

Charles Smith's telegraph.co.uk | [Edit your details](#) | [Free email services](#) | [Your subscriptions](#)



Search For  in  Search options

Wednesday 3 September  
2003



Tele

[telegraph.co.uk](#)

[Site index](#)

[Connected home](#)

[Science news](#)

[Technology news](#)

[Dotcom news](#)

[Boot camp](#)

[Competition](#)

[Computer books](#)

[Find a computer  
business near you](#)

[Site index](#)

[About us](#)

[Contact us](#)

## Personal View: Robbers lurk online to snatch your cash

By Charles Smith  
(Filed: 27/08/2003)

- ▼ [Does it happen?](#)
- ▼ [What you can do](#)

Today's online banking systems have presented criminals with an excellent opportunity to rob banks from the comfort of an armchair. No longer is there the need for stocking masks or guns, but just a laptop PC and a telephone connection located anywhere in the world.

When you join an online internet banking system great care is taken over the security of providing a user-identity code, PIN and password. The data transmitted between your PC and the bank's computers is encoded by very secure methods. The process is normally indicated by a small padlock symbol appearing on the web browsing screen.

There is, however, a major security flaw in the process. No breaches have yet been detected in the UK, but retail banks need to do more to protect their customers by addressing the potential pitfalls.

There is software out there that has the capability to record every keystroke that you make on your PC keyboard before they become encoded by your web browser. This key-stroke information is stored in hidden data files.

The software operates in a "stealth mode", which means that a normal PC user will be unaware that the software is present on their machine. The spyware will also log the website pages that you are visiting at the time and full details of the data you are keying in, such as your user ID and password.

You might ask how a thief can get at those keystroke log files hidden on your PC. The spyware will generate e-mail messages containing the hidden log files. The next time that you connect to the internet it will silently e-mail them to the hacking thief. The thief does not have to be connected to your PC at the same time as you to get at the information on passwords.

The thief can have a daisy chain of e-mail accounts, in different countries, that forward the keystroke log file e-mail from your PC between themselves, making it very difficult to track the eventual destination.

**EXTERNAL LINKS**

► [Oaksys Tech](#)

The thief will dial up from a remote location and log into your bank account using the harvested user ID and passwords and have full access to the banking facilities. As far as the bank is concerned it is the authenticated account owner connecting with the correct passwords. You will have a difficult time proving otherwise.

If you have a rarely used low-activity bank account it may be used as a stepping stone in a trail of accounts used to launder ill-gotten money by transferring sums from other accounts containing large amounts of funds.

It is shockingly easy to obtain the software. I gave my schoolboy son the task of locating some. Within five minutes, using internet search tools such as Google, he had located, downloaded and installed a shareware version of the software on one of our home computers.

How would a thief install the spyware on your PC? If you share a computer with other people at work or a cyber cafe it can be done easily while you are away. Or the thief may send you a "spam" e-mail containing a Trojan/virus program. The Trojan either installs the software or provides a backdoor program that tells the thief where the PC is located so he can break in electronically and install the software from a remote location.

Maybe your children have downloaded some MP3 music sharing software. Many of these programs contain software Trojans that could lead to a break-in to your PC.

Another method of extracting your user ID and password from you is called "Phishing". In this case the criminal sends you an official looking e-mail. The e-mail will be forged so that it appears that it has come from your own bank, share trading account or online auction service. The e-mail will invite you to log on to the company's website to verify the details of your account. There will be a link in the e-mail that you can click on to go to the website.

The provided link will send you to a forged website, looking identical to the official company website. It will invite you to sign on and check your details.

When you have entered the important user data such as user ID, password, credit card, you will be switched from the forged website to the official one. When you reach the official site it will look as though your log-on failed. You have entered your user ID and password into the criminal's own database for future use.

■ Charles Smith is a director of Oaksys Tech, an information technology consultancy

### **Does it happen?**

In New York shops called Kinko's provide internet

access through rented internet cafe PCs. In July 2003 CNN reported that Juju Jiang had installed keystroke logging software on the Kinko's PCs and over a year had captured the details of over 450 people.

This year a Boston college student had installed spyware software on over 100 campus PCs. Some employers use spyware to monitor employee internet usage of work PCs. I personally receive at least one Phishing email a week.

### **What you can do**

- Change your bank account password frequently.
- If someone purporting to be from the bank calls you, never give them the password. Call back using their published support desk number.
- If you get an unexpected email from the bank asking you to log on to their site and check your details, do not use the link provided. Call the Bank's support desk and check if it is a valid email.

© Copyright of Telegraph Group Limited 2003. [Terms & Conditions of reading.](#)  
[Commercial information.](#) [Privacy Policy.](#)