How USB-C Is Going to Get More Secure

In the present scenario, we find more **USB cables** in our drawers than the documents. I am sure that your drawers are full of different USB drives, cables, and chargers you bought over the years. Their overall quality has improved over the years. Now, they charge your devices more quickly and transfer files at an astonishing rate. But they haven't gotten any secure.

SFCable

And that changed a few months ago.

We all are aware of the USB-IF. It is an industry group which is responsible for the development of USB standards. Back in January, they announced the USB Type-C Authentication Program. During the press conference, they put the utmost importance on authentication. Further, they said that it would empower the host system to protect against non-compliant USB adapters and decrease the risks of malicious firmware or hardware in USB devices.

How USB Cables Are At Risk?

In case you are not aware of it, the USB ports on your devices entail a crucial security point. There are major hacking risks from hackers, as they can tamper with public chargers and use them to hack phones and other devices with malware. They

SFCable

can easily ship some nasty malware which would seriously damage your data.

USB-C With A Solution

With USB-C authentication, it would be an obstacle for hackers to attack your devices. For example, while connecting your phone with a charger, it would establish a particular connection with that charger. If everything works out well, it would create the connection and the current would start flowing. In case anything looks suspicious the phone would deny the connection.

The USB Type-C authentication program would address two major issues with Type-C hardware:

SFCable

It can damage your important devices with faulty cables. If you are new to this, it is important for you to be aware.

Cables and chargers would need proper implementation of USB power delivery specification. And by using the authentication framework, the device can block uncertified cable users under the assumption that they may harm your devices.

Hence, by implementing this authentication program, at the hardware level, can protect users from harmful firmware

SFCable

which might be hiding on USB devices. The related authentication keys would prove that USB-C is safe, which would allow your computer or phone's safe and secure connectivity.

The major purpose behind creating such security is to create a secured junction between different USB Type-C devices. For instance, if you're at the shopping mall, and want to charge your phone at one of those charging stations, you are worried about its security. When there is an authentication program in place, your phone will instantly deny any connection if there is a chance of malware.

However, for now, this program is going to be optional for the users. But there is a possibility that the program could become mandatory which help all USB Type-C equipment to stay safe. Recently USB-IF president Jeff Ravencraft said that "USB-C is

the future,". According to him, if the connection protocol would come in effect, it would help all the devices to stay safe. In fact, there would be one cable to rule them all. Hence, they are working toward making its security more authentic and prevent nefarious elements from violating the ubiquity of cables and ports.

This authentication program could protect your laptop or desktop PC from malicious USB drives in the same way any anti-virus software protects your PC. The USB-C signature on the drive would be compulsory as a sign of reorganization, otherwise, the computer won't permit a connection.

Till this date, the security upgrade is welcome. But, there is a chance that manufacturers could theoretically lock their devices to their own cables and **USB *adapters***. It could all

come down to how selective companies will be about implementing USB type-C authentication.

Currently, at this stage, this program is only here as a recommendation. It is not mandatory to implement it to your computers. But we can say that such initiative certainly points to the future security requirements for USB-C according to USB-IF president. In the present year, the latest iPads even include USB Type-C ports. The first Apple mobile product, which is not using one of the company's proprietary ports. You can literally connect keyboards, audio interfaces USB, MIDI devices, cameras, external storage Ethernet cables, and what not!

It is not adding anything in terms of compatibility with other USB devices. It will be just the way you connect them.

SFCable

The beauty of a USB-C hub is that you can create a permanent workstation on your desk and dock the iPad to it. This hub can connect power, an audio interface and speakers, musical instruments, a USB keyboard, and also provide an SD card reader. Now, if Apple itself could use the USB-C, we can expect a better future which is more secure. What do you say?

With the increasing hacking and an unsecured environment, even a USB can be a big threat to your data. *Learn what the future looks like for USB security*.

If you found this Blog post useful, here are some other Blog posts that may be of interest.

Five Types of USB Type-C Adapters You Must Know About

Why Should You Choose USB Type C Over All Other Cables?

Some FAQs About USB C Cables Answered!

SFCable

SFCable