Stay 100% safe when charging

Thanks to charging stations in public spaces, topping up your phone and tablet's battery when out and about is easier than ever. But as **Nik Rawlinson** explains, there may be hidden dangers lurking behind the USB port you're plugging into

What's on the other end of your charging cable? It's easy enough to answer that question when you're at home, but what about when you're plugged into a public charging point at a train station, pub, coffee shop, airport or on a bus (pictured below)? Behind the USB socket, there could be a tiny computer quietly stealing your data – a hacking attack known as 'juice jacking'.

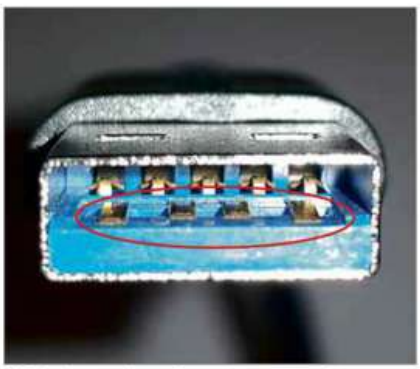
The concept of juice jacking is as simple as it is scary. You believe you're plugging into a standard powered USB socket when, in reality, you're connecting your phone or tablet to a computer run by hackers designed to do a simple job very effectively: siphon off your personal data so that hackers can use it to steal your identity or install malware on your device, so even when you disconnect, the hackers will retain a degree of control over your device. While the risk of becoming a victim of this kind of attack is relatively small, the consequences for those who do can be grave.

Computers are becoming smaller all the time. When you consider that even modern charging cables (such as Apple's Lightning connector) contain processors that regulate the charging process, think how powerful a concealed computer in a USB adapter or desk-mounted plug socket might be.

Juice jacking is a growing threat. It first came to prominence at the 2011 Defcon security conference in Las Vegas. Since then several law-enforcement agencies, including the FBI, have issued warnings.

In 2013, researchers at the Georgia Institute of Technology developed a juice-jacking device that installed a fake Facebook app on iPhones and iPads in under 90 seconds. Although this was just a theoretical attack and the fake app wasn't actually malicious, it illustrated how hackers could use the same approach to secretly install malware.

USB charging points can be found everywhere these days – even on buses



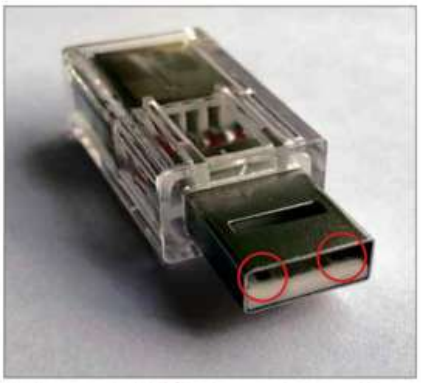
USB adapters have four primary metal contacts – two for power, the other two for data

Buy a USB 'condom'

Juice jacking is only possible because USB cables typically fulfil two roles: they carry both power and data. Look inside the connector that plugs into an adapter or your PC's port, and you'll see at least four small metal contacts (pictured below left). Some USB 3.0 adapters have as many as nine contacts.

The two outer contacts are used for power, the two inner ones data. Knowing this, it's easy to combat juice jacking by disabling the two data contacts. You could feasibly create your own power-only USB cable by forcibly removing these contacts, thereby preventing any data transfer, but it's not something we recommend because you could end up damaging both the USB cable and the device you plug it into. Instead, you should consider buying an inexpensive data-blocking adapter - often referred to as a 'USB condom'.

We bought a Pure USB Data Blocker from UK-based company PortaPow (£6 from Amazon www.snipca.com/33993), opting for the clear version that shows the tiny circuit board inside and how the two inner connectors don't carry through



Unlike standard USB adapters, the PortaPow Data Blocker only has two data connectors

A USB condom sits between your USB cable and the device you're plugging into

Avoid carrying a separate adapter by buying a USB cable with a data blocker built in

from one end of the adapter to the other (see photo above). These are used purely for charging, not transferring data. It's also available in red or black with a SmartCharge chip (more on this later) and with a USB-C connector for newer devices.

Using the Data Blocker is simple: just plug it into the PC port, charger or public USB socket you're using to power your device, then plug your phone/tablet's USB cable into its output socket (see photo above right). When you do this, power will flow to your device, but data will be blocked.

This doesn't let your computer connect to your phone like an external drive, and your phone won't pop up any alerts if you use it to charge from an adapter in your car's cigarette lighter, which will help avoid distractions when driving.

This does mean you can't synchronise your device when using the Data Blocker, but as you'd only want to do that when connected to your own computer – or when using online backup services – that shouldn't be a problem.

PortaPow is just one of several manufacturers of USB condoms. If you choose to use another manufacturer, and you can't see inside the USB condom, check that the middle two visible contacts have been removed, so you can be sure there's no chance of data leaking in or out.

Nor are you restricted to buying an adapter that relies on your current cable. If you're about to replace your existing charging cable, and your device doesn't use an older or less common USB connection, you can buy a USB connector cable with data-blocking capabilities (for example, PortaPow's USB-C Data Blocker cable – £5 from www.snipca.com/34029).

However, if you're like us (we need to charge two phones, one which has an Apple Lightning connector, the other microUSB), the PortaPow adapter is a compact and convenient option.

Fast charging with a USB condom

You can charge any phone or tablet using a USB condom, as long as it uses a matching USB connection. However, phones with fast-charging features, like those with Samsung Adaptive Fast Charging or Motorola TurboPower, will take longer than normal to charge when using the PortaPow data blocker. That's because these features rely on a technology called 'active data transfer' to communicate with the charging source. Because these fast-charging features can't use active data transfer with a data blocker, they reduce the charging rate to avoid causing damage.

PortaPow also makes a data blocker that includes a SmartCharge chip (£6 from Amazon at www.snipca.com/33994). This switches the blocker's charging profile between Apple, Samsung and Universal standards, and passes a 2.4-amp current to allow faster charging. ca

Carry your own personal charging station

Alongside using a USB condom, the safest way to charge your tablet or phone is to use the adapter and cable supplied with your device, plugging it directly into a three-pin power socket. However, this isn't always possible, so what are your other options?

We recommend using a portable power pack, which has the added benefit of letting you charge your battery when you're nowhere near a power outlet – such as when on rural walking holidays.

These can be fairly cheap at around £15 for a 5,000mAh unit (such as this Energizer power bank from www.snipca.com/33999). This should be enough to charge new phones and tablets twice over. However, a 5,000mAh power bank would only top up the 11in iPad Pro to around 60 per cent, and the 12.9in version to just over 50 per cent.

If you're heading off on a longer excursion, consider spending more on a higher-capacity power bank. These will be larger, but they'll also charge your devices several times over before they need to be charged themselves.

The Zendure A6PD may be expensive (£84 from Amazon at www.snipca.com/34000, pictured), but its 20,000mAh capacity means it can even recharge a laptop. If you're going on a remote holiday, it could be the perfect solution – letting you charge your phone, tablet and camera when you're out on your day trip. Simply recharge the power bank overnight before your next outing the following day.