



Dangers of Digital Photo Frames

Kelli Tarala

originally printed December, 2008

Digital photo frames were popular gifts during the Holiday season. Digital photo frames contain a screen that displays pictures that had been loaded onto a little onboard computer. The Consumer Electronics Association estimated that 7.4 million such frames were sold in 2008 - up 41 percent from 2007. These popular gifts are sold at Wal-Mart, Amazon.com, and many other locations.

The easiest way to load pictures on a digital photo frame is by plugging the frame into your home computer via a USB port. Universal Serial Bus (USB) ports are standard on all desktops and laptops.

USB ports were designed to allow many peripherals such as cameras, printers, and MP3 players to be connected using a single standardized interface socket. USB ports were also designed to allow hot swapping, that is, by allowing devices to be connected and disconnected without rebooting the computer or turning off the device. USB ports allow pictures to be copied from your home computer to the picture frame very quickly. Unfortunately, other things can be copied back forth quickly as well.

These digital photo frames can carry a big surprise, and I don't mean that picture of you with your head stuck in a bucket! The big surprise is that the digital frame may be infected with viruses and other malicious software. Once you connect the digital frame

to your home computer, the malicious software can jump onto your home computer.

According to Karel Obluk, the chief technology officer of AVG, a security vendor with offices in the United States and Europe, "Users don't realize that bad guys can make use of each and every computer they can control, even if you don't do Internet banking or have any sensitive information. They can profit by spam or other illegal activities and make (your) personal computer part of an illegal network. It's something that users should always be reminded of."

No one really knows how many infected digital photo frames are out in stores. A few frames known to be infected include Mercury 1.5-inch frames sold by Wal-Mart, Element 9-inch frames sold by Circuit City, and Samsung 8 inch frames sold by Amazon.com. The infected code can do a variety of nasty things. Some of the code is old and can be easily detected and removed with current antivirus software. Newer more dangerous code is capable of stealing data, calling out to other malicious code once it is installed itself on your computer, and can record all keystrokes from your keyboard including passwords to online banking and other highly confidential sources.

This malicious code works by taking advantage of a feature in Microsoft Windows called Autorun.



Securing our Digital Future

Kelli Tarala

originally printed December, 2009

Autorun is a application that enables digital frames and other peripherals to run automatically when they are plugged into your computer. Microsoft turns on Autorun by default to make devices easier to use , although security experts at Enclave Hosting and Security routinely turn Autorun off.

Microsoft, however, advises against this. Turning off Autorun is not a simple step, said Ziv Mador, a senior program manager at Microsoft's malware protection center, and home computer users who try it are likely to wind up confused. "They're used to entering a CD (or plugging in a frame) and it loads automatically, and that will not work anymore," he said. "The important thing is to have up-to-date antivirus software and keep it turned on. That will mitigate much of the risk."

If you have received a digital photo frame for the Holiday season, be aware that these devices many contain malicious code. Here are a couple points to remember:

- If you are a computer expert, turn off Autorun in Windows and configure Windows to show hidden files.
- If you are not an expert, do not try this. Keep your antivirus software turned on and up-to-date.
- Buy photo frames manufactured by vendors with known, reputable brands.

Article reprinted courtesy

