What is Jacking Juice? Why shouldn't the phone be charged in a public place?

Public battery charging kiosks can make you a victim of hackers who want to collect your personal information and benefit from that information.

There is a fairly common situation as follows.Suppose your beloved phone is running out of battery while you're having an interesting conversation with your new girlfriend on Facebook, and the 'good news' is that you forget the damn charger at home, Then suddenly you see a public USB charging column on the corner.Without hesitation, plug your phone in and continue to enjoy the sweet taste of the unfinished conversation.That comfort can make you a victim of hackers who want to collect your personal information and benefit from that information.

What is Jacking Juice exactly?

Regardless of the type of modern smart phone today, it is possible that Android, iPhone or BlackBerry devices all have a common feature that is the charging power and the data stream passing on the same port and a cable line. .Whether you are using the current standard miniB USB connection, USB typeC connection or Apple's exclusive Lightning cable, the cable used to charge the battery also functions as a data transfer and synchronization function on the phone. .

'Only by plugging the phone into an unknown charging source, your device is at risk of being infected with malicious code.You may have to pay for all your data, 'explained security expert Drew Paik of Authentic8.

Phone charging points and public Wi-Fi are often found in places like airports, airplanes, parks or convention centers.Connecting the phone at these charging points brings small risks.

"The type of cord you use to charge your phone is also the data cord from the phone to another device. For example, when you connect your iPhone to your Mac with the charger cord, you can download photos from your phone to Mac. If Public charging ports are hacked, bad guys have unlimited access to your data, "Paik explained.

Such data can be email, messages, photos or contacts.The method of hacking this information is called 'juice jacking' - the term was created in 2011. Last year, it was also discovered the 'video jacking' method, using hacked and screened ports. picture of the phone to record everything the user typed and looked at.

It can be understood simply that these are invasions of privacy.Specifically, data such as private photos and contact information will be copied to malicious devices through connections to public charging devices.In addition hackers can also transmit malicious code directly to your device and then steal the information for a long time.At this year's BlackHat security conference, security researchers Billy Lau, YeongJin Jang and Chengyu Song presented the topic 'MACTANS: Bringing malware to iOS devices through unreliable chargers. say 'and this is an excerpt from their presentation:

'In this presentation, we present how iOS devices can be compromised within a minute after they are plugged into a malicious charger. We will first look at Apple's existing security mechanisms to protect against arbitrary software installation, then describe the possibilities that USB ports can be used as a tool to bypass. through these protection mechanisms. To demonstrate the existence of malicious code, we will show you that an attacker can hide their malware in the same way that Apple hides its own integrated applications. To demonstrate the practical consequences of these security holes, we have gathered information about the concept of malicious chargers using BeagleBoard, called Mactans'.

Using cheap hardware and taking advantage of security holes on the device, hackers can access existing iOS devices in less than a minute, although there are many security measures that Apple has taken. out to deal with this problem.

For many years, at the 2011 DEF CON security conference, security researchers from Aires Security: Brian Markus, Joseph Mlodzianowski, and Robert Rowley, have built a charging kiosk to specifically demonstrate the danger. Juice Jacking and alerting the public to the dangers of connecting the phone to malicious charging kiosks.

Even more troublesome is that exposure to malicious charging kiosks can create a prolonged security problem even if the device is no longer connected to that charging kiosk.In a recent article on this topic, security researcher Jonathan Zdziarski points out how iOS vulnerabilities still exist and can provide malicious users with your device window even after when you no longer contact kiosks:

'If you don't know how to pair on your iPhone or iPad, here's the pairing mechanism that your computer establishes a reliable connection with your phone, so you can connect to iTunes, Xcode. or other tools. When a desktop computer is paired with the phone, it can access a variety of personal information on that phone, including contacts, notes, photos, music collections, sms databases. , cache and can even backup all data on the phone. When a device is paired, all this and many other things can be accessed wirelessly at any time, regardless of whether you turn on WiFi synchronization or not. You can liken these malicious software as a

chronic virus, they will only disappear when your iPhone or iPad restores your settings first. "

How to avoid getting Juice Jacking?

Although Juice Jacking is not currently a common threat such as phone theft or malicious virus exposure through download data, you should still take the usual precautions to avoid further Contact the systems that may have malicious access to your personal device.

The simplest and most effective way of preventing is simply to limit or avoid charging your phone from third-party charging systems:

Keep your device running out of battery: Get in the habit of charging your home and office phone when you're not using them.Current battery technology allows you to charge stuffed, unplug your charger comfortably without worrying about battery packs, so try to keep your smartphone always energized before you go out.In addition to making sure your phone is fully battery-powered, you can also use additional power management applications, which save battery life.The effectiveness of these applications is still relatively vague, but it is definitely better than not doing anything.

Use backup charger: This is the most popular and convenient way to charge your phone battery in case you are not at home, simply plug the phone into the battery to charge it whenever you want.Using this charger, you will

not have to worry about security, but in return you will have to spend a small cost to buy a spare battery as well as choose the appropriate type to limit the risk of fire when not sewing to buy is less safe.

Using your own charger with AC outlet: In some cases, public charging stations may have both a standard AC outlet and a USB charging port to meet the demand for charging speeds.In this case, ignore the USB charging ports that plug the phone's standard charger directly into the AC outlet.There is no security risk when you use an AC outlet even if the network traffic is being transmitted through the power cord.Your device will be safe as long as you use a reliable charger.

Lock your phone: When your phone is locked, it won't pair with the connected device.For example, iOS devices will only pair when unlocked.But again, as we mentioned earlier, pairing only takes a few seconds, so you should make sure your phone is actually locked when charging.

Power off the phone: This method only applies to certain phone models.Although the device is powered off, the power on the entire USB circuit is turned on and allows access to the flash memory in the device.

Disable pairing (only for jailbroken iOS devices): The jailbroken iOS devices allow users to control the device's pairing behavior.

Use only adapter type: This is the last method you can use, very effective but a little inconvenient.You can buy adapters that only charge, they are quite cheap.There is absolutely no problem with this type of adapter.They are like a small dongle that you will plug into the USB port before connecting the phone's charger cable.Connection pins that act as data transmitters will be disconnected in this dongle, allowing only power to be transmitted through the connection.

However, this adapter also has a small drawback, that is, they only support charging with limited power at 1A, meaning that you cannot use any other fast charging technology.1A is the maximum capacity you get.However, many public USB charging ports even have slower charging speeds.In addition, it is worth noting that the device will only charge at 500mA (0.5A) from the USB port of the computer, so this adapter can speed up charging if you are charging the device from the device. laptop or desktop.

If you are using Android devices, you can also purchase charging cables that act like a dongle, then the data transmission pins in the cable will be missing, resulting in the connection for the purpose of giving Data exchange will never be done via cable.As for Apple's Lightning port devices, it seems that there are currently no charging Lightning-to-USB cables available on the market.However, iOS users can still use charging adapters, which can work with both iPhone and Android phones.

Finally, the best protection against infringement is in your own awareness.Always keep your device always charged with the necessary power, regularly updating the security features provided by the operating system (although they are not easy to use and every security system can be exploited) and finally, avoid plugging the phone into charging stations and unspecified computers in the same way you avoid opening mail attachments from unknown senders.

See more:

1. How to protect your computer against a Foreshadow security vulnerability
2. Top 10 compact antivirus programs for USB
3. What to do if your computer has a virus?
4. Remove root malware (malware) on Windows 10 computers
5. How to use the public USB charging port safely?

You finished reading the article "**What is Jacking Juice? Why shouldn't the phone be charged in a public place?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.