Issued 9/25/18

With USB-C, Even Plugging in Can Set You Up to be Hacked

Plugging in the power -- or at least what you think is power -- to a USB-C powered laptop can connect your computer, and the valuable personal data on it, directly to hackers. Your personal financial information, passwords and documents stored on the laptop could help a cybercriminal steal your identity. The laptop may even be used to attack your employer's computers and network. Some attackers are finding a weakness in phone charging. Many newer phones use the same port – one of several types of USB – for both connecting to a computer and charging. A charger could be modified to attack your phone via that trusted connection. This has led some researchers to recommend never using public USB chargers for your smartphone. Older mobile phones, including some smartphones, which used power-only connections didn't have to worry about this issue. Users of these devices can plug in to public multi-device charging stations without worry, as there is no connection to the device's data. For those with combined data and power ports, however, the same port that many people only use to power their phone is commonly used by hackers and even law enforcement to access the data on it. Until recently, laptop computers had enjoyed some protection, with most having a dedicated power port to connect their chargers to. Other purpose-specific ports allowed connections to desktop monitors, conference room projectors and other devices, without need for concern. USB-C changed this, with one high-speed port now able to provide and receive power, send video signals to projectors and monitors, and connect to USB thumb drives and numerous other peripheral devices. Most of the time, this is extremely convenient, reducing the number of different ports needed on today's lightweight and compact laptops. However, it also allows

criminals to attack the computer of an unsuspecting user who is just trying to charge the device's battery. USB-C laptop users should not plug in to airport, hotel or other public USB ports without protection. Charge-only adapters, portable USB batteries and cables that can shield the data connection are possible solutions. At present, in most cases, it is best to just plug the laptop's power supply into a normal wall power outlet; many public USB ports, which follow the older USB-A standard, don't yet provide enough power to run and charge a laptop anyway. When connecting to other devices, check for signs of tampering, such as missing screws, scuffing and other wear – particularly around screw holes and edges. When projecting for others, use your own USB-C to VGA or HDMI converter and connecting to these ports. USB-C users need to protect themselves by not connecting to public, insecure and other potentially compromised or suspicious USB ports. Information technology managers face a tougher battle and may try to avoid USB-C powered devices or train users to use them safely.