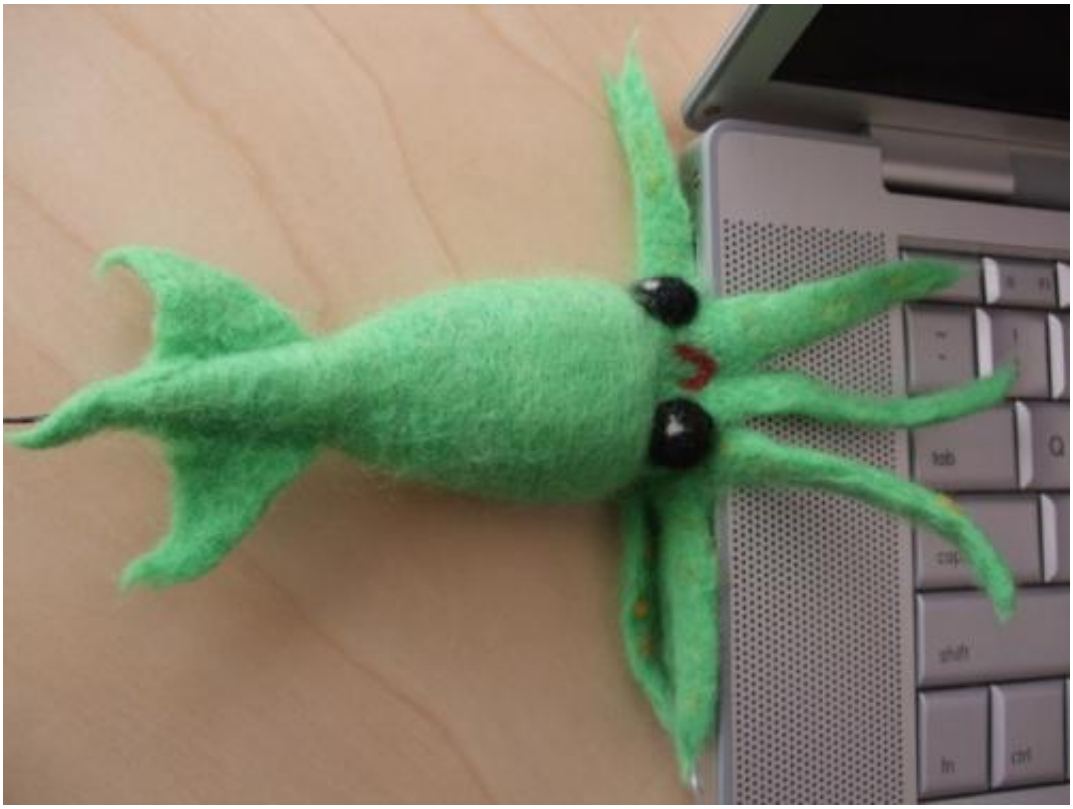
Is your USB stick the enemy?

August 12 2014, by Andrew Smith



Slurping up your data like it’s an all-you-can eat krill buffet. Credit: Scott Beale, CC BY-NC-SA

Computer users everywhere are looking at the USB stick sat next to their computer this week with trepidation. Many are now wondering if this trusted friend has turned against them now that cybersecurity experts say they've found a massive flaw in the very make up of these devices. It seems the humble USB drive can easily be used to compromise basic

security principles in your machine.

The issue is considered so serious that a statement has been issued by the USB working party, the body that regulates this technology standard.

The group admits that there are security flaws in USBs but says that manufacturers should build in existing standards to protect consumers. This would mean that your average USB stick would be more expensive but more secure. In the meantime, you might want to take a second look at the stick on your desk.

Sticky problem

USB storage devices are still a staple tool for many of us. They are great for keeping a copy of your data, especially if you have to take it from home to work and if an online data transfer would take a long time.

The problem is that many files can be hidden on a USB without the user knowing they are there at first glance. And when your computer detects that you have inserted a USB storage device, it may well try to automatically run any code it finds on the stick. This process is a feature of many computers and dates back to the days of the CD-ROM, when you could load a disk and your computer would start running it without the need for you to click on any icons.

This is indeed a scary prospect and it gets even scarier when you learn that one of the most famous computer attacks of all time was started from a USB stick. We still don't know for sure who released the Stuxnet computer worm that disrupted Iran's entire nuclear programme but we do know that it came out of a USB stick.

In fact, this is still considered to be one of the most common methods of social engineering. Some cyber-criminals target companies simply by

dropping USB sticks next to car doors in the car park. Curiosity gets the better of a passing employee and they insert the USB stick into their office computer. Before they know it, their machine has been compromised.

Hackers can easily write code that essentially turns the USB stick into a mouse or keyboard. They can then control your machine remotely, accessing your files and personal information. The code deposited on a computer can send screenshots of everything you do via the internet and these days, speeds are so good that you might not even notice them taking up the bandwidth on your home network as they do it.

Stick or twist?

This is definitely a very worrying problem but it is actually something that has been known about for some time in the industry. Corporate IT professionals try their best to mitigate the problems posed by rogue USB sticks. In fact many employers ban insecure USB devices on their systems.

As an ordinary user, you are at risk but avoiding the problem is very easy. All you need is good practice. Many of us scan our personal computers regularly using anti-malware software. This should be extended to any external storage devices, including USB sticks. In addition, make sure that your anti-malware software of choice automatically scans any new USB device. This should overcome the problem of an infected USB stick auto running.

If you are more technologically minded, you can disable your operating system's inclination to automatically install drivers and other software when a new USB stick is connected. The process differs between operating systems, but most have an option to do it. Microsoft Windows is relatively straightforward in this respect and there are many different

approaches for Linux users. Mac users can feel extra smug here as OSX doesn't support autorun in the first place.

While we trust our friends, we should not trust their USB sticks, no matter how nice a person they may be. Be prepared to check their devices before they are ever attached to your machine.

This probably may never be resolved but it might not matter. Many of us enjoy good bandwidth and can transfer large amounts of data with ease. And cloud storage is fast becoming the best option anyway. If you use Dropbox, OneDrive or Google Drive, you might find yourself forgetting what a USB stick is in the the next few years, anyway.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation