phone battery is low again, and you're miles from your charger at home. There's a public charging kiosk or maybe a USB charging port right at the airport terminal counter you're sitting at. But is it safe to charge your phone with a public port?

What Exactly Is Juice Jacking?

Juice jacking pops up in the news every few years—like it did again recently when the FBI warned people about the risk—and you might be wondering exactly what it is and whether you should be worried about it. Whether you have an iPhone or an Android phone, both devices have something in common. The power supply and the data stream pass over the same cable. It doesn't seem like a big deal at first glance, but it creates a unique attack vector for a malicious user to access your phone during the charging process using hardware or software exploits. This attack method is known as "juice jacking," a term coined by security journalist Brian Krebs while writing about the concept in 2011 after seeing a demonstration of the exploit in a compromised charging kiosk at the Defcon security conference.

Since 2011, security researchers have set up a new compromised kiosk at each subsequent Defcon security conference to demonstrate known vulnerabilities and raise public awareness about juice jacking. Over the years, there have been multiple identified exploits that target USB-based charging. Security researcher Kyle Osborn demonstrated a juice jacking attack that could attack an unlocked and tethered phone, stealing data, including Google authentication keys. Georgia Tech graduate students demonstrated a proof-of-concept attack that could hijack an iOS device over a USB charging cable—the attack was undetectable to iOS and gave the attackers complete access to the device. Another proof-of-concept attack was showcased at Defcon that allowed the person in control of the compromised charger to monitor the screen of iOS and Android devices via a screen mirror exploit. So for as long as you were charging your phone at the compromised station, the attacker could watch everything you were doing like they were looking over your shoulder. An even more concerning exploit was showcased by Symantec researchers. The exploit they uncovered started with juice jacking, but persisted even after you disconnected from the compromised charger. They called the attack "TrustJacking" because it exploited the handshake between an iOS device and iTunes, allowing the malicious actor to maintain a connection to the iOS device after the device was unplugged.

Should You Be Worried About Juice Jacking?

The chances that the USB charging ports in the kiosk at your local airport are actually a secret front for a data-siphoning and malware-injecting computer are relatively low. This doesn't mean, however, that you should just shrug your shoulders and promptly forget about the very real security risk plugging your smartphone or tablet into an unknown device poses. The worst time to find out about an exploit is after you've been targeted by the exploit. And the best way to avoid being targeted by an exploit is to engage in best practices that minimize your risk. Juice jacking might not be a widespread (and easily deployed) problem like text message bank fraud scams, but that doesn't mean you should just dismiss the potential risk altogether. The best way to avoid ever ending up on the losing side of a juice jacking attempt is to use some simple practices to ensure your phone never has a "naked" interaction with a public charging station. First, let's look at some best practices that avoid exposure to insecure ports in the first place, and then some tips for avoiding issues when using a charging station or port.

Keep Your Phone Updated - Before we share any other tips, the best phone security tip in regard to juice jacking (and just about every other smartphone security issue out there) is to keep your phone updated. As we mentioned above, juice jacking exploits are a real thing, but there are no reports of them being successfully deployed in the wild. When security researchers show off the exploit, it gets patched. You're not getting the exploit patches if you're not updating your phone.

Bring a Charger with You - Phone chargers are so small and lightweight that they scarcely weigh more than the USB cable they attach to, and advances in charger technology mean you're not sacrificing charging speed and power if you go small. Gallium Nitride (GaN) chargers are petite but powerful, you can add a 30W charger to your work or travel bag and not even feel it. So throw a charger in there to charge your own phone and maintain control over the data port. Not many devices have user-swappable batteries these days, so if you want to keep using your device without relying on the charging ports at the airport (or you can't find a good spot to plug in your personal charger) you'll need a portable charger. Something inexpensive and compact like the Anker 313 Power Bank should do the trick. With 10,000 mAh of battery life, it will charge your average smartphone completely 2-3 times before running out. That's more than enough juice to make it through playing on your phone at the airport and the flight itself.

Use a Power-Only Cable or Adapter - Ideally, you never physically tether your phone to a device you don't have complete control over. But if you use a charging port on a device you don't control, a good stop-gap measure is to use a cable or USB adapter that interrupts the data connections, leaving only the charging connections available. Data-blocking USB adapters, are the most convenient way to do it because you can use any of your existing cables with them, and they'll stop any data connection between the phone and the compromised charging port. One of the best known companies in the niche market is PortaPow. They have a USB-A to USB-A adapter, a USB-A to USB-C adapter, and USB-C to USB-C adapter. Given that most public charging ports are still USB-A, you'll want to buy a USB-A to USB-A or C adapter based on your needs. It's worth noting that there is one big downside to using a power-only cable or adapter. USB fast-charging standards use the data connection to identify the device and negotiate a charge rate. No data? No negotiation, and the charing rate defaults to the basic USB speed.

Lock or Power Down Your Phone - Don't use your phone while charging if you want to play it safer with a public charging port. Keep the phone locked or, better yet, power it down. It's far better to avoid using an unknown port altogether, but if you do, keeping the phone locked or powered down helps prevent simple exploits that reply on you accepting a connection.

Use Wireless Charging - If your phone supports wireless charging and you are in a location with wireless charging pads thoughtfully embedded in the counter or armrests, you're in luck. Wireless charging is inherently data-free, and there is zero risk involved in dropping your phone onto a wireless charging logo on a Starbucks table at the airport.

Ultimately, the best defense against a compromised mobile device is awareness. Keep your device charged, enable the security features provided by the operating system (knowing that they aren't foolproof and every security system can be exploited), and avoid plugging your phone into unknown charging stations and computers the same way you wisely avoid opening attachments from unknown senders.