

Securing a connection with the bank



Although it does not seem like it, the malware situation nowadays is worrying. There are more people creating malware than ever before and more examples appearing every day, yet users are less worried. The theft of login details for accessing online banks is not only due to phishing, but also to other circumstances.

One of them is users' overconfidence. Most Internet users think they are not hackers' potential victims. Who is going to target them if they barely have any savings in the bank? Surely hackers only raid the accounts of those with yachts in Montecarlo?

Wrong. Very wrong. If you have an Internet-connected home computer and you access your bank's website via broadband, your spending power is very high. Bear in mind that your 1,000 euro system –a luxury item, after all- is the equivalent of the annual per capita income in more than 60 countries.

A hacker from these countries will no doubt think that there is plenty enough money in your bank account and that by the time they have also emptied your neighbours' and friends' accounts, they'll have a tidy sum stashed away. Less, of course, than if they had robbed Bill Gates or the Queen of England, but no doubt your computer will be easier to attack.

Most Internet users think they are normal users, and that hackers are more likely to attack corporate systems or a millionaire's system than their own.

Bear in mind that as soon as you connect to the Internet, you are no longer yourself, but an IP address. It takes a hacker the same effort to attack the address 12.34.56.78 (in the U.S.) as the address 87.65.43.21 (in Belgium). If either of the addresses has bank accounts managed over the Internet, it means profits. As small as the amount may be, it is better than nothing. A legend claims that Pericles was thinking about his own misfortune while eating a piece of bread. As he wondered whether there could be anyone more unfortunate than himself, he saw another man collecting the crumbs he had dropped. There is always someone who can benefit from your piece of bread, even if they are only scraps.

Danger in commercial transactions is high. To avoid it, users generally rely on antivirus that detect Trojans or spyware that have entered computers. But is this enough?

Statistics indicate that the malware situation on the Internet is much more critical than you imagine. Over a thousand threats appear each day, nearly one per minute. Are you therefore, protected 'by-the-minute'? This is almost impossible. You would need to be connected to research laboratories all the time and have extremely advanced tools on your system to identify suspicious codes.

Many users update their antivirus before performing an online transaction. This is not a bad idea, as in that way, you can be sure that all known malicious codes are detected. However, as up-to-date as the product may be, you should not forget it will only detect the codes known the moment the update is released, and it may not

Securing a connection with the bank



detect a code that has been stealing data from other systems worldwide for one hour or just a few minutes...

Therefore, before logging in to your bank account, it is best to scan the system with the latest available data from the virus investigation laboratory, and also by using a system capable of detecting unknown malicious codes.

Although the idea is good, whoever has tried to carry out an antivirus scan on the computer will have realized that due to current hard disk sizes, the scan can take much longer than what you are willing to wait.

And why search all the hard disk? When you log in to the bank's website, the object is to find malicious codes that can affect you at that moment, not the ones that are on the hard disk, hiding in a directory you do not use, presently inactive and therefore not causing immediate problems.

If the search is limited exclusively to the memory, to the programs running, you can decrease the scan time. In just one minute you can find out if any of the latest threats discovered are lurking on your system. Do you want to check it? Try <http://www.nanoscan.com>.

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