# How Trojan Horses Work

One of the most enduring stories of the Trojan War, the most important conflict in Greek mythology, is the tale of the Trojan horse. Trying to find a way into the city of Troy, the great warrior Odysseus ordered his men to build a massive wooden horse, one big enough for several Greek soldiers to fit in. Once the structure was finished, he and several other warriors climbed inside, while the rest of the Greeks sailed away from Troy. One man named Sinon, however, stayed behind in order to deceive the Trojans, convincing them that his fellow Greeks had betrayed him and fled from the city. The wooden horse, he told the Trojans, was safe and would bring them luck.

After some discussion over the matter, the Trojans agreed to wheel the horse through their gates, unknowingly giving the Greek enemy access to the city. After proclaiming victory and partying all night, the citizens of Troy went to sleep -- it was then that Odysseus and his men crept out of the Trojan horse and wreaked havoc on the city.

­Although you've probably heard of the Trojan horse from Greek mythology, chances are you've also heard of Trojan horses in reference to computers. **Trojan horses** are common but dangerous programs that hide within other seemingly harmless programs. They work the same way the ancient Trojan horse did: Once they're installed, the program will infect other files throughout your system and potentially wreak havoc on your computer. They can even send important information from your computer over the Internet to the developer of the virus. The developer can then essentially control your computer, slowing your system's activity or causing your machine to crash.

­Though they're not actually viruses, they're referred to as "Trojan horse viruses," "Trojan viruses," "Trojan horses" or just plain "Trojans." Regardless of what people call them, they all mean the same thing. But what happened? How did you let this Trojan horse into your computer in the first place? And what can you do to stop one from getting in?

# Protecting Yourself from Trojan Horses

So how do Trojan horses infect ­computers? Believe it or not, you have to do some of the work yourself. In order for a Trojan to infect your machine, you have to install the server side of the application. This is normally done by social engineering -- the author of the Trojan horse has to convince you to download the application. Alternately, he or she might send the program to you in an e-mail message hoping you execute it. Again, this is why it is called a Trojan horse -- you have to consciously or unconsciously run the .exe file to install the program -- it doesn't propagate on its own like a virus. Once you execute the program, the Trojan server is installed and will start running automatically every time you power up your computer.

The most common way Trojan horses spread is through e-mail attachments. The developers of these applications typically use spamming techniques to send out hundreds or even thousands of e-mails to unsuspecting people; those who open the messages and download the attachment end up having their systems infected.

Sometimes, it's not even a person manually spreading malware -- it's possible for your own computer to do so, if it's been infected already. **Crackers --** hackers who use their computer skills to create mischief or cause damage intentionally -- can send out Trojans that turn innocent Web surfer's computers into **zombie computers**, so-called because the person with the infected computer rarely knows his system is under control. Crackers then use these zombie computers to send out more viruses, eventually creating networks of zombie computers known as **botnets**.

There are several things you can do to protect yourself from Trojan horses. The easiest thing to do is to never open any e-mails or download any attachments from unknown senders. Simply deleting these messages will take care of the situation. Installing antivirus software will also scan every file you download (even if it's from someone you know) and protect you from anything malicious. If you ever find your computer has been infected with a Trojan, you should disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. You can call your computer's manufacturer, your local computer store or a knowledgeable friend if you need help.

# How do touch-screen monitors know where you're touching?

Touch-screen monitors have become more and more commonplace as their price has steadily dropped over the past decade. There are three basic systems that are used to recognize a person's touch:

* Resistive
* Capacitive
* Surface acoustic wave

The **resistive system** consists of a normal glass panel that is covered with a conductive and a resistive **metallic** layer. These two layers are held apart by spacers, and a scratch-resistant layer is placed on top of the whole setup. An electrical current runs through the two layers while the monitor is operational. When a user touches the screen, the two layers make contact in that exact spot. The change in the electrical field is noted and the coordinates of the point of contact are calculated by the computer. Once the coordinates are known, a special driver translates the touch into something that the operating system can understand, much as a computer mouse driver translates a mouse's movements into a click or a drag.

In the **capacitive system**, a layer that **stores electrical charge** is placed on the glass panel of the monitor. When a user touches the monitor with his or her finger, some of the charge is transferred to the user, so the charge on the capacitive layer decreases. This decrease is measured in circuits located at each corner of the monitor. The computer calculates, from the relative differences in charge at each corner, exactly where the touch event took place and then relays that information to the touch-screen driver software. One advantage that the capacitive system has over the resistive system is that it transmits almost 90 percent of the light from the monitor, whereas the resistive system only transmits about 75 percent. This gives the capacitive system a much clearer picture than the resistive system.

On the monitor of a **surface acoustic wave system**, two **transducers** (one receiving and one sending) are placed along the x and y axes of the monitor's glass plate. Also placed on the glass are **reflectors** -- they reflect an electrical signal sent from one transducer to the other. The receiving transducer is able to tell if the wave has been disturbed by a touch event at any instant, and can locate it accordingly. The wave setup has no metallic layers on the screen, allowing for 100-percent light throughput and perfect image clarity. This makes the surface acoustic wave system best for displaying detailed graphics (both other systems have significant degradation in clarity).

Another area in which the systems differ is in which **stimuli** will register as a touch event. A resistive system registers a touch as long as the two layers make contact, which means that it doesn't matter if you touch it with your finger or a rubber ball. A capacitive system, on the other hand, must have a conductive input, usually your finger, in order to register a touch. The surface acoustic wave system works much like the resistive system, allowing a touch with almost any object -- except hard and small objects like a pen tip.

As far as price, the resistive system is the cheapest; its clarity is the lowest of the three, and its layers can be damaged by sharp objects. The surface acoustic wave setup is usually the most expensive.