USB killer stick attacks

Often times when we talk cyber-security, we focus on online methods of attack. But there's a real physical threat to computers you may not have heard about called a USB killer device.

Recently, a former student at a New York college used a thumb drive to destroy 63 computers and other devices with USB ports causing nearly $60,000 in damage.

Instead of using malicious software, a USB killer device delivers an electrical charge that fries the device. It uses the USB charging function of the port to charge capacitors in the USB killer and then deliver an electrical death blow to your device. This doesn't just affect computers, any device with a USB port is vulnerable.

A USB killer can be purchased for around $60 online. I won't share the link to the site, but it's as easy as any online purchase. What's even scarier is that it looks just like an ordinary USB drive.

How can you protect yourself? The first step is to be very careful about inserting flash drives from unknown sources into your devices. Don't leave your equipment unattended even if the system itself is password protected. If your devices never leave the house and you don't allow anyone else to touch them or insert USB drives into them, you're pretty safe.

If you're in a situation where your equipment is going to be exposed, consider a USB port lock like the one shown below. It runs about $15 and comes with three locks.
Just insert the lock and remove the key. The USB port will remain blocked until you come back with the key to remove it.

You can check it out at this link: https://amzn.to/2XCgEIa

There are several other locks on the market and you may be able to find some at local computer stores. We are an Amazon associate, so if you were to buy one of these locks after clicking on the link, this site would receive a few pennies on the purchase.

Questions about this or anything else? Click here to ask.
This tip was sent to us by Cyn Mackley, previously the tip expert at WorldStart.com.