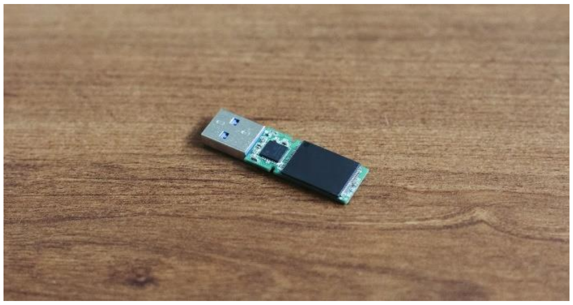
Security Breaches by USB -

The Danger of “Lost and Found” Thumb Drives



USB attacks might sound like they’d be limited to personal devices, but the implications can in fact be much bigger.

A particularly well-known example of a USB drop attack is Stuxnet, a computer worm that infected software at industrial sites in Iran, including a uranium-enrichment plant. The virus **targeted industrial control systems** made by Siemens, compromised the system’s logic controllers, spied on the targeted systems, and provided false feedback to make detection even more difficult, and it all began with a USB stick infection.

Don’t be a victim. When it comes to your vessel’s Cyber Security, active prevention is the best strategy. Do not plug in any “found” thumb drives.

The United States government, too, has fallen victim to flash drive attacks. In 2008 an infected flash drive was plugged into a **US military laptop** in the Middle East and established “a digital beachhead” for a foreign intelligence agency. The malicious code on the drive spread undetected on both classified and unclassified systems enabling data to be transferred to servers under foreign control.

A company in Hong Kong has even developed a USB that could **kill a computer**. Collecting power from the USB line, it absorbs power until it reaches about 240 volts and then discharges that energy back into the data lines in devastating power surges. Oh, and the USB Kill drive is available for just $56 — in case you think this is only something someone could accomplish if they’re tech savvy and have deep pockets.

USB Security Awareness

Think about the effort expended on telling children not to take candy from strangers. It's the same idea with encouraging employees not to put found USB devices into their computers. **One 2016 study** dropped 297 USBs on a university campus. Of the 98% of found devices that were picked up, 45% were plugged into computers.

These convenient drives are also easy to lose. In fact, **one 2008 study** found an estimated 9,000 memory sticks were found in people's pant pockets at the dry cleaners. If the information on these left-behind drives is not encrypted and can be accessed by the wrong parties. This in and of itself represents a security risk.

So what's to be done?

- **Do not put any USB drive into the vessel pc system. Should a surveyor/agent want something printed, the USB Drive MUST be inserted directly into the printer and the forms printed off that printer.**

- **Ensure that crew don't store sensitive information on USB devices.**

- **If important data must be stored on a USB device, make sure it's protected with encryption or another safety feature such as fingerprint authentication and only used for vessel business.**

- **All crew to separate flash drives used for personal use from those used on the vessel.**
- **Most of the vessel business pc's have the USB ports blocked to avoid attack.**

- **And of course, it's always smart to keep security policies and patches up to date on the crew's personal laptops.**