

Fraudsters target Gmail and Facebook

Criminals are raking in £10m per day from identity fraud and the number of victims is rising rapidly.

According to the latest figures from Cifas, the UK's Fraud Prevention Agency, nearly 27,000 victims of impersonation were recorded during the first three months of this year - an increase of just over 6,000.

Social networking sites such as Facebook are fertile hunting grounds for fraudsters. Those who are overly liberal with their personal information or who don't activate the privacy settings could be leaving themselves vulnerable.

The site came under fire in December last year from privacy groups, the Electronic Frontier Foundation and the American Civil Liberties Union, for 'encouraging' its 350 million users to make their personal details available to everyone on the internet.

Users are now asked to choose whether to make various settings available to 'everyone' or continue with the old settings.

Information which users had saved on the site, which could include where you live, date of birth, family, relationships, work and education, were automatically made public unless users 'unticked' the correct boxes.

Concerns have also been raised recently over the security of millions who use Gmail - Google's email service. If a user leaves their account open, personal email setups can be changed with just a few simple clicks to allow fraudsters to divert financially sensitive emails to their own account.

Cases have been reported where emails featuring words such as 'sort code' or 'bank details' are diverted to another email account - without the intended recipient ever knowing the email was sent. Anyone who leaves a public computer unattended with their account open could have their settings altered in seconds to forward sensitive emails.

James Jones from credit reference agency Experian says: 'There is a huge disconnect between the privacy we crave and the information we give away on social networks. It's hardly surprising that identity fraudsters have been cashing in.'

A favourite ploy used by criminals is phishing - where victims receive an email purporting to be from a bank or other organisation. Victims click on to a link to a fake website where they are asked to enter their personal details.