

# Preparing for Predatory Peripherals

February 2011



Your mouse may no longer be a friendly. That goes for your keyboard as well. Cyber security researchers have reportedly found a way to create peripherals that can be programmed to steal and transmit data when certain actions or keystrokes are performed. This is done by implanting a circuit board off a commercially available USB microcontroller within a keyboard or mouse.

When originally reported, this new threat was only a proof of concept device and not a technology discovered to be in use by the bad guys. However, by the time you read this that may no longer be true. Even with the Army banning the use of USB devices until protections and protocols are in place, our sensitive data is always at risk. The fact that such devices can be built demonstrates that for every precaution taken to ensure cyber security, there are always new potential threats and intrusions.

This kind of news might inspire us to never boot up again. However, reality does not give us that option. Computers and the military are forever integrated until we perfect that thought-activated technology. (Author's Note: Two large fellows in black suits wearing dark sunglasses just showed up (that was QUICK). So I'm not going to write about that mind stuff anymore, because it doesn't exist! Never did! Never will! Whew – they're gone. Anyway the bad guys are probably working on it too.)

Joking aside, the message here is that a machine can always be compromised and sometimes in ways we may not expect. So once again we need to rely on our greatest cyber security resources: awareness and common sense. The ability to switch our innocent looking peripherals for ones that can secretly access and transmit data reinforces the need to keep your computer equipment physically safe as well as virtually safe. If they have not done so already, the smart guys and gals in IT will figure out a method of detecting this kind of intrusion and create safeguards. Yet, once again it is the responsibility of each and every computer user in the military to be aware of the latest security hardware, software, policies and procedures (AR 25-2), and use them.

The old nuclear control saying is "trust but verify." Unfortunately, if a common peripheral has been compromised, it is difficult, if not impossible, to verify. You might get lucky and notice something different about the physical appearance of a peripheral. But unless there's a unique dent in your mouse or keyboard that might have "accidentally" occurred after a data-losing system crash, your chances of noticing are slim. However, it can't hurt to take the time to check. A little well placed paranoia never hurt in the constant effort to protect military and personal data.

Take a few moments to check your equipment if you think something is out of place. Make sure that your computer is always under your control when on TDY or in an unsecured location. Along with staying on top of the latest potential cyber security threats, both virtual and physical, and following information assurance best practices is the best way to protect your hardware and data. Is it a pain? Could be. Is it REALLY necessary? Absolutely!

Now, for all you smug laptop users saying that you don't have peripherals that can be compromised, rumor has it that they are developing key covers that.....(Author's 2nd and possibly last Note: Those big guys just showed up again. I think I'll just stop here. Stay Cyber Safe!)