

# Corporate protection against fraud



Imagine the following situation: a friend tells you that a new island is about to emerge in the middle of the ocean. Your friend gives you a wealth of detail about the news and at the end, he says very seriously: "I heard in on TV." If that's the case, it must be true, if they said it on TV...

Generally, there could be an element of truth in these statements, and depending on who tells you, you should have many reservations when affirming that they are true. Your friend could have seen a science fiction program, or heard news about Graham Island/Ferdinandea/Giulia (the name changes depending on the source). It might not have any basis at all, or could be completely true.

Often, too many people would accept it as true "if they said it on TV," as happened 20 years ago when someone told me that bacteria that destroyed computers had been discovered (there's a long distance between this news and the first computer virus). Fortunately, another large group of people put certain statements in the "dubious" zone until they can contrast them against some other media source.

But, we are almost in the year 2007 and the experience of rumors has changed. Although we are uncertain in some cases, "I read it on the Internet" is the latest phrase. Everything seen on screen and provides some information is true. Even though the information I received via email is crazy, as it arrived "via the Internet," it's valid. This way of thinking is going to cause many problems for computer users and many more for network administrators in 2007.

The main problem for users in 2007 will be Internet fraud. The most well-known is the classic phishing. If gullible users receive an email from their bank, they will go where they are told to and leave enough data to seriously compromise their checking account without thinking twice. But there are fewer and fewer users of this kind, as the information is slowly getting through to Internet users. Even banks are aware of these problems and in some cases (which deserve praise), they warn their users of a possible fraud in their bank accounts.

On the other hand, network administrators are going to have the same problem with this fraud, but from two very different aspects. On the one hand, they must prevent these thefts at corporate level, so that money is not stolen from corporate accounts, which are without a doubt much more attractive than accounts belonging to users (to the average user at least).

But indirectly, they must also protect the gullible users in their networks. They are responsible for ensuring that the content that gets through to their networks is not dangerous, not only to data (viruses, worms, etc.), but also to network users. Protection does not directly protect the company, but protects the assets of employees. Added-value that administrators often don't perceive.

But in spite of this, there can always be some malicious code on a computer that is causing problems. That funny video downloaded by a user that could need a codec

# Corporate protection against fraud



hosted on a malicious web page, so that when the user downloads and installs the video, a Trojan is installed at the same time. But it is not a known Trojan. It is an exclusive Trojan, of which there are only a few examples circulating in the Internet. By doing this, it will be very complicated for classic systems to detect it. If the network is equipped with proactive detection systems, these threats, which are complicated to detect, can be detected.

In a personal computer, it is not too difficult to setup a more or less adequate protection system. It all depends on the knowledge of the user: if users are aware of the risks they are running, they can install a solution for each problem, including protection against unknown codes.

However, installing protection in a corporate environment poses a problem: to what extent is the network in danger? Am I correctly blocking the threats that can reach my users? If users are not correctly protected, they can have a classic problem, such as files disappearing or the computer not starting up (which nowadays is almost a minor problem). But if a flaw in the security system means that an email message that tries to defraud network users can enter the system, the problem is more serious. And even more serious if the possible defrauded user is in charge of the corporate checking accounts.

When protecting a network, it is not enough to think about installing an antivirus and that's it. Global protection should also consider tricks and swindles, all centralized with clear risk management systems.

**Fernando de la Cuadra**  
**International Technical Editor**  
Panda Software (<http://www.pandasoftware.com>)  
E-mail: [Fdelacuadra@pandasoftware.com](mailto:Fdelacuadra@pandasoftware.com)